

**THE CITY OF NEW YORK
OFFICE OF PAYROLL ADMINISTRATION**

**REQUEST FOR PROPOSALS
TO PROVIDE TRANSIT BENEFIT SERVICES FOR CITY EMPLOYEES
PIN # 09131000042569**

TABLE OF CONTENTS

- I. TIMETABLE**
- II. SUMMARY OF REQUEST FOR PROPOSALS**
- III. SCOPE OF SERVICES**
- IV. FORMAT AND CONTENT OF THE PROPOSAL**
- V. PROPOSAL EVALUATION AND CONTRACT AWARD PROCEDURES**
- VI. GENERAL INFORMATION TO PROPOSERS**
- VII. ATTACHMENTS AND ENCLOSURES**

**ATTACHMENT A – PROPOSAL COVER LETTER
ATTACHMENT B – PRICE PROPOSAL FORM
ATTACHMENT C – ACKNOWLEDGEMENT OF ADDENDA
ATTACHMENT D – TAX AFFIRMATION FORM
ATTACHMENT E – VENDEX INFORMATION
ATTACHMENT F - LOCAL LAW 34 DOING BUSINESS DATA FORM
ATTACHMENT G – SUPPLY AND SERVICE EMPLOYMENT REPORT**

EXHIBIT 1 – LIST OF SUBCONTRACTORS

ENCLOSURES:

**APPENDIX A – GENERAL PROVISIONS GOVERNING CONTRACTS FOR
CONSULTANTS, PROFESSIONAL AND TECHNICAL SERVICES**

SECURITY POLICIES

This Request for Proposals (RFP) solicits the services of one or more companies to assist the New York City Office of Payroll Administration (OPA) in the operation and administration of a Transit Benefit program for City employees in conformance with 26 U.S.C. § 132(f). Once proposals have been received, OPA will conduct a selection process based on an evaluation of a proposers' technical ability to provide the required services at a cost that is most advantageous to the City. Proposers will be required to submit both a Technical Proposal as well as a Price Proposal (in combination, "the Proposal") in response to this RFP.

SECTION I. TIMETABLE

- A. Pre-Proposal Conference: A Pre-Proposal Conference will be held at One Centre Street, 18th Floor Conference Room (enter through the south side of the building), on December 15, 2008 at 10:30 AM. Proposers will be required to pass through metal detectors and present photo identification to building security to enter the facility. Attendance at this pre-proposal conference is not mandatory to propose on the contract described in this RFP; however, it is strongly encouraged.

Submissions: Submissions shall be delivered at or before 12:00 Noon on January 9, 2009, clearly marked with "Office of Payroll Administration Transit Benefit Proposal" on the exterior of the envelope or other packaging.

Authorized Agency Contact Person: Proposers are advised that the authorized agency contact person for all matters concerning this RFP is:

Valerie Himelewski, ACCO
Office of Payroll Administration
One Centre Street, Room 200N
New York, New York 10007
E-mail: vhimelewski@payroll.nyc.gov
Phone: (212) 669-3455
Fax: (212) 669-4626

The proposer shall hand deliver or deliver via an express mail service the Proposal to the authorized agency contact person at the above address.

NOTE: Proposers are held responsible for ensuring that the RFP response is received at the Office of Payroll Administration no later than the deadline for submissions.

- B. Inquiries: In the event a proposer desires any explanation regarding the meaning or interpretation of any of the provisions of this RFP, such explanation must be requested in writing (e-mail requests are acceptable), no later than the date and time of the Pre-Proposal Conference prescribed in Section I(A) of this RFP. In the event OPA determines that it is necessary to respond in writing to the inquiry, such response will be furnished as an addendum to the RFP to all potential proposers.
- C. Addenda: Receipt of an addendum to this RFP by a proposer must be acknowledged by attaching an original signed copy of the addendum to the Proposal. All addenda shall become a part of the requirements for this RFP.
- D. RFP Schedule: The following is the estimated timetable for receipt, evaluation, and selection of proposals. This is only an estimate and is provided to assist responding firms in planning.
 - a. Identify Contractor: Within eight weeks of submission deadline.
 - b. Contract Registration: Approximately four months from date of Contractor selection.
 - c. Contract Commencement: Upon receipt of Advice of Award.

SECTION II. SUMMARY OF THE REQUEST FOR PROPOSALS

- A. Background and Objectives of the Project: The New York City Office of Payroll Administration (“OPA”) currently administers three transit benefit programs for the City’s employees. These programs are described in detail below and are funded by a combination of payroll deductions taken by the City’s Payroll Management System (“PMS”) from the earnings of participating employees for the purchase of transportation fare media and a City contribution to cover some administrative costs. The programs allow employees who elect to participate to purchase transit fare media (transit passes) with pre-tax funds deducted from their paychecks in conformance with 26 U.S.C. §132(f). Supported transportation options include City subways and buses as well as Access-A-Ride paratransit service. A desired expansion in the participating population and in the number of benefits to be offered has led OPA to seek the services of one or more vendors to administer a revised Transit Benefits Program.

The selected vendor(s) will be expected to provide transit passes, transportation debit/credit cards, reimbursement services (as applicable), administrative support and customer service, including employee enrollment, replacement of lost or damaged vendor-provided media and suspension or termination of employee participation, in connection with

the operation of the transit benefit programs. In addition, the selected vendor(s) will interface with OPA and representatives of other relevant City agencies in support of the provided transit benefit services to City employees.

It is the goal of this RFP to maximize the transportation options available to City employees under this program to the degree allowed by 26 U.S.C. §132(f). The only restrictions are those directed by City policy. An example of such a policy driven exception is that the City may choose, at its option, to impose geographic limitations on commuter parking under this program. OPA seeks to obtain maximum contractor-provided services in connection with administration of the transit benefit programs and to limit the use of City resources in connection with operation of the programs.

- B. Joint Ventures and Other Contractor Relationships: To meet the requirements of this RFP, a proposer may propose to provide services in conjunction with one or more other company(ies) in a joint venture. There is no minimum requirement for the proportion of work by any such joint ventured parties; however, one of the parties must be the prime contractor with the other party or parties, the sub-contractor(s). The prime contractor will be held responsible for performance under the resulting contract. Joint ventures must carry the required insurance either as policies written specifically for the joint venture entity, or by using their existing single entity policies with endorsements written for the joint venture activity.

OPA does not recognize the corporate configuration wherein one company is “in association with” another. Relationships between two or more firms shall be either as joint venture or prime contractor/subcontractor. In the event that a proposal is received wherein two or more firms are described as being “in association with” each other, OPA will treat the relationship as one of prime contractor/subcontractor(s). The proposal evaluation process will be handled accordingly, and if chosen as a winner, the contract documents will show only the prime firm on the signature page, and all other firms will be relegated to Exhibit 1, which lists any subcontractors that the Proposer will be engaging in connection with the project.

- C. Anticipated Contract Term: It is anticipated that the term of the contract shall commence on the date set forth in the Advice of Award and shall continue for a term of four (4) years with the opportunity of two additional two (2) year renewals, exercisable at OPA’s sole discretion.
- D. Insurance: The selected contractor(s) providing services for the project must provide the types and amounts of insurance specified in the contract. At a minimum, the contractor(s) will be required to provide Commercial

General Liability Insurance in the amount of One Million Dollars (\$1,000,000).

- E. Anticipated Payment Structure: It is anticipated that the payment structure of the contract awarded from this RFP will be based on payment to the contractor for the value of any transportation passes or qualified services purchased by the contractor for participating City employees plus an administrative fee per participating employee. However, OPA will consider alternative payment structures and reserves the right to select any payment structure that is in the City's best interest.

SECTION III. SCOPE OF SERVICES

- A. Transit Benefit Options: This RFP is intended to provide maximum flexibility and options for City employees to use pre-tax and post-tax earnings to purchase transportation fare media (transit passes) and other transportation options as may be permitted by 26 U.S.C. § 132. Respondents may therefore submit a Proposal to provide services in connection with City employee purchase of transit passes on any one or more of the following types of mass transportation or (as applicable) to provide reimbursement for costs related to the services listed below:

1. City subways and buses, including express buses;
2. the Metropolitan Transportation Authority's Access-a-Ride paratransit service;
3. other paratransit service for the disabled;
4. regional commuter railroads;
5. regional commuter bus lines;
6. regional commuter ferries and water taxis;
7. commuter van service; and
8. commuter parking (subject to geographic limitations and facility connection with mass transportation).

- B. Compliance with Federal Regulations: The selected vendor(s) must comply with 26 U.S.C. § 132(f) and all federal laws and regulations applicable to the pre-tax purchase of transit passes that are currently in effect or that will be enacted or revised during the term of the contract. The selected vendor(s) will be liable for and must indemnify and hold the City and its employees harmless from any costs incurred by the City or its employees which result from the failure of the vendor(s) to operate the Transit Benefit Program in full compliance with all relevant laws and regulations. Such costs may include, but are not limited to, fines, penalties, and additional tax liabilities imposed on the City or its employees.

C. Current Transit Benefit Programs Administered by OPA: OPA currently administers three transit benefit programs for City employees.

1. Transportation Spending Account Commuter Savings Card – This program provides a Personal Identification Number (PIN)-based debit card (TSA Card) linked to a Transportation Spending Account secured by the City's current contractor. The TSA card is mailed to each participant's designated transit benefit address. It can only be funded by transportation deductions taken from each participant's pay. Participants may choose one of five deduction plans. The TSA Card is restricted so that it only functions at MetroCard Vending Machines and can only be used to purchase MetroCards for use on New York City Transit subways, local buses and express buses.

There are no enrollment periods for the TSA Card program. Participants may enroll at any time and will receive the TSA Card in the mail at the designated address within 10 business days. Participants may also change address or deduction plans, temporarily suspend transportation deductions from their pay, or cancel their participation at any time. All transactions (new enrollments, changes and cancellations) require the provision of the City's unique seven digit numeric employee reference number and are requested via the completion of the TSA Card form/application. The form must be completed and signed by the participant and submitted to the designated agency Transit Benefit coordinator for manual processing within PMS. PMS creates and sends an electronic file containing all new enrollments, changes of address and cancellations to the TSA Card program contractor each night (deduction plan changes and suspensions are not sent to the contractor). On the following business day, the TSA Card contractor returns an electronic file to PMS containing a TSA Card account number for each new enrollment. Upon receipt of the account number file, PMS sets up the deduction within the participant's PMS record. TSA payroll deductions begin on the first paycheck that is calculated after PMS sets up the deduction. TSA Card deductions are sent via Automated Clearing House (ACH) transactions to each individual TSA Card account. The ACH settlement date is the pay date. The participant may purchase any type of MetroCard, unlimited or pay-per-ride, in the denomination of their choice, up to the available balance. Upon cancellation, the participant has up to 30 days to spend any available balance to purchase MetroCards. The account is then closed and any remaining funds are returned to the City.

The TSA Card program contractor provides customer service options to the participant such as read-only online account balance and status access and a toll-free customer service phone number. The phone number is a Voice Response Unit (VRU) and has an option that directs the caller to speak with a contractor representative. Both options are available to participants 24 hours a day, seven days a week. Participants report problems with the delivery or functioning of their TSA Card directly to the contractor via the VRU. The contractor will send replacement of damaged, lost, stolen or undelivered TSA Cards directly to the transit benefit address on file. There is a fee for damaged card replacements. The replacement fee is invoiced by the contractor to OPA on a monthly basis. OPA collects the fee from the participants via payroll deduction, processed manually in PMS by OPA. Participants report any TSA Card funding issues to the designated agency Transit Benefit coordinator or to OPA.

The contractor provides OPA access to a TSA Card web-based system maintained by the contractor. OPA's user role allows OPA to view cardholder account status and deduction history information. The system allows OPA the ability to run management reports such as account status and replacement card reports. It also allows for the transfer of funds to cardholder accounts from the funding account.

OPA prefers the ease with which TSA Card accounts are funded via ACH each pay date and the flexibility of allowing the employee to select from varying deduction amounts with the option to temporarily suspend deductions from pay without interrupting the service of the TSA Card.

The major challenges that OPA has faced with the TSA Card program include, but are not limited to:

- Problems with vendor technology changes
- Duplicate TSA Card issuance
- Mis-posted debit and credits
- Contractor customer service staff supplying incorrect information
- Debit cards not working at MetroCard Vending Machines
- Poor marketing support
- ACH account information not transmitted
- Incorrect participant address on contractor file
- Solicitation of TSA Card participants of other vendor products and services

There are approximately 4,000 participants enrolled in this program to date.

2. Premium TransitChek MetroCard – This program offers an annual, unlimited ride MetroCard provided by a City contractor. The Premium TransitChek MetroCard (Premium Card) is mailed to each participant's designated transit benefit address and can be used for a continuous twelve-month period for unlimited rides on the subway and local buses. This card is funded by a set deduction that is taken on a completely pre-tax basis from each participant's pay. The continuous use of the Premium Card is contingent upon continued payroll deductions.

OPA maintains a monthly enrollment period schedule whereby an employee can opt to participate in the program with the expectation of having use of the Premium Card on the first day of the second month following enrollment. All transactions (new enrollments, changes of address and cancellations) currently require the provision of the social security number and are requested via the completion of the Premium Card form/application. The form must be completed and signed by the participant and submitted to the designated agency Transit Benefit coordinator for manual processing within PMS. The payroll deductions of new enrollees commence on the first pay date occurring in the month after the enrollment information is entered into PMS.

Each month a data file, participation file, containing all new enrollments, changes of address and cancellations processed during the enrollment period is produced out of PMS and transmitted to OPA by the Financial Information Services Agency (FISA). Each record contains a status of either active or inactive that determines whether or not an employee will be able to use the Premium Card during the following month. A status of active on the participation file is contingent upon an active PMS enrollment status and continued payroll deductions and results in the continued usability of the Premium Card during the following month. A status of inactive, due to a cancelled PMS enrollment status or missed payroll deduction(s), results in the deactivation of the Premium Card on the first day of the following month.

Upon receipt of the file, OPA reviews it, updates if necessary the file content, uploads the data into an internal Premium Card database system, and then transmits the file to the Premium Card contractor via secure FTP transmission. The contractor acknowledges receipt of the file via e-mail and proceeds to issue new Premium Cards, update addresses, and process the

deactivation of existing Premium Cards that have a status of inactive on the file. The contractor will mail out new Premium Cards to the participant's transit benefit address during the month when payroll deductions commence. These cards will become active for use on the first day of the month after deductions started. Payroll deductions will continue until the employee either terminates enrollment or has insufficient earnings.

The internal Premium Card system maintained by OPA allows OPA staff to view participant enrollment status and history and to produce several reports. One of the reports is the monthly payment statement which is used by OPA to notify the contractor of the enrollment count and payment due them. The contractor receives the statement and payment via wire transfer once a month. The contractor will only activate and deactivate cards on the first calendar day of each month. Participants can use the Premium Card an unlimited number of times during the month on the subway and local buses.

The Premium Card contractor does not provide direct customer service to participants. They do provide a customer service phone number for inquiries; however, callers are directed to OPA for specific program information. Premium Cards that become damaged, lost, stolen or undelivered must be replaced by OPA. There is no fee for replacements but participants may only request a replacement Premium Card from OPA by mail, fax, or in person.

The contractor supplies OPA with a stock of replacement Premium Cards each month to be assigned to participants with defective or missing cards. The contractor also provides OPA with an online replacement system, maintained by the contractor, which allows the deactivation and assignment of replacement Premium Cards.

OPA prefers the marketing support supplied by the contractor. Annual marketing campaigns bring awareness of the program to our eligible employee base.

The major challenges that OPA has faced with the Premium Card program include, but are not limited to:

- Premium Card Replacement system data corruption
- Problems with vendor technology changes
- Duplicate Premium Cards issued to participants
- Triplicate Premium Cards issued to participants
- Missed Premium Card mailings
- Late Premium Card mailings

- In-house replacement card process is labor intensive for OPA
- Incorrect Premium Card deactivations
- System not tracking correct anniversary card date
- Use of social security numbers instead of employee reference number
- Problems with tracking monthly employee deduction balances to determine the enrollment status on the participation file
- Lag time between date of enrollment and receipt of an active Premium Card
- Outdated technology platform of the internal Premium Card system makes it difficult to maintain

There are approximately 55,000 participants enrolled in the Premium TransitChek MetroCard program to date.

3. Access-A-Ride Transit Benefit – This program offers City employees with disabilities who are actively enrolled in the Metropolitan Transportation Authority New York City Transit (MTA NYCT) Access-A-Ride paratransit service to receive reimbursement of pre-tax payroll deductions with coupons that are accepted fare media on the MTA Access-A-Ride vans that provide the paratransit service. Each coupon is the equivalent of a single ride fare. The Access-A-Ride (AAR) program is provided by a City contractor. The contractor mails AAR coupons to each participant's designated transit benefit address, which equal the value of monthly deductions from a participant's pay. Two deduction plans are available.

AAR enrollments are limited to employees who obtain approval to receive Access-A-Ride services from the MTA NYCT. OPA maintains a monthly enrollment period schedule whereby an employee can opt to participate in the program with the expectation of receiving AAR coupons during the first month following enrollment. All transactions (new enrollments, changes of deduction plan, address and cancellations) currently require the provision of the social security number and are requested via the completion of the AAR form/application. The form must be completed and signed by the participant and submitted, along with proof of MTA NYCT AAR participation approval, to the designated agency Transit Benefit coordinator for manual processing within PMS.

PMS will create a data file containing all new enrollments, cancellations, changes of address and total monthly deduction

amounts processed during the enrollment period. This data file is produced out of PMS by FISA and transmitted to OPA once a month. The file contains a record for active AAR participants from the previous period in addition to any new enrollments from the current period. Each record contains the most recent mailing address and the total amount deducted from pay during the month. Upon receipt of the file, OPA reviews and updates the file content, uploads the data into an internal AAR database system, and then transmits the file to the contractor via secure FTP transmission. The contractor acknowledges receipt of the file via e-mail and proceeds to mail AAR coupons to the latest address received on the file. The payroll deductions of new enrollees commence on the first pay date occurring after the enrollment is processed in PMS. Payroll deductions will continue until the employee either terminates enrollment or has insufficient earnings.

The internal AAR system, maintained by OPA, allows OPA staff to view participant enrollment status and history and to produce several reports. One of the reports is the monthly payment statement which is used by OPA to notify the contractor of the enrollment count and payment due them. The contractor receives the statement and payment via wire transfer once a month.

The AAR contractor provides customer service to participants by way of a customer service phone number for inquiries. AAR coupons that become damaged, lost, stolen or undelivered are replaced by the contractor. There is no fee for replacements. Participants report any AAR funding issues to the designated agency Transit Benefit coordinator or to OPA.

The major challenges that OPA has faced with the AAR program, include but are not limited to:

- AAR coupons mailed to inactive participants
- AAR coupons mailed late to active participants
- Use of social security numbers instead of employee reference number

There are approximately 60 participants enrolled in the AAR program to date.

D. New Program Specifications:

1. Enrollment Data/Data Entry – OPA will provide enrollment data. The successful vendor(s) must be able to capture and maintain that data in a system that will support vendor management of administrative processes and OPA customer service. Enrollment data will include the following for each participant:
 - Employee Full Name
 - Employee Reference Number (OPA will not provide employee social security numbers)
 - The City's three digit numeric payroll number (this number is used to identify the business unit/department where employee works and is used for demographic data and sorting purposes)
 - Employee designated transit benefit mailing address
 - Employee e-mail address, if available, to be used as a means of communication and marketing
 - Employee day-time phone number
 - Employee enrollment date
 - Transit Benefit program(s) in which the employee is enrolled, as updated
 - Employee cancellation date (designated as 99/99/99 or similar value while the enrollment is active)

All participating employee data collected and/or maintained in connection with the transit benefit programs must be kept strictly confidential.

City employees validate and update certain payroll information tracked in the City's Human Resources System, New York City Automated Personnel System (NYCAPS). The Employee Self-Service (ESS) component of NYCAPS is securely accessible by City employees through the City's Intranet as well as the Internet. ESS is the controlling mechanism by which employees will enroll, change, suspend or cancel their participation and transit benefit deduction amounts. Once enrollment data and deduction amounts are entered in ESS, NYCAPS interfaces nightly to PMS. PMS will update the employee's Transit Benefit information. The selected vendor(s) will receive required data from PMS.

OPA may provide the selected vendor(s) with a file containing information about participants in one or more of the existing transit benefit programs listed in Section III C as part of a transition process to new programs under contracts negotiated after the RFP process.

2. Transit Benefit Accounts – A transit benefit account must be established for each participant to maintain a detailed history of the balance of funds deducted from enrollees' pay and the transit fare media purchased. Open deduction amounts in denominations to be determined by the employee/participants are preferred. System accommodations for both pre-tax and post-tax deductions which are clearly identified and calculated for the enrollees should be available to allow participants full access to all transportation fare media options. Unless the selected vendor(s) can demonstrate to OPA's satisfaction that it would be impracticable under certain benefit programs, all programs must allow each participant the ability to elect the temporary suspension of payroll deductions without cancellation from the program and/or the requirement to re-enroll in the program when deductions resume from pay.
3. Transit Benefit Account Funding – The City has various payroll pay cycle dates. Pay dates can occur each and every business day. They are:
 - Weekly (Fridays, 52 pay dates per year)
 - Bi-weekly I (Thursdays same week as bi-weekly III, 26 pay dates per year)
 - Bi-weekly II (alternate Thursdays, 26 pay dates per year)
 - Bi-weekly III (Fridays, 26 pay dates per year)
 - Semi-monthly (24 pay dates per year)
 - Supplemental pay dates as needed

The pay calculation date for each payroll cycle's pay date is normally 6-7 calendar days prior to the pay date. Supplemental payrolls are processed intermittently with a shorter lead time. In addition, Summer payrolls for Department of Education pedagogues and hourly support staff have pay calculation dates at the end of May/beginning of June. Checks are pre-printed for the Summer payrolls. Participant transit benefit deductions occur on each pay date. The City intends to send ACH transactions on a daily basis to the vendor(s) to transfer deduction amounts into participant Transit Benefit accounts. Funds for transit benefit accounts must be available on the pay date. The vendor(s) must be able to accommodate ACH reversals. An ACH reversal is defined as the action the City takes to reverse an employee ACH deduction transaction for Transit Benefits from the Transit Benefit account. As part of the enrollment application process, the employee will grant authorization for the reversal of a credit to his/her account in the event the credit was made in error. This authorization remains in effect until he/she cancels the transit benefit deduction.

4. Fare Media Purchase Methods and Restrictions – OPA prefers that the selected vendor(s) provide as many options for purchase of transportation fare media to enrollees as possible including, at a minimum, equivalence to the options already provided by the City. Options may include, but are not limited to, online purchases directly from the vendor website, purchases through a vendor Voice Response Unit (VRU), debit/credit card purchases from MTA and other approved mass transit provider vending machines, certain approved merchants or online from mass transit providers. Under circumstances when the selected vendor(s) can demonstrate to OPA's satisfaction that it would be otherwise impracticable, a reimbursement type program may also be acceptable. To maintain compliance with the eligibility requirements for the pre-tax status of the deductions taken from employees' pay according to 26 U.S.C § 132, credit/debit cards provided under this program must have their use restricted to only allow the purchase of commuting goods and services. Credit/debit cards that may be used for the purchase of non-commuting goods and services may not be offered to City enrollees in transit benefit programs. Any transportation fare media and debit/credit cards which will be provided by the vendor must be delivered via mail to an enrollee's designated transit benefit address.
5. Transit Benefit Account Closures - Residual closed account balances are to be refunded automatically to the participant within accepted IRC specifications. Employees must be notified when their account is closed or changed. Funds must be available in the closed account for a negotiated period of time to allow the employee to draw down the remaining funds.
6. Customer Service – The selected vendor(s) must provide customer service to enrollees at a minimum through both a website and a toll free customer service phone number. These systems must maintain functionality to log the number of online inquiries or telephone calls received. The employee should be able to access account/program status, address information, transaction history, customer service information, and any service announcements related to the program and/or their benefit. All types of customer service must be accessible, at a minimum, from 8AM through 6PM, Monday through Friday. Extended hours beyond this minimum are preferred. Any replacements of transit benefit products or fare media for enrollees must be provided by the selected vendor(s). Exceptions may be made for fare media replaced by the transportation provider. OPA should not be expected to handle

customer service issues on behalf of the vendor(s). OPA expects that the expansion of transit benefit options will result in a substantial increase in the number of participants in transit benefit programs with the City. There are approximately 306,000 City employees eligible to participate in transit benefit programs. Accordingly, the selected vendor(s) should have a demonstrated ability to service a large customer base. The City will not guarantee that a specific number of City employees will enroll in any transit benefit programs.

7. Marketing/Promotion – OPA expects the selected vendor(s) to increase awareness of the City's transit benefit programs by engaging in marketing campaigns and outreach to eligible City employees. Proposers should thus include in their technical proposals a description of any anticipated marketing/promotion tools that will be used in such efforts. Examples of some prior marketing tools used in the promotion of City transit benefit programs include annual posters about the programs, payroll companions, e-mail notifications and targeted direct mail outreach. The City must approve all marketing or promotional materials used in connection with the transit benefit programs.

Any contract(s) resulting from this RFP shall contain language in substantially the same form as outlined below regarding ownership and copyright of materials. The City may grant the contractor(s) permission to use the City seal, the name of the City and the names of City officials in the marketing and promotional materials, which grant of permission shall be governed by the terms and conditions that will be set forth in the contract(s) awarded pursuant to this RFP. Upon OPA's request, the contractor(s) shall grant permission to use the vendor's name and logo in the marketing and promotional materials, which grant of permission shall be governed by the terms and conditions that will be set forth in the contract(s) awarded pursuant to this RFP.

Copyrightable Materials

Any reports, documents, data, photographs and/or other materials, including software, produced pursuant to this Agreement (Copyrightable Materials"), shall be considered "work-made-for-hire" within the meaning and purview of Section 101 of the United States Copyright Act, 17 U.S.C. § 101, and the City shall be the copyright owner thereof and of all aspects, elements and components thereof in which copyright protection might subsist. To the extent that the Copyrightable Materials do not qualify as "work-made-for-hire," the Contractor hereby irrevocably transfers, assigns

and conveys exclusive copyright ownership in and to the Copyrightable Materials to the City, free and clear of any liens, claims, or other encumbrances. The Contractor shall retain no copyright or intellectual property interest in the Copyrightable Materials, and they shall be used by the Contractor for no other purpose without the prior written permission of the City.

The Contractor acknowledges that the City may, in its sole discretion, register copyright in the Copyrightable Materials with the U.S. Copyright Office or any other government agency authorized to grant copyright registrations. The Contractor shall cooperate in this effort, and agrees to provide any further documentation necessary to accomplish this.

To the extent that any artwork does not qualify as a “work-made-for-hire,” the artist acknowledges the existence, if any, of his or her statutory moral rights as those rights are described in 17 U.S.C. § 106A, and any rights arising under federal or state law or under the laws of any other country that conveys rights of the same nature as those conveyed by 17 U.S.C. § 106A, or any other type of moral right or droit moral.

The contractor(s) shall defend, indemnify and hold harmless OPA and the City, and their officers, employees and agents, from and against any and all claims, suits, damages, judgments, liabilities, costs and expenses, including reasonable attorney’s fees, to which they may be subject because of or related to any claim that the Copyrightable Materials infringe or violate the copyright, trademark, tradename or any other proprietary or personal right of any third party. This indemnification provision shall not be limited in any way by the Contractor’s obligations to obtain insurance as provided under the contract(s) awarded pursuant to this RFP.

8. Program Management System for OPA – The City/OPA will require access to the vendor(s) website or system containing participant records. The access is needed for OPA to provide information on an as-needed basis to participants or agency personnel and to monitor the progress of the programs. Information that will need to be accessed includes but is not limited to:

- Account Status
- Account Balance
- Transaction History
- Personal Account Information
- Financial Reports (Account Balance, Reversals)
- Other Reports (Active, Inactive, Closed, Summary)

- Demographic Reports (Enrollment by Payroll Number)
9. Continuity of Operations Plan – Vendors should specify the contingency plans that will be put into effect to ensure continuity of operations in all aspects of the transit benefit program in the event of emergencies or system interruptions.
 10. Quality Control Process – Vendors should provide a detailed description outlining the quality control process that will be in place to identify, prevent, inform and correct problems in the operation of the transit benefit program. Specifically, vendors should address how the quality control process will address the challenges described in Section III C of this RFP that have been encountered in the operation of our current programs.
 11. Data Security (IT) Requirements: OPA maintains a technical infrastructure and highly complex network environment comprised of many security features to protect and safeguard the City's sensitive information assets. These assets are maintained in a Microsoft Windows multi-tiered environment which includes enterprise class servers issuing services such as SQL databases, File & Print, Visual Studio Team Foundation (development of in-house applications) and Terminal services (remote access management). In addition, identity and authentication management is performed within the OPA Active Directory domain structure, where domain controller servers provide domain name services (DNS), group policy management and access control management of directories and files. The Information Technology Services/Network Operations division is charged with the responsibility of providing and maintaining a network environment in compliance with the directives and policies promulgated by the New York City Department of Information Technology and Telecommunications (DoITT) Security Division and its predecessor, the New York City Department of Investigation Citywide Information Security Architecture Formulation and Enforcement (CISAFE). Additionally, the DoITT Security Division plays an immense role in OPA's application security by providing directives to ensure that developed applications whether designed in-house or by outside vendors maintain the highest level of security and integrity. Through these directives, guidelines and procedures, compliance must be maintained throughout the applications' life cycle. Moreover, applications, once developed, must undergo an accreditation process by DoITT's security division before the application can be utilized by the OPA user community.

The DoITT policies govern how users interact with highly sensitive data in conjunction with methods of authentication, authorization and accounting to provide the highest security protection to safeguard the data from unauthorized individuals and to ensure that the data is used strictly for business purposes. The OPA network environment is a member of the larger City of New York network system (CityNet) that adheres to and is compliant with all policies and guidelines that govern the extremely large and complex CityNet intranet. The intranet offers extranet capabilities that provide external entities Wide Area Network (WAN) access to OPA resources through various network applications (i.e. HTTPS, Secure FTP, etc.) These various connection services are also governed by DoITT, which sets policies on security and connection implementations. All City and non-City personnel including temporary contract employees, contractors, vendors, consultants and the vendor/consultant Company for which they work are subject to these policies.

In addition to Citywide requirements, the selected vendor(s) will be required to adhere to specific OPA security requirements. Vendor staff that will have access to City employee personal data may be required to undergo nationwide background checks (at the vendor's expense) and sign non-disclosure/confidentiality agreements before accessing any such data. These agreements prohibit the vendor's staff from disclosing to any third party any confidential, non-public information concerning the operations of the City.

Vendors should specify the security measures they currently have in place with respect to their operations and staff.

- E. Failure to Perform Contracted Services: As further described in any contract(s) awarded pursuant to this RFP, the selected vendor(s) shall be liable to the City for any and all damages incurred by the City as the result of the vendor(s) failure to perform the services required under the contract(s). Such damages may include, but are not limited to; costs for City staff time and resources (including correspondence or technical programming costs) required to address contractor performance failures; and any fees, costs, penalties or additional tax liability incurred by the City or its employees based on Contractor failures to operate the Transit Benefit Program in full compliance with relevant laws and regulations.

SECTION IV – FORMAT AND CONTENT OF THE PROPOSAL

Instructions: Proposers should provide all information requested on 8 ½ x 11” paper, double-sided. Pages should be paginated and sections clearly defined. The proposal will be evaluated on the basis of its content, not length.

A. Proposal Format

1. Proposal Cover Letter – The Proposal Cover Letter form (Attachment A) transmits the Proposal Package to the Agency. It must be completed, signed and dated by an authorized representative of the Proposer.
2. Technical Proposal – The Technical Proposal is a clear, concise narrative that addresses the following:

- a. Experience

Describe the successful relevant experience of the Proposer, each proposed subcontractor if any, and the proposed key staff who will provide the work described in Section III of this RFP. Specifically, address the following:

- Describe the Proposer’s successful experience in providing the services described in Section III of this RFP, detailing the number of years of experience in performing services of the type required by this RFP, the specific services performed, the entity for which the work was performed, the number of participants served, and the outcome or status of such projects (e.g., whether or not the programs were/are successful and if not, why not).
- Identify each proposed subcontractor, if any, to be involved with this project, describing their roles in the project and their relevant experience.

In addition:

- Attach (for the Proposer and each subcontractor, if any) a listing of at least two relevant professional references, including the name of the reference entity, a brief statement of the relationship between the Proposer or proposed subcontractor (as applicable) and the reference entity, and

the name, title, and telephone number of a contact person at the reference entity.

- Attach for each key staff position a resume and/or description of the qualifications of the key staff. In addition, provide a statement certifying that the proposed key staff will be available for the duration of the project (normal staff attrition excepted).

b. Organizational Capability

Demonstrate the Proposer's organizational (i.e., technical, managerial and financial) capability to provide the services described in Section III of this RFP. Specifically, address the following:

- Provide a brief history of the Proposer's firm, its overall firm organization and a statement of its mission or philosophy.
- Indicate and demonstrate the sufficiency of the number, level and qualifications of staff that will be allocated to the contract work.
- Indicate and demonstrate the sufficiency of the level of managerial resources that will be allocated to the contract.
- Describe how the Proposer's finances are sufficient to support the contract requirements.

In addition:

- Attach a chart showing where, or provide an explanation as to how, the proposed services will fit within the Proposer's organization.
- Attach a copy of the Proposer's latest independent audit report or certified financial statement, or provide a statement as to why no report is available.

c. Proposed Approach

Describe in detail how the Proposer intends to provide the services described in Section III of this RFP and demonstrate that the proposed approach will fulfill OPA's goals and objectives. OPA's goals include the provision of the greatest number of transit benefit options to City employees. Therefore, Proposers are encouraged to propose a transit benefit program that will provide as many of the transit benefit options listed in Section III A of this RFP as possible. OPA's goals also include minimizing the cost of transit benefit programs to the City and its employees. Therefore, Proposers are encouraged to propose cost-effective strategies and methods in the provision of transit benefit services to eligible City employees. OPA's goals additionally include an expedited transition to the new transit benefit programs. Therefore, Proposers are encouraged to propose efficient, time-saving methods for such set-up and transition to the new programs. Specifically, address the following:

- Provide a brief description outlining the Proposer's understanding of the overall project.
- Describe in detail how the Proposer will provide the services described in Section III of this RFP.
- Provide a Responsibility Matrix
- Provide a detailed project plan that may include, but is not limited to:
 1. Implementation work plan
 2. Technical environment description
 3. Business workflows
 4. Interface requirements
 5. Data conversion requirements
 6. Report/User interface prototypes
 7. Logical data model
 8. Data dictionary
 9. Communication management process
 10. Testing and training plan
- Describe in detail any additional services not listed in this RFP which the Proposer believes are necessary or would be of benefit to the City in the administration of its transit benefit programs.

OPA's assumptions regarding contractor approach represent what the Agency believes to be most likely to achieve its goals and objectives. However, Proposers are encouraged to propose an approach that they believe will most likely achieve OPA's goals and objectives. Proposers may also propose more than one approach. However, if an alternative approach affects other areas of the proposal such as experience, organizational capability or price, that alternative approach should be submitted as a complete and separate proposal providing all of the information specified in Section IV of this RFP.

3. Price Proposal

The Price Proposal Form is included as Attachment B to this RFP. Proposers should propose an administrative fee per participant to cover the costs of providing services to the City under the transit benefit program. If a Proposer intends to provide services for only one or more of the transit benefit options listed in Section III A of this RFP, the Proposer must list each option on the Price Proposal Form with a specific administrative fee proposal that corresponds to the option(s) to be provided. If the fee proposed will change based on the number of participants enrolled in the transit benefit program, the Proposer must indicate the specific administrative fee that will be imposed based on a range of the estimated number of enrollees for each option to which the fee applies. Proposers should note any additional fees that are not included in the administrative fee per participant in the space provided on the Price Proposal Form. A description of the fees must be included. As further described in the contract that will be awarded to the successful Proposer(s), the fees proposed and accepted by the City, after any negotiations, will be fixed for the initial term of the contract. The successful contractor(s) will be permitted an opportunity to request an increase in the fees upon each renewal of the contract. The contractor(s) will be entitled to an increase in fees only if the contractor(s) demonstrate to the City's satisfaction that the contractor's costs have increased, and that there is a corresponding need for an increase in the fees the contractor(s) will charge the City for specific services provided.

Proposers are encouraged to propose innovative payment structures. OPA reserves the right to select the payment structure that is in the City's best interest.

4. Acknowledgement of Addenda

The Acknowledgement of Addenda Form (Attachment C) serves as the Proposer's acknowledgement of the receipt of addenda to this RFP which may have been issued by the Agency prior to the Proposal Due Date and Time, as set forth in Section I A of this RFP. The Proposer should complete this form as instructed on the form.

5. Other Documents

All other documents should be completed by the Proposer as instructed in the noted Attachments.

B. Proposal Package Contents ("Checklist")

The Proposal Package should contain the following materials. Proposers should utilize this section as a "checklist" to assure completeness prior to submitting their Proposal to the Agency.

1. A sealed inner envelope labeled "Program Proposal", containing one original set and the stated number of duplicate sets of the documents listed below in the following order:
 - Proposal Cover Letter (Attachment A)
 - Technical Proposal
 - oo Narrative (10)
 - oo References for the Proposer and Subcontractor(s) (10)
 - oo Resumes and Descriptions of Qualifications for Key Staff (10)
 - oo Organizational Chart (10)
 - oo Audit Report or Certified Financial Statement or Statement as to why no Report is available (1)
 - Acknowledgement of Addenda Form (Attachment C)
 - Exhibit 1 – List of Subcontractors (1, if applicable)

2. A separate sealed inner envelope labeled "Cost Proposal" containing one original set and (10) duplicate sets of the Cost Proposal.
 - Price Proposal Form (Attachment B) (10)
 - Price Proposal Form, Other Payment Structures, Optional (10)

3. A sealed outer envelope, enclosing the two sealed inner envelopes. The sealed outer envelope should have two labels containing:

- The Proposer’s name and address, the Title and PIN # of this RFP (RFP to Provide Transit Benefit Services for City Employees PIN #09131000042569) and the name and telephone number of the Proposer’s contact person.
- The name, title and address of the Authorized Agency Contract Person.

4. Other Documents **(Only To Be Provided Upon Contract Award)**

- Tax Affirmation Form (1)
- Vendex Memorandum informing OPA that the appropriate Vendex Questionnaires have been sent to the Mayor’s Office of Contracts (1)
- Local Law 34 Doing Business Data Form (1)
- Supply and Service Employment Report (1)

SECTION V – PROPOSAL EVALUATION AND CONTRACT AWARD PROCEDURES

A. Evaluation Procedures

All proposals accepted by OPA will be reviewed to determine whether they are responsive or non-responsive to the requisites of this RFP. Proposals that are determined by OPA to be non-responsive will be rejected. OPA’s Evaluation Committee will evaluate and rate all remaining proposals based on the Evaluation Criteria prescribed below. OPA reserves the right to conduct interviews and/or to request that Proposers make presentations and/or demonstrations, as OPA deems applicable and appropriate. Although discussions may be conducted with Proposers submitting acceptable proposals, OPA reserves the right to award contracts on the basis of initial proposals received, without discussions; therefore, the Proposer’s initial proposal should contain its best technical and price terms.

B. Evaluation Criteria

- Demonstrated quantity and quality of successful relevant experience 40%
- Demonstrated level of organizational capability 20%
- Quality of Proposed Approach 40%

C. Basis for Contract Award

A contract will be awarded to the responsible Proposer whose proposal is determined to be the most advantageous to the City, taking into consideration the price and such other factors or criteria which are set forth in this RFP. Contract award shall be subject to the timely completion of contract negotiations between OPA and the selected Proposer. The contents of the selected proposal, together with this RFP and any addendum(s) provided during the proposal process, may be incorporated into the final contract to be developed by the Agency.

SECTION VI – GENERAL INFORMATION TO PROPOSERS

A. Non-Binding Acceptance of Proposals: This RFP does not commit the City to award a contract for any services. Further, the City may award one or several contracts for services in relation to this project.

B. Incurring Proposal Costs: The City of New York is not liable for any costs incurred in the preparation of a response to this RFP. If Proposers choose to participate in negotiations, they may be asked to submit such price, technical data, or other revisions to their proposals as may be required by the City.

C. Confidential, Proprietary or Trade Secrets: The contents of a Proposer's RFP response are not deemed confidential unless the Proposer identifies those portions of its response which it deems confidential, or containing proprietary information or trade secrets. The Proposer must provide justification as to why such materials, upon request, should not be disclosed by the City. Such information must be easily separable from the non-confidential sections of the proposal. All information not identified as confidential may be disclosed by the City.

D. Multi-Year Contracts: Multi-year contracts are subject to modification or cancellation if adequate funds are not appropriated to the Agency to support continuation of performance in any City fiscal year succeeding the first fiscal year and/or if the contractor's performance is not satisfactory. The Agency will notify the contractor as soon as is practicable that the funds are, or are not, available for the continuation of the multi-year contract for each succeeding City fiscal year. In the event of cancellation, the contractor will be reimbursed for those costs, if any, which are so provided for in the contract.

E. Reserved Rights: All proposal material submitted becomes the property of the City of New York and the City reserves the right, at its sole discretion, to:

1. Reject any and all proposals received in response to this RFP;

2. Award a contract to other than the lowest fee Proposer;
3. Waive, modify or correct any irregularities in proposals received, after notification to the Proposer;
4. Use without limitation any or all of the ideas from submitted proposals;
5. Act on all or selected parts of the Proposer's proposal, selecting from the services offered without affecting any itemized pricing;
6. Extend the time for submission of all proposals after notification to all prospective Proposers;
7. Conduct discussions with proposers submitting acceptable proposals; however, award may be made without any discussion;
8. Terminate negotiations with a selected Proposer and select the next most responsive and advantageous Proposer, or take such other action as deemed appropriate if negotiations fail to result in a signed contract within a reasonable time of the commencement of negotiations as determined by OPA's Executive Director or designee;
9. Postpone or cancel this RFP, in whole or in part, and reject all proposals.

F. Proposer Appeal Rights: Pursuant to New York City's Procurement Policy Board Rules, Proposers have the right to appeal Agency non-responsiveness determinations and Agency non-responsibility determinations and to protest an Agency's determination regarding the solicitation or award of a contract.

G. Prices Irrevocable: Prices proposed by the Proposer shall be irrevocable until contract award, unless the proposal is withdrawn. Proposals may only be withdrawn by submitting a written request to the Agency prior to contract award but after the expiration of 90 days after the opening of proposals. This shall not limit the discretion of the Agency to request Proposers to revise proposed prices through the submission of best and final offers and/or the conduct of negotiations.

H. Complaints and Comptroller Audit Rights: The New York City Comptroller is charged with the audit of contracts in New York City. Any proposer who believes that there has been unfairness, favoritism or impropriety in the proposal process should inform the Comptroller, Office of Contract Administration, 1 Centre Street, Room 1005, New York, NY 10007, telephone number (212) 669-4600. In addition, the New York City Department of Investigation should be informed of

such complaints at its Investigations Division, 80 Maiden Lane, New York, NY 10038.

I. Prompt Payment Policy: Pursuant to New York City's Procurement Policy Board Rules, it is the policy of the City to process contract payments efficiently and expeditiously.

J. General Contract Provisions: This RFP and the resulting contract award(s), if any, unless otherwise stated, are subject to all applicable provisions of New York State Law, the New York City Administrative Code, the New York City Charter, the New York City Procurement Policy Board (PPB) Rules and all of the City's standard contract provisions in substantially the same form in which they appear in Appendix A annexed to this RFP. A copy of the PPB Rules may be obtained by accessing the City's website at nyc.gov/ppb.

K. Contract Award: Contract award is subject to each of the following applicable conditions and any others that may apply: New York City MacBride Principles Law; submission by the Proposer of the requisite New York City Department of Business Services/Division of Labor Services Employment Report and certification by that office; submission of the requisite Vendex Questionnaires or Affidavits of No Change and review of the information contained therein by the New York City Department of Investigation; all other required oversight approvals; applicable provisions of federal, state and local laws and executive orders concerning affirmative action and equal employment opportunity.

L. Charter Section 312(a) Certification: [if applicable]

The Agency has determined that the contract(s) to be awarded through this Request for Proposals will not directly result in the displacement of any New York City employee.



Agency Chief Contracting Officer

11/21/08
Date

ATTACHMENT A

**PROPOSAL COVER LETTER
RFP TITLE: TRANSIT BENEFIT PROGRAM
PROJECT CODE #: 09131000042569**

PROPOSER:

NAME: _____

ADDRESS: _____

TAX IDENTIFICATION #: _____

PROPOSER'S CONTACT PERSON:

NAME: _____

TITLE: _____

TELEPHONE #: _____

EMAIL ADDRESS: _____

PROPOSER'S AUTHORIZED REPRESENTATIVE:

NAME: _____

TITLE: _____

EMAIL ADDRESS: _____

SIGNATURE: _____

DATE: _____

ATTACHMENT B PRICE PROPOSAL FORM

Mass Transit Product Type

Debit		Credit		Pay Per Ride MetroCard		Unlimited Ride MetroCard		Online Purchase/Mail Order		Other: Describe _____	
Fixed Fee Per Participant \$ _____		Fixed Fee Per Participant \$ _____		Fixed Fee Per Participant \$ _____		Fixed Fee Per Participant \$ _____		Fixed Fee Per Participant \$ _____		Fixed Fee Per Participant \$ _____	
Check All that Apply	*Additional Fee for Service (if any)	Check All that Apply	*Additional Fee for Service (if any)	Check All that Apply	*Additional Fee for Service (if any)	Check All that Apply	*Additional Fee for Service (if any)	Check All that Apply	*Additional Fee for Service (if any)	Check All that Apply	*Additional Fee for Service (if any)
Mass Transit Covered Services											
New York City Transit Subways and Local Buses											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
New York City Transit Express Buses											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
MetroNorth											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
LIRR											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
PATH											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
NJ Transit (Buses + Rails)											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Other Regional Railroads											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	

(Specify: Services)

New York Water Taxi											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Other Regional Ferries/Water Taxis											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	

(Specify: Services)

Long Island Bus											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Other Regional Buses											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	

(Specify: Services)

MTA Access-A-Ride											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Other Paratransit for the Disabled											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	

(Specify: Services)

Commuter van Services											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Qualified Parking											
<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	

(Specify: Services)

FOR EACH PRODUCT THE PROPOSER INTENDS TO PROVIDE, INDICATE THE FEE PER PARTICIPANT EVEN IF THE FEES ARE THE SAME FOR EACH PRODUCT. FOR EACH PRODUCT THE PROPOSER WILL NOT PROVIDE, "N/A" SHOULD BE INDICATED AS THE FIXED FEE.

*** If there are any additional fees per participant in excess of the fixed fee per participant for any particular covered service, indicate such fees in the corresponding columns.**

OTHER NON-RECURRING FEES: _____

Describe: _____

(Attach additional sheets if necessary)

ATTACHMENT B PRICE PROPOSAL FORM

IF THE FEE PER PARTICIPANT WILL VARY BASED ON THE VOLUME OF ENROLEES, PLEASE INDICATE FEES PER PARTICIPANT BASED ON ESTIMATED ENROLLMENT VOLUME AS INDICATED BELOW. IF THE FEE WILL NOT VARY, "N/A" SHOULD BE INDICATED IN ALL SPACES.

	Fee Per Participant Based On Enrollment Volume (Number of Participants)			
	<u>0 - 25,000</u>	<u>25,001 - 75,000</u>	<u>75,000 - 125,000</u>	<u>125,000 +</u>
<u>Mass Transit Product</u>				
Pay Per Ride MetroCard	_____	_____	_____	_____
Unlimited Ride MetroCard	_____	_____	_____	_____
<hr/>				
(Specify: Annual, Monthly Semi-Monthly, etc.)				
Debit Card	_____	_____	_____	_____
Credit Card	_____	_____	_____	_____
Online Purchase/Mail Order	_____	_____	_____	_____
Other	_____	_____	_____	_____
<hr/>				
(Describe)				

<u>Mass Transit Covered Services</u>				
New York City Transit Subways & Local Buses	_____	_____	_____	_____
New York City Transit Express Buses	_____	_____	_____	_____
MetroNorth	_____	_____	_____	_____
LIRR	_____	_____	_____	_____
PATH	_____	_____	_____	_____
NJ Transit (Buses + Rails)	_____	_____	_____	_____
Other Regional Railroads	_____	_____	_____	_____
<hr/>				
(Specify: Services)				
New York Water Taxi	_____	_____	_____	_____
Other Regional Ferries/Water Taxis	_____	_____	_____	_____
<hr/>				
(Specify: Services)				
Long Island Bus	_____	_____	_____	_____
Other Regional Buses	_____	_____	_____	_____
<hr/>				
(Specify: Services)				
MTA Access-A-Ride	_____	_____	_____	_____
Other Paratransit for the Disabled	_____	_____	_____	_____
<hr/>				
(Specify: Services)				
Commuter Van Services	_____	_____	_____	_____
Qualified Parking	_____	_____	_____	_____
<hr/>				
(Specify: Services)				

PRINT NAME: _____
 AUTHORIZED SIGNATURE: _____
 DATE: _____

ATTACHMENT C

ACKNOWLEDGEMENT OF ADDENDA

<u>RFP TITLE</u> TRANSIT BENEFIT RFP	<u>PIN #</u> 09131000042569
------------------------------------------------	---------------------------------------

DIRECTION: COMPLETE PART I, OR PART II, WHICH EVER IS APPLICABLE

PART I: LISTED BELOW ARE THE DATES OF ISSUE FOR EACH ADDENDUM RECEIVED IN CONNECTION WITH THIS RFP.

ADDENDUM #1, DATED _____, 20_____

ADDENDUM #2, DATED _____, 20_____

ADDENDUM #3, DATED _____, 20_____

ADDENDUM #4, DATED _____, 20_____

ADDENDUM #5, DATED _____, 20_____

ADDENDUM #6, DATED _____, 20_____

ADDENDUM #7, DATED _____, 20_____

ADDENDUM #8, DATED _____, 20_____

ADDENDUM #9, DATED _____, 20_____

PART II:

_____ NO ADDENDUM WAS RECEIVED IN CONNECTION WITH THIS RFP

PROPOSER (NAME) _____ DATE ____ / ____ / ____

PROPOSER (SIGNATURE) _____

ATTACHMENT D

TAX AFFIRMATION FORM

The undersigned proposer or bidder affirms and declares that said proposer or bidder is not in arrears to the City of New York upon dept, contract or taxes and is not a defaulter, as surety or otherwise, upon obligation to the City of New York, and has not been declared not responsible, or disqualified by any agency of the City of New York, nor is there any proceeding pending relating to the responsibility or qualification of the proposer or bidder to receive public contracts except

Full name of Proposer or Bidder _____

Address _____

City _____ State _____ Zip Code _____

CHECK ONE BOX AND INCLUDE APPROPRIATE NUMBER:

- A - Individual or Sole Proprietorship
SOCIAL SECURITY NUMBER

- B - Partnership, Joint Venture or other unincorporated organization
EMPLOYER IDENTIFICATION NUMBER

- C - Corporation
EMPLOYER IDENTIFICATION NUMBER

By _____
Signature

Title

If a corporation place seal here

Must be signed by an officer or duly authorized representative.

ATTACHMENT E

VENDEX INFORMATION

NOTICE TO CITY VENDORS - VENDEX PROCEDURES

GENERAL INFORMATION

In an effort to streamline the operation of VENDEX, the Mayor's Office of Contract Services has made some significant changes in the processing of VENDEX forms.

- ◆ There are only two Questionnaires; the **Vendor Questionnaire** and the **Principal Questionnaire**.
- ◆ Questionnaires are submitted directly to MOCS; Questionnaires will no longer go directly to the agencies.
- ◆ Questionnaires are valid for three years from the date of the certifications.
- ◆ The new forms are available on line at www.nyc.gov/vendex

CERTIFICATIONS OF NO CHANGE

- ◆ Affidavits of no change are no longer accepted. Instead vendors are required to complete under penalty of perjury, a Certification of No Change which states that the information contained in the most recent VENDEX submission/ changed questionnaire is current and accurate, Unlike affidavits of no change, principals are not required to submit individual Certifications of No Change.
- ◆ The vendor must execute **TWO ORIGINAL** Certifications of No Change and return them to the agency.
- ◆ If the vendor has a parent or controlling entity that is required to submit VENDEX Questionnaires, the parent or controlling entity must also execute 2 original Certifications of No Change. **The Certification of No Change that is executed on behalf of the vendor will not be sufficient to cover the parent or the controlling entity of the vendor.**
- ◆ It is recommended that either the individual who signs the contract on behalf of the vendor, or one of the principal officers executes the Certifications of No Change on behalf of the vendor.

**HOW TO DETERMINE WHETHER YOU NEED TO FILE NEW FORMS/
MAKE CHANGES/ CERTIFY THAT THERE ARE NO CHANGES**

- ◆ If the vendor has never completed VENDEX questionnaires, or has not made a complete VENDEX submission in the last 2 1/2 years, the vendor should complete the new forms and return them directly to MOCS, Mayor's Office of Contract Services, VENDEX UNIT, 253 Broadway, 9th Floor, New York, NY 10007. In order to inform the agency that the Questionnaires were sent to MOCS the vendor must complete the **submitted VENDEX memorandum** and return it to the agency. The submitted VENDEX memorandum can also be found on www.nyc.gov/vendex.
- ◆ If the vendor has made a complete VENDEX submission in the last 2 1/2 years and there have been no changes in information requiring an update of the forms, the vendor should execute a Certification of No Change. Certifications should be included as part of the vendor's response to bids, solicitations or RFP's.
- ◆ If the vendor has made a complete VENDEX submission in the last 2 1/2 years and there have been changes in information requiring an update of the forms, the vendor is required to submit full questionnaires using the new forms. **MOCS will not be able to process changed questionnaires using the new forms if they are attempting to update old forms.** The vendor should inform the agency that changed questionnaires were sent to MOCS by returning the **submitted VENDEX memorandum** to the agency as part of their response.
- ◆ A changed questionnaire consists of the first page of the questionnaire with a check in the box marked "changed questionnaire," the relevant changed pages, any additional pertinent information and a signed certification page.



Doing Business Data Form

To be completed by the City Agency prior to distribution			
Agency: 131 (OPA)		Transaction ID: TRANSITBENEFIT RFP (09131000042569)	
Check One:	Transaction Type (check one):		
<input checked="" type="checkbox"/> Proposal	<input type="checkbox"/> Concession	<input checked="" type="checkbox"/> Contract	<input type="checkbox"/> Economic Development Agreement
<input type="checkbox"/> Award	<input type="checkbox"/> Franchise	<input type="checkbox"/> Grant	<input type="checkbox"/> Pension Investment Contract

Any entity receiving, applying for or proposing on an award or agreement must complete a Doing Business Data Form (see Q&A sheet for more information). Please either type responses directly into this fillable form or print answers by hand in black ink, and be sure to fill out the certification box on the last page. **Submission of a complete and accurate form is required for a proposal to be considered responsive or for any entity to receive an award or enter into an agreement.**

This Data Form requires information to be provided on principal officers, owners and senior managers. The name, employer and title of each person identified on the Data Form will be included in a public database of people who do business with the City of New York; no other information reported on this form will be disclosed to the public. **This Data Form is not related to the City's VENDEX requirements.**

Please return the completed Data Form to the City Agency that supplied it. Please contact the Doing Business Accountability Project at DoingBusiness@cityhall.nyc.gov or 212-788-8104 with any questions regarding this Data Form. Thank you for your cooperation.

Section 1: Entity Information

Entity Name: _____

Entity EIN/TIN: _____

<p>Entity Filing Status (select one):</p> <p><input type="checkbox"/> Entity has never completed a Doing Business Data Form. <i>Fill out the entire form.</i></p> <p><input type="checkbox"/> Change from previous Data Form dated _____. <i>Fill out only those sections that have changed, and indicate the name of the persons who no longer hold positions with the entity.</i></p> <p><input type="checkbox"/> No Change from previous Data Form dated _____. <i>Skip to the bottom of the last page.</i></p>

Entity is a Non-Profit: Yes No

Entity Type: Corporation (any type) Joint Venture LLC Partnership (any type)
 Sole Proprietor Other (specify): _____

Address: _____

City: _____ State: _____ Zip: _____

Phone : _____ Fax : _____

E-mail: _____

Provide your e-mail address and/or fax number in order to receive notices regarding this form by e-mail or fax.

Section 2: Principal Officers

Please fill in the required identification information for each officer listed below. If the entity has no such officer or its equivalent, please check "This position does not exist." If the entity is filing a Change Form and the person listed is replacing someone who was previously disclosed, please check "This person replaced..." and fill in the name of the person being replaced so his/her name can be removed from the *Doing Business Database*, and indicate the date that the change became effective.

Chief Executive Officer (CEO) or equivalent officer This position does not exist

The highest ranking officer or manager, such as the President, Executive Director, Sole Proprietor or Chairperson of the Board.

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

 This person replaced former CEO: _____ on date: _____**Chief Financial Officer (CFO) or equivalent officer** This position does not exist

The highest ranking financial officer, such as the Treasurer, Comptroller, Financial Director or VP for Finance.

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

 This person replaced former CFO: _____ on date: _____**Chief Operating Officer (COO) or equivalent officer** This position does not exist

The highest ranking operational officer, such as the Chief Planning Officer, Director of Operations or VP for Operations.

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

 This person replaced former COO: _____ on date: _____

Section 3: Principal Owners

Please fill in the required identification information for all individuals who, through stock shares, partnership agreements or other means, own or control 10% or more of the entity. If no individual owners exist, please check the appropriate box to indicate why and skip to the next page. If the entity is owned by other companies, those companies do not need to be listed. If an owner was identified on the previous page, fill in his/her name and write "See above." If the entity is filing a Change Form, list any individuals who are no longer owners at the bottom of this page. If more space is needed, attach additional pages labeled "Additional Owners."

There are no owners listed because (select one):

- The entity is not-for-profit There are no individual owners No individual owner holds 10% or more shares in the entity
 Other (explain): _____

Principal Owners (who own or control 10% or more of the entity):

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

Remove the following previously-reported Principal Owners:

Name: _____ Removal Date: _____

Name: _____ Removal Date: _____

Name: _____ Removal Date: _____

Section 4: Senior Managers

Please fill in the required identification information for all senior managers who oversee any of the entity's relevant transactions with the City (e.g., contract managers if this form is for a contract award/proposal, grant managers if for a grant, etc.). Senior managers include anyone who, either by title or duties, has substantial discretion and high-level oversight regarding the solicitation, letting or administration of any transaction with the City. **At least one senior manager must be listed, or the Data Form will be considered incomplete.** If a senior manager has been identified on a previous page, fill in his/her name and write "See above." If the entity is filing a Change Form, list individuals who are no longer senior managers at the bottom of this section. If more space is needed, attach additional pages labeled "Additional Senior Managers."

Senior Managers:

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

First Name: _____ MI: _____ Last: _____

Office Title: _____

Employer (if not employed by entity): _____

Birth Date (mm/dd/yy): _____ Home Phone #: _____

Home Address: _____

Remove the following previously-reported Senior Managers:

Name: _____ Removal Date: _____

Name: _____ Removal Date: _____

Certification

I certify that the information submitted on these four pages and _____ additional pages is accurate and complete. I understand that willful or fraudulent submission of a materially false statement may result in the entity being found non-responsible and therefore denied future City awards.

Name: _____

Signature: _____ Date: _____

Entity Name: _____

Title: _____ Work Phone #: _____

Return the completed Data Form to the agency that supplied it.

For information or assistance, call the Doing Business Accountability Project at 212-788-8104.



DOING BUSINESS ACCOUNTABILITY PROJECT
QUESTIONS AND ANSWERS ABOUT THE DOING BUSINESS DATA FORM

What is the purpose of this *Data Form*?

To collect accurate, up-to-date identification information about entities that have business dealings with the City of New York in order to comply with Local Law 34 of 2007 (LL 34), the recently passed campaign finance reform law. LL 34 limits municipal campaign contributions from principal officers, owners and senior managers of these entities and mandates the creation of a *Doing Business Database* to allow the City to enforce the law. The information requested in this *Data Form* must be provided, regardless of whether the entity or the people associated with it make or intend to make campaign contributions. No sensitive personal information collected will be disclosed to the public.

Why have I received this *Data Form*?

The contract, franchise, concession, grant or economic development agreement you are proposing on, applying for or have already been awarded is considered a business dealing with the City under LL 34. No proposal or application will be considered and no award will be made unless this *Data Form* is completed. Most transactions valued at more than \$5,000 are considered business dealings and require completion of the *Data Form*. Exceptions include transactions awarded on an emergency basis or by publicly advertised, non-pre-qualified competitive sealed bid. Other types of transactions that are considered business dealings include real property and land use actions with the City.

What entities will be included in the *Doing Business Database*?

Entities that hold \$100,000 or more in grants, contracts for goods or services, franchises or concessions (\$500,000 or more for construction contracts), along with entities that hold any economic development agreements or pension fund investment contracts, are considered to be doing business with the City for the purposes of LL 34 and will be included in the *Doing Business Database*. Because all of the business that an entity does or proposes to do with the City will be added together, the *Data Form* must be completed for all covered transactions even if an entity does not currently do enough business with the City to be listed in the *Database*.

What individuals will be included in the *Doing Business Database*?

The principal officers, owners and certain senior managers of entities listed in the *Doing Business Database* are themselves considered to be doing business with the City and will also be included in the *Database*.

- **Principal Officers** are the Chief Executive Officer (CEO), Chief Financial Officer (CFO) and Chief Operating Officer (COO), or their functional equivalents. See the *Data Form* for examples of titles that apply.
- **Principal Owners** are individuals who own or control 10% or more of the entity. This includes stockholders, partners and anyone else with an ownership or controlling interest in the entity.
- **Senior Managers** include anyone who, either by job title or actual duties, has substantial discretion and high-level oversight regarding the solicitation, letting or administration of any contract, concession, franchise, grant or economic development agreement with the City. At least one Senior Manager must be listed or the *Data Form* will be considered incomplete.

I provided some of this information on the VENDEX Questionnaire; do I have to provide it again?

Although the *Doing Business Data Form* and the VENDEX Questionnaire request some of the same information, they serve entirely different purposes. In addition, the *Data Form* requests information concerning senior managers, which is not part of the VENDEX Questionnaire.

My organization is proposing on a contract with another firm as a Joint Venture that does not exist yet; how should the *Data Form* be completed?

A joint venture that does not yet exist must submit *Data Forms* from each of its component firms. If the joint venture receives the award, it must then complete a form in the name of the joint venture.



Will the information on this *Data Form* be available to the public?

The names and titles of the officers, owners and senior managers reported on the *Data Form* will be made available to the public, as will information about the entity itself. However, personal identifying information, such as home address, home phone and date of birth, will not be disclosed to the public, and home address and phone number information will not be used for communication purposes.

No one in my organization plans to contribute to a candidate; do I have to fill out this *Data Form*?

Yes. All entities are required to return this *Data Form* with complete and accurate information, regardless of the history or intention of the entity or its officers, owners or senior managers to make campaign contributions. The *Doing Business Database* must be complete so that the Campaign Finance Board can verify whether future contributions are in compliance with the law.

I have already completed a *Doing Business Data Form*; do I have to submit another one?

Yes. An entity is required to submit a *Doing Business Data Form* each time it proposes on or enters a transaction considered business dealings with the City. However, the *Data Form* has both a No Change option, which only requires an entity to report its EIN and sign the last page, and a Change option, which allows an entity to only fill in applicable information that has changed since the previous completion of the *Data Form*. No entity should have to fill out the entire *Data Form* more than once.

How does a person remove him/herself from the *Doing Business Database*?

Any person who believes that s/he should not be listed may apply for removal from the *Database* by submitting a Request for Removal. Reasons that a person would be removed include his/her no longer being the principal officer, owner or senior manager of the entity, or the entity no longer being in business. Entities may also update their database information by submitting an update form. Both of these forms are available online at www.nyc.gov/mocs (once there, click MOCS Programs) or by calling 212-788-8104.

How long will an entity and its officers, owners and senior managers remain listed on the *Doing Business Database*?

- **Contract, Concession and Economic Development Agreement holders:** generally for the term of the transaction, plus one year.
- **Franchise and Grant holders:** from the commencement or renewal of the transaction, plus one year.
- **Pension investment contracts:** from the time of presentation on an investment opportunity or the submission of a proposal, whichever is earlier, until the end of the contract, plus one year.
- **Line item and discretionary appropriations:** from the date of budget adoption until the end of the contract, plus one year.
- **Contract proposers:** for one year from the proposal date or date of public advertisement of the solicitation, whichever is later.
- **Franchise and Concession proposers:** for one year from the proposal submission date.

For information on other transaction types, contact the Doing Business Accountability Project.

What are the new campaign contribution limits for people doing business with the City?

Contributions to City Council candidates are limited to \$250 per election cycle; \$320 to Borough President candidates; and \$400 to candidates for citywide office. Please contact the NYC Campaign Finance Board for more information at www.nycctfb.info, or 212-306-7100.

The *Data Form* is to be returned to the contracting agency.

If you have any questions about the *Data Form* please contact the Doing Business Accountability Project at 212-788-8104 or DoingBusiness@cityhall.nyc.gov.

ATTACHMENT G

SUPPLY AND SERVICE EMPLOYMENT REPORT

WHO MUST FILE A SUPPLY AND SERVICES EMPLOYMENT REPORT

An S&S Employment Report (ER) must be filed if you meet the following conditions:

CONTRACTOR	CONTRACT VALUE	COMPANY SIZE	SUBMISSION REQUIREMENT
Prime and subcontractors	\$100,00 or greater	50 or more Employees	S&S Employment Report
		Less than 50 Employees	Less than 50 Employees Waiver

- ◆ A separate ER must be submitted for each facility involved in the performance of the contract. This may be headquarters or any "independently operating facility". An "**independently operating facility**" is headquarters or a site separate from headquarters that makes its own personnel decisions including hires, transfers, promotions and terminations. If the staff employed by a facility is simply sent to a separate location to perform their work, they are still considered part of that facility and are included in one ER.

Example for which ERs must be filed from separate facilities: If your firm is supplying data processing equipment that is manufactured at your Chicago, Illinois plant, sold by your sales office in East Orange, New Jersey and serviced by your maintenance center in New York City, then an ER is necessary for each of the three sites. DLS retains the right to request the submission of an ER from headquarters, if deemed appropriate.

- ◆ If your contract value exceeds \$100,000 and your company at all of its facilities employs fewer than 50 employees, you need only submit a "Less than 50 Employees" waiver.
- ◆ It is the responsibility of the contractor to promptly inform all proposed subcontractors that each subcontract must comply with the equal employment opportunity requirements of E.O. 50 and the implementing Rules. Each covered subcontractor must submit a completed Employment Report, or a "Less than 50" waiver, for each of its operating facilities to the contracting agency before the fifth day following the award date (Comptroller's Office Registration Date) of the contract. DLS will review the subcontractor's Employment Report(s) for compliance.

WHERE TO FILE

Employment Reports must be filed with the City agency awarding the contract. If you are contracted through the Department of General Services/Division of Municipal Supplies, submit the ER directly to DLS.

DLS' REVIEW PROCESS

In accordance with Executive Order 50 (EO 50), upon receipt by DLS of a completed ER, DLS conducts a review of the contractor's current employment policies, practices and procedures, as well as perform a statistical analysis of the contractor's workforce, if necessary. The process is as follows:

1. Within five (5) business days, DLS will review the ER for completeness and accuracy. If any information is omitted or incorrect, or if necessary documents are not submitted, the submission shall be deemed incomplete and DLS will inform the contractor. The substantive compliance review does not commence until the submission is complete. **An incomplete submission will delay the review process and may preclude or interrupt the contract approval.**
2. If the ER submission is complete, the compliance review will proceed, resulting in one of the following:

Certificate of Approval

The contractor is found to be in compliance with all applicable laws and regulations. The approval is valid for 24 months.

Continued Approval Certificate

The contractor has been issued a Certificate of Approval in the previous 24 months which is good for the applicable contract.

An Administrative Certificate of Compliance

Issued when the contractor has been audited by the United States Department of Labor, Office of Federal Contract Compliance Programs (OFCCP) and is valid for 24 months.

Conditional Certificate of Compliance

The contractor is required to take corrective actions in order to be in compliance with EO 50. The Contractor must meet the conditions within three months of the issue of the Conditional Certificate.

Determination of Nonperformance

The contractor has failed to take the required corrective actions stipulated in the Conditional Certificate. A determination of nonperformance may prevent a contractor from receiving an award of a contract.

EXHIBIT 1

LIST OF SUBCONTRACTORS

PRIME CONTRACTOR:

NAME: _____

ADDRESS: _____

TAX IDENTIFICATION #: _____

CONTACT: _____

TELEPHONE: _____ EMAIL: _____

SUBCONTRACTOR:

NAME: _____

ADDRESS: _____

TAX IDENTIFICATION #: _____

CONTACT: _____

TELEPHONE: _____ EMAIL: _____

SUBCONTRACT AMOUNT: \$ _____

TYPE OF SERVICES TO BE PERFORMED: _____

NOTE: If the subcontract amount is greater than \$100,000.00, the Subcontractor(s) must comply with the same requirements as the Prime Contractor.

APPENDIX A

GENERAL PROVISIONS GOVERNING CONTRACTS FOR CONSULTANT, PROFESSIONAL, AND TECHNICAL SERVICES

ARTICLE 1. DEFINITIONS

As used throughout this Agreement, the following terms shall have the meaning set forth below:

- a. "City" shall mean the City of New York, its departments and political subdivisions.
- b. "Comptroller" shall mean the Comptroller of the City of New York.
- c. "Department" shall mean the Office of Payroll Administration.
- d. "Commissioner" or "Administrator" shall mean the Executive Director, OPA or his or her duly authorized representative. The term "duly authorized representative" shall include any person or persons acting within the limits of his or her authority.
- e. "Law" or "Laws" shall include but not be limited to the New York City Charter, the New York City Administrative Code, a local law of the City of New York, and any ordinance, rule or regulation having the force of law.

ARTICLE 2. REPRESENTATIONS AND WARRANTIES

2.1 PROCUREMENT OF AGREEMENT

- A. The Contractor represents and warrants that no person or selling agency has been employed or retained to solicit or secure this Agreement upon an agreement or understanding for a commission, percentage, brokerage fee, contingent fee or any other compensation. The Contractor further represents and warrants that no payment, gift or thing of value has been made, given or promised to obtain this or any other agreement between the parties. The Contractor makes such representations and warranties to induce the City to enter into this Agreement and the City relies upon such representations and warranties in the execution hereof.
- B. For a breach or violation of such representations or warranties, the Administrator shall have the right to annul this Agreement without liability, entitling the City to recover all monies paid hereunder and the Contractor shall not make claim for, or be entitled to recover, any

sum or sums due under this Agreement. This remedy, if effected, shall not constitute the sole remedy afforded the City for the falsity or breach, nor shall it constitute a waiver of the City's right to claim damages or refuse payment or to take any other action provided for by law or pursuant to this Agreement.

2.2 CONFLICT OF INTEREST

The contractor represents and warrants that neither it nor any of its directors, officers, members, partners or employees, has any interest nor shall they acquire any interest, directly or indirectly, which would or may conflict in any manner or degree with the performance or rendering of the services herein provided. The Contractor further represents and warrants that in the performance of this Agreement no person having such interest or possible interest shall be employed by it. No elected official or other officer or employee of the City or Department, nor any person whose salary is payable, in whole or in part, from the City Treasury, shall participate in any decision relating to this Agreement which affects his personal interest or the interest of any corporation, partnership or association in which he is directly or indirectly, interested; nor shall any such person have any interest, direct or indirect, in this Agreement or in the proceeds thereof.

2.3 FAIR PRACTICES

The Contractor and each person signing on behalf of any contractor represents and warrants and certifies, under penalty of perjury, that to the best of its knowledge and belief:

- A. The prices in this contract have been arrived at independently without collusion, consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with any other bidder or with any competitor;
- B. Unless otherwise required by law, the prices which have been quoted in this contract and on the proposal submitted by the Contractor have not been knowingly disclosed by the Contractor prior to the proposal opening, directly or indirectly, to any other bidder or to any competitor; and
- C. No attempt has been made or will be made by the Contractor to induce any other person, partnership or corporation to submit or not to submit a proposal for the purpose of restricting competition.

The fact that the Contractor (a) has published price lists, rates, or tariffs covering items being procured, (b) has informed prospective customers of proposed or pending publication of new or revised price lists for such items, or (c) has sold the same items to other customers at the same prices being bid, does not constitute, without more, a disclosure within the meaning of

the above.

ARTICLE 3. AUDIT BY THE DEPARTMENT AND THE CITY

- 3.1 All vouchers or invoices presented for payment to be made hereunder, and the books, records and accounts upon which said vouchers or invoices are based are subject to audit by the Department and by the Comptroller of the City of New York pursuant to the powers and responsibilities as conferred upon said Department and said Comptroller by the New York City Charter and Administrative Code of the City of New York, as well as all orders and regulations promulgated pursuant thereto.
- 3.2 The Contractor shall submit any and all documentation and justification in support of expenditures or fees under this Agreement as may be required by said Department and said Comptroller so that they may evaluate the reasonableness of the charges and shall make its records available to the Department and to the Comptroller as they consider necessary.
- 3.3 All books, vouchers, records, reports, canceled checks and any and all similar material may be subject to periodic inspection, review and audit by the State of New York, Federal Government and other persons duly authorized by the City. Such audit may include examination and review of the source and application of all funds whether from the City, any State, the Federal Government, private sources or otherwise.
- 3.4 The Contractor shall not be entitled to final payment under the Agreement until all requirements have been satisfactorily met.

ARTICLE 4. COVENANTS OF THE CONTRACTOR

4.1 EMPLOYEES

- A. All experts or consultants or employees of the Contractor who are employed by the Contractor to perform work under this contract are neither employees of the City nor under contract to the City and the Contractor alone is responsible for their work, direction, compensation and personal conduct while engaged under this Agreement. Nothing in this contract shall impose any liability or duty on the City for the acts, omission, liabilities or obligations of the Contractor any person, firm, company, agency, association, expert, consultant, independent contractor, specialist, trainee, employee, servant, or agent, or for taxes of any nature including but not limited to unemployment insurance, workmen's compensation, disability benefits and social security, or, except as specifically stated in this contract, to any person, firm or corporation.

B. The Contractor shall be solely responsible for all physical injuries or death to its agents, servants, or employees or to any other person or damage to any property sustained during its operations and work on the project under this Agreement resulting from any act of omission or commission or error in judgment of any of its officers, trustees, employees, agents, servants, or independent contractors, and shall hold harmless and indemnify the City from liability upon any and all claims for damages on account of such injuries or death to any such person or damages to property on account of any neglect, fault or default of the Contractor, its officers, trustees, employees, agents, servants, or independent contractors. The Contractor shall be solely responsible for the safety and protection of all of its employees whether due to the negligence, fault or default of the Contractor or not.

C. **Workers Compensation and Disability Benefits**

If this Agreement be of such a character that the employees engaged thereon are required to be insured by the provision of Chapter 615 of the Laws of 1922, known as the "Workers' Compensation Law" and acts amendatory thereto, the Agreement shall be void and of no effect unless the Contractor shall secure compensation for the benefit of, and keep insured during the life of this Agreement such employees in compliance with the provisions of said law, inclusive of Disability Benefits; and, shall furnish the Department with two (2) certificates of these insurance coverages.

D. **Unemployment Insurance**

Unemployment Insurance coverage shall be obtained and provided by the Contractor for its employees.

E. **Minimum Wage**

Except for those employees whose minimum wage is required to be fixed pursuant to Section 220 of the Labor Law of the State of New York, all persons employed by the Contractor in the performance of this Agreement shall be paid, without subsequent deduction or rebate, unless expressly authorized by law, not less than the minimum wage as prescribed by law. Any breach or violation of the foregoing shall be deemed a breach or violation of a material provision of this Agreement.

4.2 **INDEPENDENT CONTRACTOR STATUS**

The Contractor and the Department agree that the Contractor is an independent contractor or and not an employee of the Department or the City of New York, and that in accordance with such status as independent contractor, the Contractor covenants and agrees that neither

it nor its employees or agents will hold themselves out as, nor claim to be, officers or employees of the City of New York, or of any department, agency or unit thereof, by reason hereof, and that they will not, by reason hereof, make any claim, demand or application to or for any right or privilege applicable to an officer or employee of the City of New York, including, but not limited to, Workmen's Compensation coverage, Unemployment Insurance Benefits, Social Security coverage or employee retirement membership or credit.

4.3 INSURANCE

- A. The Contractor shall carry paid up insurance in the sum of not less than One Million (1,000,000) Dollars per occurrence to protect the Department and the City of New York against any and all claims, loss or damage, whether in contract or tort, including claims for injuries to, or death of persons, or damage to property, whether such injuries, death or damages be attributable to the negligence or any other acts of the Contractor or its employees or otherwise. Such policy or policies of insurance, shall be obtained from a company, or companies that may lawfully issue the required policy and have an A.M. Best rating of at least A-7 or a Standard and Poor's rating of at least AA, unless prior written approval is obtained from the Mayor's Office of Operations. Such policy or policies of insurance shall name the Department and the City of New York as additional parties insured thereunder, and shall provide that in the event of cancellation thereof the Department shall be notified at least fifteen (15) days in advance thereof. Two (2) certificates of insurance shall be delivered to the Department for approval as to form prior to the effective date of this contract.

- B. In the event that any claim is made or any action is brought against the City arising out of negligent or careless acts of an employee of the Contractor, either within or without the scope of his employment or arising out of Contractor's negligent performance of this Agreement, then the City shall have the right to withhold further payments hereunder for the purpose of set off in sufficient sums to cover the said claim or action. The rights and remedies of the City provided for in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or this Agreement.

4.4 PROTECTION OF CITY PROPERTY

- A. The Contractor assumes the risk of, and shall be responsible for, any loss or damage to City property, including property and equipment leased by the City, used in the performance of this Agreement; and caused, either directly or indirectly by the acts, conduct, omissions or lack of good faith of the Contractor, its officers, managerial personnel and employees, or any person, firm, company, agent or others engaged by the Contractor as expert, consultant, specialist or subcontractor hereunder.

- B. In the event that any such City property is lost or damaged, except for normal wear and tear, then the City shall have the right to withhold further payments hereunder for the purpose of set-off, in sufficient sums to cover such loss or damage.
- C. The Contractor agrees to indemnify the City and hold it harmless from any and all liability or claim for damages due to any such loss or damage to any such City property described in subsection A above.
- D. The rights and remedies of the City provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law or by this Agreement.

4.5 CONFIDENTIALITY

All of the reports, information or data, furnished to or prepared, assembled or used by the Contractor under this Agreement are to be held confidential and prior to publication, the Contractor agrees that the same shall not be made available to any individual or organization without the prior written approval of the Department.

4.6 BOOKS AND RECORDS

The Contractor agrees to maintain separate and accurate books, records, documents and other evidence and accounting procedures and practices which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Agreement.

4.7 RETENTION OF RECORDS

The Contractor agrees to retain all books, records, and other documents relevant to this Agreement for six years after the final payment or termination of this Agreement, whichever is later. City, State and Federal auditors and any other persons duly authorized by the Department shall have full access to and the right to examine any of said materials during said period.

4.8 COMPLIANCE WITH LAW

Contractor shall render all services under this Agreement in accordance with the applicable provisions of federal, state and local laws, rules and regulations as are in effect at the time such services are rendered.

4.9 INVESTIGATION CLAUSE

A. The parties to this Agreement to cooperate fully and faithfully with any investigation, audit or inquiry conducted by a State of New York (State) or City of New York (City) governmental agency or authority that is empowered directly or by designation to compel the attendance of witnesses and to examine witnesses under oath, or conducted by the Inspector General of a governmental agency that is a party in interest to the transaction, submitted bid, submitted proposal, contract, lease, permit, or license that is the subject of the investigation, audit or inquiry.

B. If any person who has been advised that his or her statement, and any information from such statement, will not be used against him or her in any subsequent criminal proceeding refuses to testify before a grand jury or other governmental agency or authority empowered directly or by designation to compel the attendance of witnesses and to examine witnesses under oath concerning the award of or performance under any transaction, agreement, lease, permit, contract, or license entered into with the City, the State, or any political subdivision or public authority thereof, or the Port Authority of New York and New Jersey, or any local development corporation within the City, or any public benefit corporation organized under the laws of the State of New York, or;

If any person refuses to testify for a reason other than the assertion of his or her privilege against self-incrimination in an investigation, audit or inquiry conducted by a City or State governmental agency or authority empowered directly or by designation to compel the attendance of witnesses and to take testimony under oath, or by the Inspector General of the governmental agency that is a party in interest in, and is seeking testimony concerning the award of, or performance under, any transaction, agreement, lease, permit, contract, or license entered into with the City, the State, or any political subdivision thereof or any local development corporation within the City, then;

The commissioner or agency head whose agency is a party in interest to the transaction, submitted bid, submitted proposal, contract, lease, permit, or license shall convene a hearing, upon not less than five (5) days written notice to the parties involved to determine if any penalties should attach for the failure of a person to testify.

C. If any non-governmental party to the hearing requests an adjournment, the commissioner or agency head who convened the hearing may, upon granting the adjournment, suspend any contract, lease, permit, or license pending the final determination pursuant to paragraph 5 below without the City incurring any penalty or damages for delay or otherwise.

D. The penalties which may attach after a final determination by the commissioner or agency head may include but shall not exceed:

(a) The disqualification for a period not to exceed five (5) years from the date of an adverse determination for any person, or any entity of which such person was a member at the time the testimony was sought, from submitting bids for, or transacting business with, or entering into or obtaining any contract, lease, permit or license with or from the City; and/or

(b) The cancellation or termination of any and all such existing City contracts, leases, permits or licenses that the refusal to testify concerns and that have not been assigned as permitted under this Agreement, nor the proceeds of which pledged, to an unaffiliated and unrelated institutional lender for fair value prior to the issuance of the notice scheduling the hearing, without the City incurring any penalty or damages on account of such cancellation or termination; monies lawfully due for goods delivered, work done, rentals, or fees accrued prior to the cancellation or termination shall be paid by the City.

5. The commissioner or agency head shall consider and address in reaching his or her determination and in assessing an appropriate penalty the factors in paragraphs (a) and (b) below. He or she may also consider, if relevant and appropriate, the criteria established in paragraphs (c) and (d) below in addition to any other information which may be relevant and appropriate:

(a) The party's good faith endeavors or lack thereof to cooperate fully and faithfully with any governmental investigation or audit, including but not limited to the discipline, discharge, or disassociation of any person failing to testify, the production of accurate and complete books and records, and the forthcoming testimony of all other members, agents, assignees or fiduciaries whose testimony is sought.

(b) The relationship of the person who refused to testify to any entity that is a party to the hearing, including, but not limited to, whether the person whose testimony is sought has an ownership interest in the entity and/or the degree of authority and responsibility the person has within the entity.

(c) The nexus of the testimony sought to the subject entity and its contracts, leases, permits or licenses with the City.

(d) The effect a penalty may have on an unaffiliated and unrelated party or entity that has a significant interest in an entity subject to penalties under 4 above, provided that the party or entity has given actual notice to the commissioner or agency head upon the acquisition of the interest, or at the hearing called for in 3(a) above gives notice and proves that such interest was previously acquired. Under either circumstance the party or entity must present evidence at the hearing demonstrating the potential adverse impact a penalty

will have on such person or entity.

6(a) The term "license" or "permit" as used herein shall be defined as a license, permit, franchise or concession not granted as a matter of right.

(b) The term "person" as used herein shall be defined as any natural person doing business alone or associated with another person or entity as a partner, director, officer, principal or employee.

(c) The term "entity" as used herein shall be defined as any firm, partnership, corporation, association, or person that receives monies, benefits, licenses, leases, or permits from or through the City or otherwise transacts business with the City.

(d) The term "member" as used herein shall be defined as any person associated with another person or entity as a partner, director, officer, principal or employee.

7 In addition to and notwithstanding any other provision of this Agreement the commissioner or agency head may in his or her sole discretion terminate this Agreement upon not less than three (3) days written notice in the event contractor fails to promptly report in writing to the Commissioner of Investigation of the City of New York any solicitation of money, goods, requests for future employment or other benefit or thing of value, by or on behalf of any employee of the City or other person, firm, corporation or entity for any purpose which may be related to the procurement or obtaining of this Agreement by the contractor, or affecting the performance of this contract.

4.10 ASSIGNMENT

A. The Contractor shall not assign, transfer, convey or otherwise dispose of this Agreement or of Contractor's rights, obligations, duties, in whole or in part, or of its right to execute it, or its right, title or interest in it or any part thereof, or assign, by power of attorney or otherwise, any of the notices due or to become due under this contract, unless the prior written consent of the Administrator shall be obtained. Any such assignment, transfer, conveyance or other disposition without such consent shall be void.

B. Failure of the Contractor to obtain any required consent to any assignment, shall be cause for termination for cause, at the option of the Administrator; and if so terminated, the City shall thereupon be relieved and discharged from any further liability and obligation to the Contractor, its assignees or transferees, and all monies that may become due under the contract shall be forfeited to the City except so much thereof as may be necessary to pay the Contractor's employees.

- C. The provisions of this clause shall not hinder, prevent, or affect an assignment by the Contractor for the benefit of its creditors made pursuant to the laws of the State of New York.
- D. This Agreement may be assigned by the City to any corporation, agency or instrumentality having authority to accept such assignment.

4.11 SUBCONTRACTING

- A. The Contractor agrees not to enter into any subcontracts for the performance of its obligations, in whole or in part, under this Agreement without the prior written approval of the Department. Two copies of each such proposed subcontract shall be submitted to the Department with the Contractor's written request for approval. All such subcontracts shall contain provisions specifying:
 - 1. That the work performed by the subcontractor must be in accordance with the terms of the Agreement between the Department and the Contractor,
 - 2. That nothing contained in such Agreement shall impair the rights of the Department,
 - 3. That nothing contained herein, or under the Agreement between the Department and the Contractor, shall create any contractual relation between the subcontractor and the Department, and
 - 4. That the subcontractor specifically agrees to be bound by the confidentiality provision set forth in this Agreement between the Department and the Contractor.
- B. The Contractor agrees that it is fully responsible to the Department for the acts and omissions of the subcontractors and of persons either directly or indirectly employed by them as it is for the acts and omissions of person directly employed by it.
- C. The aforesaid approval is required in all cases other than individual employer - employee contracts.
- D. The Contractor shall not in any way be relieved of any responsibility under this Contract by any subcontract.

4.12 PUBLICITY

- A. The prior written approval of the Department is required before the Contractor or any of its employees, servants, agents, or independent contractors may, at any time, either during or after completion or termination of this Agreement, make any statement to the press or issue any material for publication through any media of communication bearing on the work performed or data collected under this Agreement.
- B. If the Contractor publishes a work dealing with any aspect of performance under this Agreement, or of the results and accomplishments attained in such performance, the Department shall have a royalty free, nonexclusive and irrevocable license to reproduce, publish or otherwise use and to authorize others to use the publication.

4.13 PARTICIPATION IN AN INTERNATIONAL BOYCOTT

- A. The Contractor agrees that neither the Contractor nor any substantially-owned affiliated company is participating or shall participate in an international boycott in violation of the provisions of the Export Administration Act of 1979, as amended, or the regulations of the United States Department of Commerce promulgated thereunder.
- B. Upon the final determination by the Commerce Department or any other agency of the United States as to, or conviction of the Contractor or a substantially-owned affiliated company thereof, participation in an international boycott in violation of the provisions of the Export Administration Act of 1979, as amended, or the regulations promulgated thereunder, the Comptroller may, at her option, render forfeit and void this contract.
- C. The Contractor shall comply in all respects, with the provisions of Section 6-114 of the Administrative Code of the City of New York and the rules and regulations issued by the Comptroller thereunder.

4.14 INVENTIONS, PATENTS AND COPYRIGHTS

- A. Any discovery or invention arising out of or developed in the course of performance of this Agreement shall be promptly and fully reported to the Department, and if this work is supported by a federal grant of funds, shall be promptly and fully reported to the Federal Government for determination as to whether patent protection on such invention shall be sought and how the rights in the invention or discovery, including rights under any patent issued thereon, shall be disposed of and administered in order to protect the public interest.
- B. No report, document or other data produced in whole or in part with contract funds shall be copyrighted by the Contractor nor shall any notice of copyright be registered by the

Contractor in connection with any report, document or other data developed for the contract.

- C. In no case shall subsections A and B of this section apply to, or prevent the Contractor from asserting or protecting its rights in any report, document or other data, or any invention which existed prior to or was developed or discovered independently from the activities directly related to this Agreement.

4.15 INFRINGEMENTS

The Contractor shall be liable to the Department and hereby agrees to indemnify and hold the Department harmless for any damage or loss or expense sustained by the Department from any infringement by the Contractor of any copyright, trademark or patent rights of design, systems, drawings, graphs, charts, specifications or printed matter furnished or used by the Contractor in the performance of this Agreement.

4.16 ANTI-TRUST

The Contractor hereby assigns, sells, and transfers to the City all right, title and interest in and to any claims and causes of action arising under the anti-trust laws of the State of New York or of the United States relating to the particular goods or services purchased or procured by the City under this Agreement.

ARTICLE 5. TERMINATION

5.1 TERMINATION OF AGREEMENT

- A. The Department and/or City shall have the right to terminate this Agreement, in whole or in part:
 - 1. Under any right to terminate as specified in any section of this Agreement.
 - 2. Upon the failure of the Contractor to comply with any of the terms and conditions of this Agreement.
 - 3. Upon the Contractor's becoming insolvent.
 - 4. Upon the commencement under the Bankruptcy Act of any proceeding by or against the Contractor, either voluntarily or involuntarily.
 - 5. Upon the Commissioner's determination, termination is in the best interest of the

City.

- B.** The Department or City shall give the Contractor written notice of any termination of this Agreement specifying therein the applicable provisions of subsection A of this section and the effective date thereof which shall not be less than ten (10) days from the date the notice is received.
- C.** The Contractor shall be entitled to apply to the Department to have this Agreement terminated by said Department by reason of any failure in the performance of this Agreement (including any failure by the Contractor to make progress in the prosecution of work hereunder which endangers such performance), if such failure arises out of causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not restricted to: acts of God or of the public enemy; acts of the Government in either its sovereign or contractual capacity; fires; floods; epidemics; quarantine restrictions; strikes; freight embargoes; or any other cause beyond the reasonable control of the Contractor. The determination that such failure arises out of causes beyond the control and without the fault or negligence of the Contractor shall be made by the Department which agrees to exercise reasonable judgment therein. If such a determination is made and the Agreement terminated by the Department pursuant to such application by the Contractor, such termination shall be deemed to be without cause.
- D.** Upon termination of this Agreement the Contractor shall comply with the Department or City close-out procedures, including but not limited to:

 - 1.** Accounting for and refund to the Department or City, within thirty (30) days, any unexpended funds which have been paid to the Contractor pursuant to this Agreement.
 - 2.** Furnishing within thirty (30) days an inventory to the Department or City of all equipment, appurtenances and property purchased through or provided under this Agreement carrying out any Department or City directive concerning the disposition thereof.
 - 3.** Not incurring or paying any further obligation pursuant to this Agreement beyond the termination date. Any obligation necessarily incurred by the Contractor on account of this Agreement prior to receipt of notice of termination and falling due after such date shall be paid by the Department or City in accordance with the terms of this Agreement. In no event shall the "obligation", as used herein, be construed as including any lease agreement, oral or written, entered into between the Contractor and its landlord.
 - 4.** Turn over to the Department or City or its designees all books, records, documents and material specifically relating to this Agreement.

5. Submit, within ninety (90) days, a final statement and report relating to this Agreement. The report shall be made by a certified public accountant or a licensed public accountant.

- E. In the event the Department or City shall terminate this Agreement, in whole or in part, as provided in paragraphs 1, 2, 3, or 4 of subsection A of this section, the Department or City may procure, upon such terms and in such manner as deemed appropriate, services similar to those so terminated, and the Contractor shall continue the performance of this Agreement to the extent not terminated hereby.
- F. Notwithstanding any other provisions of this contract, the Contractor shall not be relieved of liability to the City for damages sustained by the City by virtue of Contractor's breach of the contract, and the City may withhold payments to the Contractor for the purpose of set-off until such time as the exact amount of damages due to the City from the Contractor is determined.
- G. The provisions of the Agreement regarding confidentiality of information shall remain in full force and effect following any termination.
- H. The rights and remedies of the City provided in this section shall not be exclusive and are in addition to all other rights and remedies provided by law or under this Agreement.

6.1 CONFLICT OF LAWS

All disputes arising out of this Agreement shall be interpreted and decided in accordance with the laws of the State of New York.

6.2 GENERAL RELEASE

The acceptance by the Contractor or its assignees of the final payment under this contract, whether by voucher, judgment of any court of competent jurisdiction or any other administrative means, shall constitute and operate as a general release to the City from any and all claims of and liability to the Contractor arising out of the performance of this Contract.

6.3 CLAIMS AND ACTIONS THEREON

- A. No action at law or proceeding in equity against the City or Department shall lie or be maintained upon any claim based upon this Agreement or arising out of this Agreement or in any way connected with this Agreement unless the Contractor shall have strictly complied with all requirements relating to the giving of notice and of information with respect to such claims, all as herein provided.
- B. No action shall lie or be maintained against the City by Contractor upon any claims based upon this Agreement unless such action shall be commenced within six (6) months after the date of filing in the Office of the Comptroller of the City of the certificate for the final payment hereunder, or within six (6) months of the termination or conclusion of this Agreement, or within six (6) months after the accrual of the Cause of Action, whichever first occurs.
- C. In the event any claim is made or any action brought in any way relating to the Agreement herein, the Contractor shall diligently render to the Department and/or the City of New York without additional compensation any and all assistance which the Department and/or the City of New York may require of the Contractor.
- D. The Contractor shall report to the Department in writing within three (3) working days of the initiation by or against the Contractor of any legal action or proceeding in connection with or relating to this Agreement.

6.4 NO CLAIM AGAINST OFFICERS, AGENTS OR EMPLOYEES

No claim whatsoever shall be made by the Contractor against any officer, agent or employee of the City for, or on account of, anything done or omitted in connection with this contract.

6.5 WAIVER

Waiver by the Department of a breach of any provision of this Agreement shall not be deemed to be a waiver of any other or subsequent breach and shall not be construed to be a modification of the terms of the Agreement unless and until the same shall be agreed to in writing by the Department or City as required and attached to the original Agreement.

6.6 NOTICE

The Contractor and the Department hereby designate the business addresses herein above specified as the places where all notices, directions or communications from one such party to the other party shall be delivered, or to which they shall be mailed. Actual delivery of any such notice, direction or communication to a party at the aforesaid place, or delivery by

certified mail shall be conclusive and deemed to be sufficient service thereof upon such party as of the date such notice, direction or communication is received by the party. Such address may be changed at any time by an instrument in writing executed and acknowledged by the party making such change and delivered to the other party in the manner as specified above. Nothing in this section shall be deemed to serve as a waiver of any requirements for the service of notice or process in the institution of an action or proceeding as provided by law, including the Civil Practice Law and Rules.

6.7 ALL LEGAL PROVISIONS DEEMED INCLUDED

It is the intent and understanding of the parties to this Agreement that each and every provision of law required to be inserted in this Agreement shall be and is inserted herein. Furthermore, it is hereby stipulated that every such provision is to be deemed to be inserted herein, and if, through mistake or otherwise, any such provision is not inserted, or is not inserted in correct form, then this Agreement shall forthwith upon the application of either party be amended by such insertion so as to comply strictly with the law and without prejudice to the rights of either party hereunder.

6.8 SEVERABILITY

If this Agreement contains any unlawful provision not an essential part of the Agreement and which shall not appear to have been a controlling or material inducement to the making thereof, the same shall be deemed of no effect and shall upon notice by either party, be deemed stricken from the Agreement without affecting the binding force of the remainder.

6.9 POLITICAL ACTIVITY

There shall be no partisan political activity or any activity to further the election or defeat of any candidate for public, political or party office as part of or in connection with this Agreement, nor shall any of the funds provided under this Agreement be used for such purposes.

6.10 MODIFICATION

This Agreement may be modified by the parties in writing in a manner not materially affecting the substance hereof. It may not be altered or modified orally.

6.11 PARAGRAPH HEADINGS

Paragraph headings are inserted only as a matter of convenience and for reference and in no way define, limit or describe the scope or intent of this contract and in no way affect this contract.

6.12 NO REMOVAL OF RECORDS FROM PREMISES

Where performance of this Agreement involves use by the Contractor of Departmental papers, files, data or records at Departmental facilities or offices, the Contractor shall not remove any such papers, files, data or records, therefrom without the prior approval of the Department's designated official.

6.13 INSPECTION AT SITE

The Department shall have the right to have representatives of the Department or of the City or of the State or Federal governments present at the site of the engagement to observe the work being performed.

ARTICLE 7. MERGER

This written Agreement contains all the terms and conditions agreed upon by the parties hereto, and no other agreement, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the parties hereto, or to vary any of the terms contained herein.

ARTICLE 8. CONDITIONS PRECEDENT

This contract shall neither be binding nor effective unless:

- (a) Approved by the Mayor pursuant to the provision of Executive Order No. 42, dated October 9, 1975, in the event the Executive Order requires such approval; and
- (b) Certified by the Mayor (Mayor's Fiscal Committee created pursuant to Executive Order No. 43, dated October 14, 1975) that performance thereof will be in accordance with the City's financial plan; and
- (c) Approved by the New York State Financial Control Board (Board) pursuant to the New York State Financial Emergency Act for the City of New York, as amended, (the "Act"), in the event regulations of the Board pursuant to the Act require such approval.
- (d) It has been authorized by the Mayor and the Comptroller shall have endorsed her certificate that there remains unexpended and unapplied a balance of the appropriation of

funds applicable thereto sufficient to pay the estimated expense of carrying out this Agreement.

The requirements of this section of the contract shall be in addition to, and not in lieu of, any approval or authorization otherwise required for this contract to be effective and for the expenditure of City funds.

ARTICLE 9. PPB RULES

This contract is subject to the Rules of the Procurement Policy Board of the City of New York effective September 2000. In the event of a conflict between set Rules and a provision of this contract, the Rules shall take precedence.

STATE LABOR LAW AND CITY ADMINISTRATIVE CODE

1. As required by New York State Labor Law Section §220-e:

(a) That in the hiring of employees for the performance of work under this contract or any subcontract hereunder, neither the Contractor, Subcontractor, nor any person acting on behalf of such Contractor or Subcontractor, shall by reason of race, creed, color, sex or national origin discriminate against any citizen of the State of New York who is qualified and available to perform the work to which the employment relates;

(b) That neither the Contractor, Subcontractor, nor any person on his behalf shall, in any manner discriminate against or intimidate any employee hired for the performance of work under this contract on account of race, creed, color, sex or national origin;

(c) That there may be deducted from the amount payable to the Contractor by the City under this contract a penalty of five dollars for each person for each calendar day during which such person was discriminated against or intimidated in violation of the provisions of this contract; and

(d) That this contract may be canceled or terminated by the City and all monies due or to become due hereunder may be forfeited, for a second or any subsequent violation of the terms or conditions of this section of the contract.

(e) The aforesaid provisions of this section covering every contract for or on behalf of the State or a municipality for the manufacture, sale or distribution of materials, equipment or supplies shall be limited to operations performed within the territorial limits of the State of New York.

2. As required by New York City Administrative Code §6-108:

(a) It shall be unlawful for any person engaged in the construction, alteration or repair of buildings or engaged in the construction or repair of streets or highways pursuant to a contract with the City or engaged in the manufacture, sale or distribution of materials, equipment or supplies pursuant to a contract with the City to refuse to employ or to refuse to continue in any employment any person on account of the race, color or creed of such person.

(b) It shall be unlawful for any person or any servant, agent or employee of any person, described in subdivision (a) above, to ask, indicate or transmit, orally or in writing, directly or indirectly, the race, color, creed or religious affiliation of any person employed or seeking employment from such person, firm or corporation.

(c) Disobedience of the foregoing provision shall be deemed a violation of a material provision of this contract.

(d) Any person, or the employee, manager or owner of or officer of such firm or corporation who shall violate any of the provisions of this section shall, upon conviction thereof, be punished by a fine of not more than one hundred dollars or by imprisonment for not more than thirty days, or both.

FORUM PROVISION

CHOICE OF LAW, CONSENT TO JURISDICTION AND VENUE

This contract shall be deemed to be executed in the City of New York, State of New York regardless of the domicile of the Contractor, and shall be governed by and construed in accordance with the laws of the State of New York.

The parties agree that any and all claims asserted by or against the City arising under this contract or related thereto shall be heard and determined either in the courts of the United States located in New York City ("Federal Courts") or in the courts of the State of New York ("New York State Courts") located in the City and County of New York. To effect this Agreement and intent, the Contractor agrees:

(a) If the City initiates any action against the Contractor in Federal Court or in New York State Court, service of process may be made on the Contractor either in person, wherever such Contractor may be found, or by registered mail addressed to the Contractor at its address as set forth in this contract, or to such other address as the Contractor may provide

to the City in writing; and

(b) With respect to any action between the City and the Contractor in New York State Court, the Contractor hereby expressly waives and relinquishes any rights it might otherwise have (i) to move to dismiss on grounds of forum non conveniens; (ii) to remove to Federal Court; and (iii) to move for a change of venue to a New York State Court outside New York County.

(c) With respect to any action between the City and the Contractor in Federal Court located in New York City, the Contractor expressly waives and relinquishes any right it might otherwise have to move to transfer the action to a United States Court outside the City of New York.

(d) If the Contractor commences any action against the City in a court located other than in the City and State of New York, upon request of the City, the Contractor shall either consent to a transfer of the action to a court of competent jurisdiction located in the City and State of New York or, if the court where the action is initially brought will not or cannot transfer the action, the Contractor shall consent to dismiss such action without prejudice and may thereafter reinstitute the action in a court of competent jurisdiction in New York City.

If any provision(s) of this Article is held unenforceable for any reason, each and all other provision(s) shall nevertheless remain in full force and effect.

E.O. 50 EQUAL EMPLOYMENT OPPORTUNITY

This contract is subject to the requirements of New York City Charter Chapter 13-B, §§350 et seq. (Chapter 13-B) Executive Order No. 50 (April 25, 1980) (E.O. 50) and the Rules and Regulations promulgated thereunder. No contract will be awarded unless and until these requirements have been complied with in their entirety. By signing this contract, the contractor agrees that it:

(1) Will not discriminate against any employee or applicant for employment because of race creed, color, national origin, sex, age, disability, marital status, sexual orientation, or citizenship status with respect to all employment decisions including, but not limited to, recruitment, hiring, upgrading, demotion, downgrading, transfer, training, rates of pay or other forms of compensation, layoff, termination, and all other terms and conditions of employment;

(2) Will not discriminate in the selection of subcontractors on the basis of the owner's, partners' or shareholders' race, color, creed, national origin, sex, age, disability, marital

status, sexual orientation or citizenship status;

(3) Will state in all solicitations or advertisements for employees placed by or on behalf of the contractor that all qualified applicants will receive consideration for employment without regard to race, color, creed, national origin, sex, age, disability, marital status, sexual orientation, or citizenship status or is an equal employment opportunity employer;

(4) Will send to each labor organization or representative of workers with which it has a collective bargaining agreement or other contract or memorandum of understanding, written notification of its equal employment opportunity commitments under Chapter 13-B and E.O. 50 and the Rules and Regulations promulgated thereunder;

(5) Will furnish before the contract is awarded all information and reports including an Employment Report which are required by Chapter 13-B, E.O. 50, the Rules and Regulations promulgated thereunder, and orders of the Director of the Office of Labor Services (OLS). Copies of all required reports are available upon request from the contracting agency; and

(6) Will permit OLS to have access to all relevant books, records and accounts for the purposes of investigation to ascertain compliance with such Rules, Regulations, and orders.

The Contractor understands that in the event of its noncompliance with nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, such noncompliance shall constitute a material breach of the contract and noncompliance with Chapter 13-B, E.O. 50 and the Rules and Regulations promulgated thereunder. After a hearing held pursuant to the rules of OLS, the Director may direct the imposition by the contracting agency head of any or all of the following sanctions:

- (i) disapproval of the Contractor;
- (ii) suspension or termination of all or parts of and/or of payments therefor;
- (iii) declaring the contractor in default; or
- (iv) in lieu of any of the foregoing sanctions, the Director may impose an employment program.

The Director of OLS may recommend to the contracting agency head that a Board of Responsibility constituted pursuant to the Rules and Regulations of the Procurement Policy Board be convened for purposes of declaring a contractor who has repeatedly failed to comply with Chapter 13-B, E.O. 50 and the Rules and Regulations promulgated thereunder to be non-responsible.

The Contractor agrees to include the provisions of the foregoing paragraphs in every subcontract or purchase order in excess of \$100,000 to which it becomes a party unless exempted by Chapter 13-B, E.O. 50 and the Rules and Regulations promulgated thereunder, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as may be directed by the Director of OLS as a means of enforcing such provisions including sanctions for noncompliance.

The Contractor further agrees that it will refrain from entering into any contract or contract modification subject to Chapter 13-B, E.O. 50 and the Rules and Regulations promulgated thereunder with a subcontractor who is not in compliance with the requirements of E.O. 50 and the Rules and Regulations promulgated thereunder.

RESOLUTION OF DISPUTES:

1. Except as provided in 1(a) and 1(b) below, all disputes between the City and the vendor that arise under, or by virtue of, this contract shall be finally resolved in accordance with the provisions of this section and Section 4-09 of the Rules of the Procurement Policy Board (“PPB Rules”). This procedure shall be the exclusive means of resolving any such disputes.
 - (a) This section shall not apply to disputes concerning matters dealt with in other sections of the PPB Rules or to disputes involving patents, copyrights, trademarks, or trade secrets (as interpreted by the courts of New York State) relating to proprietary rights in computer software.
 - (b) For construction and construction-related services this section shall apply only to disputes about the scope of work delineated by the contract, the interpretation of contract documents, the amount to be paid for extra work or disputed work performed in connection with the contract, the conformity of the vendor’s work to the contract, and the acceptability and quality of the vendor’s work; such disputes arise when the Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner makes a determination with which the vendor disagrees.
2. All determinations required by this section shall be clearly stated, with a reasoned explanation for the determination based on the information and evidence presented to the party making the determination. Failure to make such determination within the time required by this section shall be deemed a non-determination without prejudice that will allow application to the next level.
3. During such time as any dispute is being presented, heard, and considered pursuant to this section, the contract terms shall remain in full force and effect

and the vendor shall continue to perform work in accordance with the contract and as directed by the Agency Chief Contracting Officer (“ACCO”) or Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner. Failure of the vendor to continue the work as directed shall constitute a waiver by the vendor of any and all claims being presented pursuant to this section and a material breach of contract.

4. Presentation of Dispute to Agency Head.

- (a) Notice of Dispute and Agency Response. The vendor shall present its dispute in writing (“Notice of Dispute”) to the Agency Head within the time specified herein, or, if no time is specified, within thirty (30) days of receiving written notice of the determination or action that is the subject of the dispute. This notice requirement shall not be read to replace any other notice requirements contained in the contract. The Notice of Dispute shall include all the facts, evidence, documents, or other basis upon which the vendor relies in support of its position, as well as a detailed computation demonstrating how any amount of money claimed by the vendor in the dispute was arrived at. Within thirty (30) days after receipt of the complete Notice of Dispute, the ACCO or, in the case of construction or construction-related services, the Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner, shall submit to the Agency Head all materials he or she deems pertinent to the dispute. Following initial submissions to the Agency Head, either party may demand of the other the production of any document or other material the demanding party believes may be relevant to the dispute. The requested party shall produce all relevant materials that are not otherwise protected by a legal privilege recognized by the courts of New York State. Any question of relevancy shall be determined by the Agency Head whose decision shall be final. Willful failure of the vendor to produce any requested material whose relevancy the vendor has not disputed, or whose relevancy has been affirmatively determined, shall constitute a waiver by the vendor of its claim.
- (b) Agency Head Inquiry. The Agency Head shall examine the material and may, in his or her discretion, convene an informal conference with the vendor and the ACCO and, in the case of construction or construction-related services, the Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner, to resolve the issue by mutual consent prior to reaching a determination. The Agency Head may seek such technical or other expertise as he or she shall deem appropriate, including the use of neutral mediators, and require any such additional material from either or both parties as he or she deems fit. The Agency Head’s ability to render, and the effect of, a decision hereunder shall not be impaired by any negotiations in connection with the dispute presented, whether or not the Agency Head participated therein. The Agency Head may or, at the request of any party to the dispute, shall compel the participation of any other vendor with a contract related to the work of this

contract and that vendor shall be bound by the decision of the Agency Head. Any vendor thus brought into the dispute resolution proceeding shall have the same rights and obligations under this section as the vendor initiating the dispute.

- (c) Agency Head Determination. Within thirty (30) days after the receipt of all materials and information, or such longer time as may be agreed to by the parties, the Agency Head shall make his or her determination and shall deliver or send a copy of such determination to the vendor and ACCO and, in the case of construction or construction-related services, the Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner, together with a statement concerning how the decision may be appealed.
 - (d) Finality of Agency Head Decision. The Agency Head's decision shall be final and binding on all parties, unless presented to the Contract Dispute Resolution Board ("CDRB") pursuant to this section. The City may not take a petition to the CDRB. However, should the vendor take such a petition, the City may seek, and the CDRB may render, a determination less favorable to the vendor and more favorable to the City than the decision of the Agency Head.
5. Presentation of Dispute to the Comptroller. Before any dispute may be brought by the vendor to the CDRB, the vendor must first present its claim to the Comptroller for his or her review, investigation, and possible adjustment.
- (a) Time, Form, and Content of Notice. Within thirty (30) days of receipt of a decision by the Agency Head, the vendor shall submit to the Comptroller and to the Agency Head a Notice of Claim regarding its dispute with the agency. The Notice of Claim shall consist of (i) a brief statement of the substance of the dispute, the amount of money, if any, claimed and the reason(s) the vendor contends the dispute was wrongly decided by the Agency Head; (ii) a copy of the decision of the Agency Head, and (iii) a copy of all materials submitted by the vendor to the agency, including the Notice of Dispute. The vendor may not present to the Comptroller any material not presented to the Agency Head, except at the request of the Comptroller.
 - (b) Agency Response. Within thirty (30) days of receipt of the Notice of Claim, the agency shall make available to the Comptroller a copy of all material submitted by the agency to the Agency Head in connection with the dispute. The agency may not present to the Comptroller any material not presented to the Agency Head, except at the request of the Comptroller.
 - (c) Comptroller Investigation. The Comptroller may investigate the claim in dispute and, in the course of such investigation, may exercise all powers provided in sections 7-201 and 7-203 of the New York City

Administrative Code. In addition, the Comptroller may demand of either party, and such party shall provide, whatever additional material the Comptroller deems pertinent to the claim, including original business records of the vendor. Willful failure of the vendor to produce within fifteen (15) days any material requested by the Comptroller shall constitute a waiver by the vendor of its claim. The Comptroller may also schedule an informal conference to be attended by the supplier, agency representatives, and any other personnel desired by the Comptroller.

- (d) Opportunity of Comptroller to Compromise or Adjust Claim. The Comptroller shall have forty-five (45) days from his or her receipt of all materials referred to in 5(c) to investigate the disputed claim. The period for investigation and compromise may be further extended by agreement between the vendor and the Comptroller, to a maximum of ninety (90) days from the Comptroller's receipt of all the materials. The vendor may not present its petition to the CDRB until the period for investigation and compromise delineated in this paragraph has expired. In compromising or adjusting any claim hereunder, the Comptroller may not revise or disregard the terms of the contract between the parties.

6. Contract Dispute Resolution Board. There shall be a Contract Dispute Resolution Board composed of:

- (a) the chief administrative law judge of the Office of Administrative Trials and Hearings ("OATH") or his/her designated OATH administrative law judge, who shall act as chairperson, and may adopt operational procedures and issue such orders consistent with this section as may be necessary in the execution of the CDRB's functions, including, but not limited to, granting extensions of time to present or respond to submissions;
- (b) the City Chief Procurement Officer ("CCPO") or his/her designee, or in the case of disputes involving construction, the Director of the Office of Construction or his/her designee; any designee shall have the requisite background to consider and resolve the merits of the dispute and shall not have participated personally and substantially in the particular matter that is the subject of the dispute or report to anyone who so participated, and
- (c) a person with appropriate expertise who is not an employee of the City. This person shall be selected by the presiding administrative law judge from a prequalified panel of individuals, established and administered by OATH, with appropriate background to act as decision-makers in a dispute. Such individuals may not have a contract or dispute with the City or be an officer or employee of any company or organization that does, or regularly represent persons, companies, or organizations having disputes with the City.

7. Petition to CDRB. In the event the claim has not been settled or adjusted by the Comptroller within the period provided in this section, the vendor, within thirty

- (30) days thereafter, may petition the CDRB to review the Agency Head determination.
- (a) **Form and Content of Petition by Vendor.** The vendor shall present its dispute to the CDRB in the form of a Petition, which shall include (i) a brief statement of the substance of the dispute, the amount of money, if any, claimed, and the reason(s) the vendor contends that the dispute was wrongly decided by the Agency Head; (ii) a copy of the decision of the Agency Head; (iii) copies of all materials submitted by the vendor to the agency; (iv) a copy of the decision of the Comptroller, if any, and (v) copies of all correspondence with, and material submitted by the vendor to, the Comptroller's Office. The vendor shall concurrently submit four complete sets of the Petition: one to the Corporation Counsel (Attn: Commercial and Real Estate Litigation Division), and three to the CDRB at OATH's offices, with proof of service on the Corporation Counsel. In addition, the vendor shall submit a copy of the statement of the substance of the dispute, cited in (i) above, to both the Agency Head and the Comptroller.
 - (b) **Agency Response.** Within thirty (30) days of receipt of the Petition by the Corporation Counsel, the agency shall respond to the statement of the vendor and make available to the CDRB all material it submitted to the Agency Head and Comptroller. Three complete copies of the agency response shall be submitted to the CDRB at OATH's offices and one to the vendor. Extensions of time for submittal of the agency response shall be given as necessary upon a showing of good cause or, upon the consent of the parties, for an initial period of up to thirty (30) days.
 - (c) **Further Proceedings.** The Board shall permit the vendor to present its case by submission of memoranda, briefs, and oral argument. The Board shall also permit the agency to present its case in response to the vendor by submission of memoranda, briefs, and oral argument. If requested by the Corporation Counsel, the Comptroller shall provide reasonable assistance in the preparation of the agency's case. Neither the vendor nor the agency may support its case with any documentation or other material that was not considered by the Comptroller, unless requested by the CDRB. The CDRB, in its discretion, may seek such technical or other expert advice as it shall deem appropriate and may seek, on its own or upon application of a party, any such additional material from any party as it deems fit. The CDRB, in its discretion, may combine more than one dispute between the parties for concurrent resolution.
 - (d) **CDRB Determination.** Within forty-five (45) days of the conclusion of all submissions and oral arguments, the CDRB shall render a decision resolving the dispute. In an unusually complex case, the CDRB may render its decision in a longer period of time, not to exceed ninety (90) days, and shall so advise the parties at the commencement of this period. The CDRB's decision must be consistent with the terms of the contract.

Decisions of the CDRB shall only resolve matters before the CDRB and shall not have precedential effect with respect to matters not before the CDRB.

- (e) Notification of CDRB Decision. The CDRB shall send a copy of its decision to the vendor, the ACCO, the Corporation Counsel, the Comptroller, the CCPO, the Office of Construction, the PPB, and, in the case of construction or construction-related services, the Engineer, Resident Engineer, Engineering Audit Officer, or other designee of the Commissioner. A decision in favor of the vendor shall be subject to the prompt payment provisions of the PPB Rules. The Required Payment Date shall be thirty (30) days after the date the parties are formally notified of the CDRB's decision.
 - (f) Finality of CDRB Decision. The CDRB's decision shall be final and binding on all parties. Any party may seek review of the CDRB's decision solely in the form of a challenge, filed within four months of the date of the CDRB's decision, in a court of competent jurisdiction of the State of New York, County of New York pursuant to Article 78 of the Civil Practice Law and Rules. Such review by the court shall be limited to the question of whether or not the CDRB's decision was made in violation of lawful procedure, was affected by an error of law, or was arbitrary and capricious or an abuse of discretion. No evidence or information shall be introduced or relied upon in such proceeding that was not presented to the CDRB in accordance with Section 4-09 of the PPB Rules.
8. Any termination, cancellation, or alleged breach of the contract prior to or during the pendency of any proceedings pursuant to this section shall not affect or impair the ability of the Agency Head or CDRB to make a binding and final decision pursuant to this section.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

ANTI VIRUS SECURITY POLICY

THE POLICY

CITY OF NEW YORK COMPUTING RESOURCES WILL BE PROTECTED FROM MALICIOUS SOFTWARE AND VIRUSES.

SCOPE

This policy applies to all computer systems that access or process City information.

MONITORING

- 1) DoITT in conjunction with the agency CISO reserves the right to scan the network and computing resources for malicious software including but not limited to viruses¹ or spyware².
- 2) DoITT reserves the right to quarantine any agency network or computing resource that may pose a risk to Citynet.
- 3) DoITT reserves the right to immediately disconnect from Citynet any device inadequately protected by anti-virus or anti-spyware software.
 - a. Computing devices removed from Citynet for non-compliance must confirm appropriate remediation prior to reconnection to Citynet.

ANTI-VIRUS REQUIREMENTS

- 4) Servers, desktops, and laptops must have commercial anti-virus software installed, properly configured and running at all times.
- 5) Anti-virus software must be configured to automatically remove the virus.
- 6) Users shall not disable automatic virus scanning on their local machines.
- 7) Server administrators will not disable anti-virus software on server machines.

ANTI-VIRUS & SPYWARE SCANNING

- 8) Users should not initiate any scans on devices beyond their local resources (e.g. hard disk, CD, USB). Users will refrain from scanning network resources.
- 9) All electronic mail entering and leaving Citynet (i.e., to/from the Internet) must be scanned.
- 10) Electronic mail entering or leaving Citynet may be blocked on the basis of file type and file size.

¹ Software used to infect a computer.

² Software that sends information about your Web surfing habits back to its Web site.



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

- a. The criteria for blocking of items are maintained by DoITT and shall be reviewed and updated periodically as circumstances require.
- 11) Scan settings for laptops, desktops, workstations that are not explicitly addressed by this policy shall be determined by the agency level CISO.

ANTI-VIRUS UPDATING

- 12) Agency administrators are responsible for validating version and signature files for desktop and laptop machines.
- 13) Server administrators are responsible for validating version and signature files for servers.
- 14) Users are responsible for validating version and signature files for stand-alone computers that are not connected to the network.
- 15) When possible, signature updates must be installed without user intervention.
- 16) New versions of the virus signature files must be loaded within 48 hours. Failure to comply will result in disconnection from Citynet.

VIRUS REPORTING

- 17) If an agency is hosted by DoITT users must notify the DoITT helpdesk when a computer virus is suspected or detected. All other agencies should notify their local information technology team.
- 18) All virus alerts must be followed by an immediate full scan of affected devices performed by IT personnel.
- 19) Agency administrators must perform a root cause investigation when a virus is identified to ensure proper containment.

USER RESPONSIBILITIES

- 20) Users should not open any files attached to electronic mail from an unknown or un-trusted sources. Electronic messages with suspicious subject lines or content should be deleted without opening.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

APPLICATION SECURITY DEVELOPMENT

THE POLICY

ALL SYSTEMS AND APPLICATIONS THAT PROCESS OR STORE CITY OF NEW YORK INFORMATION SHALL ADDRESS INFORMATION SECURITY REQUIREMENTS DURING ALL PHASES OF THE DEVELOPMENT CYCLE.

SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATIONS

- 1) An assessment will be conducted by the business and/or system owner to identify the type of information that will be stored, processed or transmitted by the system.
- 2) Stringency of system security requirements will be defined in accordance to the value of the data contained in the system.
 - a. Systems that contain personal identifiable information (PII) or personal health information (PHI) must comply with all applicable regulatory statutes.
- 3) A comprehensive security requirements analysis will be performed for all new systems and for significant upgrades to existing systems. The security analysis will assess compliance to the Citywide Information Security Policies.
- 4) System security requirements and specifications must be compliant with industry best practice standards for technologies and system configuration and Citywide Information Security Standards where applicable.
- 5) System security requirements and specifications must ensure interoperability with all information sources and services with which it must interface.
- 6) System security requirements and specifications must ensure integration with existing security services where applicable.

SECURITY VERIFICATION

- 7) All new systems must be tested in a separate environment for stability and to identify any unanticipated interactions with existing systems before they are moved to the production environment.
- 8) All new systems must be tested for security integrity and functional verification prior to production release.
- 9) Any new applications that will connect to Citynet must be approved by the Citywide Chief Information Security Officer (CISO) to ensure that there will be no negative impact to Citynet.
- 10) The agency CISO (or equivalent position) must make final approval on all application security which has an agency level impact.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

DEVELOPMENT & TESTING

- 11) The production environment will not be used for development or testing activities.
- 12) All security functionality will be operational during formal acceptance and operational testing.
- 13) Prior to production release of any new application, testing will be done to ensure the new application will not adversely affect any existing systems.
- 14) Newly developed applications and major upgraded applications will be approved for use at the agency by the Chief Information Officer (CIO, or equivalent position) prior to migration to the production environment.

BUSINESS CONTINUITY

- 15) Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.
- 16) Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

APPLICATION SECURITY DEVELOPMENT

THE POLICY

ALL SYSTEMS AND APPLICATIONS THAT PROCESS OR STORE CITY OF NEW YORK INFORMATION SHALL ADDRESS INFORMATION SECURITY REQUIREMENTS DURING ALL PHASES OF THE DEVELOPMENT CYCLE.

SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATIONS

- 1) An assessment will be conducted by the business and/or system owner to identify the type of information that will be stored, processed or transmitted by the system.
- 2) Stringency of system security requirements will be defined in accordance to the value of the data contained in the system.
 - a. Systems that contain personal identifiable information (PII) or personal health information (PHI) must comply with all applicable regulatory statutes.
- 3) A comprehensive security requirements analysis will be performed for all new systems and for significant upgrades to existing systems. The security analysis will assess compliance to the Citywide Information Security Policies.
- 4) System security requirements and specifications must be compliant with industry best practice standards for technologies and system configuration and Citywide Information Security Standards where applicable.
- 5) System security requirements and specifications must ensure interoperability with all information sources and services with which it must interface.
- 6) System security requirements and specifications must ensure integration with existing security services where applicable.

SECURITY VERIFICATION

- 7) All new systems must be tested in a separate environment for stability and to identify any unanticipated interactions with existing systems before they are moved to the production environment.
- 8) All new systems must be tested for security integrity and functional verification prior to production release.
- 9) Any new applications that will connect to Citynet must be approved by the Citywide Chief Information Security Officer (CISO) to ensure that there will be no negative impact to Citynet.
- 10) The agency CISO (or equivalent position) must make final approval on all application security which has an agency level impact.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

DEVELOPMENT & TESTING

- 11) The production environment will not be used for development or testing activities.
- 12) All security functionality will be operational during formal acceptance and operational testing.
- 13) Prior to production release of any new application, testing will be done to ensure the new application will not adversely affect any existing systems.
- 14) Newly developed applications and major upgraded applications will be approved for use at the agency by the Chief Information Officer (CIO, or equivalent position) prior to migration to the production environment.

BUSINESS CONTINUITY

- 15) Each application must have a defined back out plan in the unlikely event that its migration to the production environment causes service degradation.
- 16) Each new application must create a business continuity and disaster recovery program in accordance with the business significance of the application.



**CITYWIDE INFORMATION SECURITY
ARCHITECTURE, FORMULATION & ENFORCEMENT
(CISAFE)**

**DEPARTMENT OF INVESTIGATION
CITY OF NEW YORK
CONFIDENTIAL**

Information Security Directive

**Application Security – Version 1.
D 4.4**

April 29, 2003

Table of Contents

1.	Application Security Overview.....	1
1.1	Introduction.....	1
1.2	Internal vs. External Attacks.....	1
1.3	Types of Security Risk.....	2
1.3.1	<i>Types of Deliberate Attack.....</i>	2
1.3.2	<i>Types of Accidental Damage.....</i>	3
1.4	Authorization.....	3
1.5	Encryption.....	4
1.6	Strong Authentication.....	4
1.7	Security by Obscurity.....	5
2.	Securing the Application.....	6
2.1	Introduction.....	6
2.2	Access control.....	6
2.2.1	<i>Authentication.....</i>	6
2.2.2	<i>Passwords.....</i>	6
2.2.3	<i>Authorization.....</i>	7
2.2.4	<i>User Accounts.....</i>	7
2.2.5	<i>Third Party Access.....</i>	8
2.2.6	<i>Protection Against Unauthorized Access.....</i>	9
2.3	Client Security.....	10
2.4	Server Security.....	11
2.5	Fault Tolerance and Contingency.....	11
2.6	Backup and Recovery.....	12
2.7	Application Output.....	12
2.8	Data Integrity.....	13
2.9	Transaction Security.....	13
2.10	Information Pollution.....	13
2.11	Workflow Transactions and City Agency Business Processes.....	15
2.12	Application Interfaces.....	15
2.13	Interfaces to External and Supplier Systems (Extranets).....	16
2.14	Cryptography and Encryption Directives.....	16
2.15	Denial of Service.....	17
2.16	Audit / Management Trails.....	17
2.17	Configuration Management and Change Control.....	18
2.18	Object Orientation.....	19
2.19	Data Warehousing.....	19
2.20	Common Security Environments.....	19
2.21	Third Party Software and Vertical Applications.....	20
2.22	Documentation.....	20
3.	Application Design Controls.....	21
3.1	Development Environment.....	21
3.2	Use of CASE.....	21

3.3	Application testing	21
3.4	Security Testing	22
3.5	User Interface Ergonomics	22
3.5.1	<i>Interface Design</i>	22
3.5.2	<i>Interface Controls and Restrictions</i>	23
4.	Application Administration	24
4.1	Roles and Least privilege	24
4.2	Segregation of Duty	26
4.3	Security Administration	27
5.	Monitoring	28
5.1	Event Logging	28
5.2	State Monitoring	28
6.	Appendix A	29
6.1	Purpose	29
6.2	Who Must Use This Directive	29
6.3	Information Security Risk Assessment	29
6.4	Document Convention	30
7.	Appendix B -- Areas of Responsibility for Implementation of this Document	31
7.1	CISAFE	31
7.2	DoITT	31
7.3	Technology Steering Committee	31
7.4	City Agency and Unit Management	32
7.5	Internal Audit	32
8.	Glossary of Application Terms	33
9.	References	34

1. Application Security Overview

1.1 Introduction

To aid understanding of the terminology presented in this and other directives, this section discusses the basic concepts of Information Technology (IT) Security and Information Security. These concepts are high level and apply to the whole IT environment, rather than any specific technology.

1.2 Internal vs. External Attacks

Most users tend to think of Information Security as perimeter security, that is, a barbed wire fence around "the organization." This implies that all the threat is on the outside. Perimeter security, as opposed to internal security (Figure 1) applies to the layer of security that surrounds the organization and its systems. The concept of perimeter security relies on the assumption that all internal personnel, including temporary staff and contractors, are completely beyond reproach.

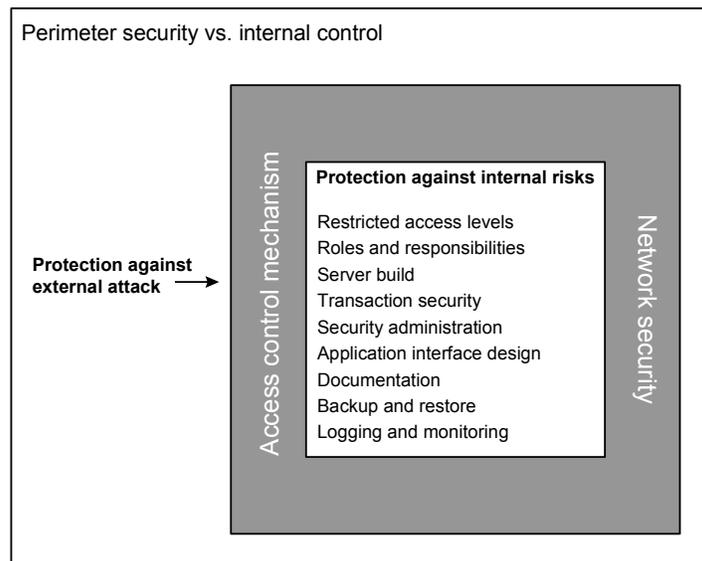


Figure 1. Perimeter Security vs. Internal Control

Accountability is a cornerstone of system security, but it is often overlooked. Logging on to a computer system is analogous to using a bank account. The Personal Identification Number (PIN) is a minor detail, simply a barrier - a means of protecting the account. The account itself has an owner and is a tangible asset. In the same way, users have accounts on computer systems. Activity is monitored and recorded to audit trails and security logs. Without accountability, any routine monitoring or security investigations lose value because activity cannot be attributed to a single user. This is why accounts may not be shared. In particular:

- all users, both internal and external must be identifiable (i.e. accounts, not just passwords); and
- systems must be protected against attack from inside as well as outside the City agency.

1.3 Types of Security Risk

The three classic facets of Information Security are confidentiality, integrity and availability. They are defined as:

- *Confidentiality*, the system contains information that requires protection from unauthorized disclosure.
- *Integrity*, the system contains information that must be protected from unauthorized, unanticipated or unintentional modification, including the detection of such activities.
- *Availability*, the system contains information or provides services, which must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Risks may be realized accidentally or deliberately. Accidental damage may occur as a result of a physical disaster, poor management or inadequate design. The press tends to report deliberate attacks but not accidental damage, except in extreme cases. This is unfortunate because it is at least as important to protect systems against poor management and control as it is to protect against crackers (often wrongly called hackers by the same newspapers).

Actions or measures that can be taken to reduce an individual risk are referred to throughout these directives as controls. A control either reduces the probability of a risk being realized or reduces its impact.

1.3.1 Types of Deliberate Attack

Disclosure (possession) occurs when an attacker reads a private message or transaction details. In all of these models, an attacker may be physically or logically within the organization. Disclosure may also occur accidentally (e.g. if a confidential message was sent to the wrong person).

Interruption occurs when the attacker performs a Denial of Service (DOS) attack. This could be in the form of physical attack on communications equipment or buildings or in the form of a software-based attack. Typically, a known vulnerability would be used to interrupt service to the system, either on a temporary or more permanent basis.

Modification occurs when the attacker changes the message. This may be done to divert funds or to impact the City's or City agency's reputation. Typically, this type of attack would be composed of an interruption and fabrication attack.

Fabrication (spoofing) occurs when the attacker masquerades as the legitimate transmitter. In the case of a payments system, a payment could be fabricated in the form of a legitimate payment message as long as the standard format of a payment message was known.

Figure 2 demonstrates how these attacks would be carried out on a message as it is sent from the transmitter to the receiver, without any controls on the transmission channel.

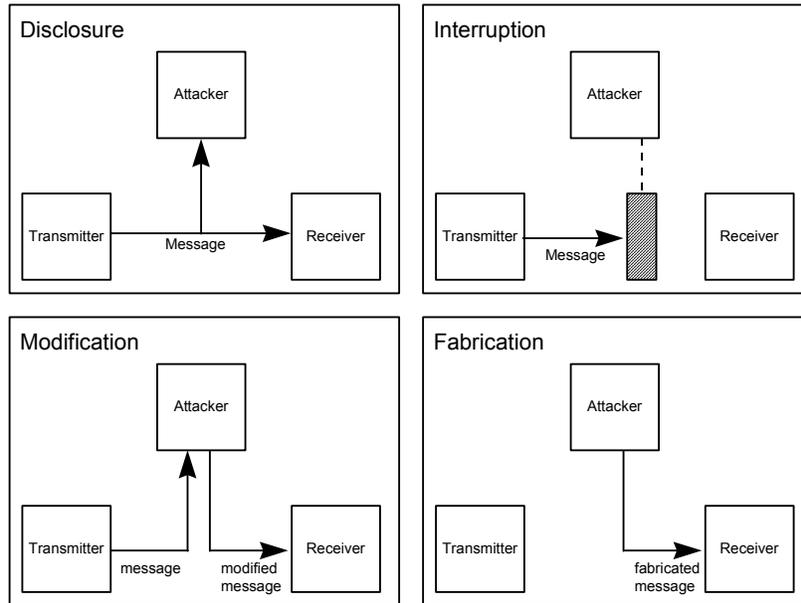


Figure 2. Types of attacks

Attacks may be combined or repeated. For example, an attacker attempting to fabricate a message might perform an Interruption (denial of service) attack first.

1.3.2 Types of Accidental Damage

Accidental damage might include a software “bug,” which may introduce an error into calculations or a physical disaster such as a fire or flood. The backup and contingency arrangements for a critical system (as determined by the results of the Information Security Risk Assessment) represent a major risk, as does the threat of a software bug. Although malicious, external attacks tend to be given more exposure by the media, the statistically greatest threat to systems is accidental loss of availability through poor internal controls. In other words, the likelihood is greater that money will be lost through failure to adequately backup data than due to so-called hacking.

1.4 Authorization

In traditional, monolithic organizations, requests for new system accounts and membership of permission groups would be authorized by the requesting user’s manager, often without intimate knowledge of the system, its criticality or the impact that making that decision might have.

Throughout this directive, the concept of authorization based on seniority is replaced with ownership of information and informed risk acceptance. That is, in the new model, the City agency information owner authorizes changes, irrespective of seniority, because the City agency owns the risk.

In practice, the City agency information owner would nominate authorized signatories. They would be authorized to sign-off user requests in their area. These signatories own the risk (vicariously) and are in a position to make risk based decisions about whether to grant an account to the requesting user and what level of access they must have.

1.5 Encryption

Cryptography is the field of mathematics concerned with protecting information by making it unreadable. The technique of encryption is fundamentally different from encoding (i.e. where the message is formatted according to a known protocol). Encryption relies on a key, which is used to encrypt the message such that, even if the encryption algorithm is published, the message cannot be read by anyone who does not hold the decryption key.

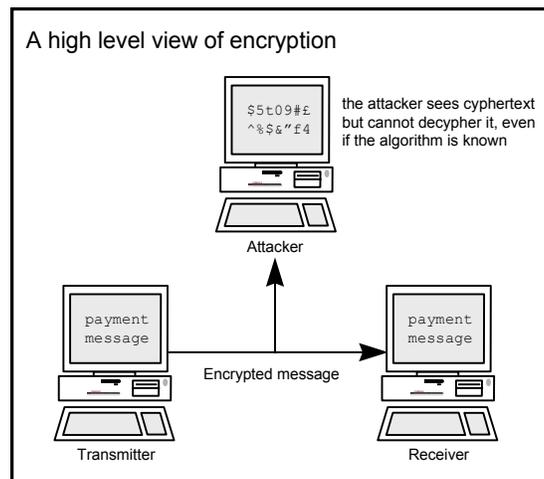


Figure 3. A high level view of encryption

Encryption and cryptographic techniques are used not only to protect information against disclosure, but also to authenticate users, to digitally sign messages and to ensure that messages arrive intact. Encryption is fundamentally different to encoding, where the objective is not to make the data secret, but to change its format. Relying on encoding to keep information confidential is an example of security by obscurity.

Cryptography and methods for encrypting messages are further discussed in the City's *Information Security Directive: Encryption*.

1.6 Strong Authentication

Strong authentication offers better protection against password scanning (or sniffing) because it relies on something more than a password. For example, two-factor strong authentication relies on something the user has (e.g. authentication token), as well as, something the user knows (e.g. a password or PIN).

Typically a one-time password pad is used to authenticate the user. The password is generated by a token and cycles periodically, so it is only good for a limited amount of time, typically thirty seconds. An example of two-factor strong authentication is illustrated below (Figure 4). Even if the attacker can see the password, it is useless, because it can only be used once.

Most non-critical applications employ weak authentication, whereby the username and password are sent on a network (e.g. from the client to the server) in clear (not encrypted). The problem with this mechanism is that the username and password can easily be picked up and reused by anyone with physical access to the network and a protocol analyzer, which is supplied with most versions of an operating system (e.g. UNIX). The password is therefore a simple defense against the casual attacker.

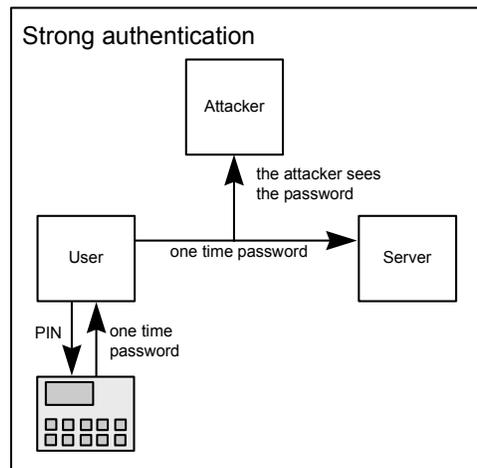


Figure 4. Example of Strong Authentication: Two-factor authentication

Session encryption may also be used as a means of strong authentication, whereby users send their passwords down secure channels to the server. For more details on session encryption, refer to the City's *Information Security Directive: Encryption*.

Strong authentication methods are further discussed in the City's *Information Security Directive: Authentication*.

1.7 Security by Obscurity

Security by obscurity is a concept sometimes used to "protect" information systems and their data, where vulnerabilities are known by the vendor or developer. The integrity of the system is wholly reliant on those vulnerabilities not becoming known or exploited. An example of security by obscurity is a transaction based system where the format of messages is not published in the hope that an attacker will not be able to fabricate payments because they do not know the format of the messages. Some vendors practice security by obscurity, tending to ignore known security vulnerabilities and failing to document them, in the hope that they will not be discovered. Historically, this approach does not work.

2. Securing the Application

2.1 Introduction

This section discusses those controls that are relevant to application developers. Techniques, products and concepts are presented in terms of approach rather than strict policies. Specific technical control objectives, including platform specific controls, are detailed in individual City *Standards*.

2.2 Access control

In the next sections we discuss the major access control mechanisms that the City agencies must deploy for their applications. For additional information and guidance, refer to the City's *Information Security Directives: Authentication, Password Management, and User Account Management*.

2.2.1 Authentication

Individual users and application entities must authenticate to the application using a unique and standard identifier, such as a user ID/password combination. As passwords often may traverse the network in clear, the traditional account/password based authentication model is only a weak access control mechanism and is not suitable for critical applications. The City agency must deploy a stronger authentication model for critical applications (e.g. one-time passwords generated by smart-cards). The City agency applications must also be designed to support deployment of a common user authentication and authorization subsystem (single sign-on mechanism).

The application must use either the operating system facilities for the management of accounts or a City agency approved single sign-on mechanism. The user may not be required to supply further authentication credentials to the application layer in order to gain access. Rather, the application must inherit the credentials of the user from the operating system layer.

All users and application entities must be authenticated before any level of access to information or functionality is granted. The minimum acceptable method of authentication must be password based. Existence of software or files on a user's workstation may not be used as the basis for authentication.

Authentication methods are further discussed in the City's *Information Security Directive: Authentication*.

2.2.2 Passwords

All users are required to have a password to access the corporate network. Users must be given the ability to choose their own password at any time and must be forced to choose a good password. As a recommendation, passwords must be at least eight characters long and must contain at least one numeric or special character. A password history facility is available with most standard operating systems and must be used to prevent the user from recycling any of their last twelve passwords. Users must also be forced to change their passwords every thirty days.

Passwords must be held in adequately protected files, preferably using an approved one-way encryption algorithm. File permission controls are detailed in relevant platform standards. *Password controls are further discussed in the Information Security Directive: Password Management.*

Passwords may not be used to form part of any error message or report, nor must they be visible or accessible to either the system administrator or the security administrator. Further more, passwords may not be coded into commands, macros, or programs, as these commands are vulnerable to attack. This is also a problem to control because those passwords would need to be built into each user's standard build profile.

2.2.2.1 PINs

Personal Identification Numbers (PINs) may be used in conjunction with smartcards or one-time password pads, as part of a strong authentication mechanism. Because PINs are more limited than passwords, controls must be in place to prevent unauthorized access to a device controlled by a PIN.

PINs must be a minimum of four digits. Where possible, they must be 6 digits. It is important to maximize the number of possible PINs to prevent speculative access attempts. Users must also be prevented from choosing easily guessed PINs, including consecutive sequences (e.g. 1234) and repeated numbers (e.g. 7777).

PINs must be randomly generated and may not be displayed on screen, either at the point of entry or in any report or administration routine.

The way PINs are stored by the application must be considered. For example, PINs must be stored in one-way encrypted form to ensure that there is no facility to read or recover them.

2.2.3 Authorization

Applications must be constructed internally on the principle of least privilege, with the underlying system acting as an additional level of control. Least privilege is the concept of giving the user no privileges by default and adding privileges as required, rather than taking away privileges that are not needed.

Application permissions may not be based on operating system permissions, although access to data objects and system utilities must also be restricted at the operating system level.

2.2.4 User Accounts

The user profile repository must be adequately protected against unauthorized modification. As a guiding principle, access to system utilities and files such as this must be restricted to the administrator group and auditing enabled to trap unauthorized activity. All application entity calls to shared libraries, especially Remote Procedure Calls (RPCs), must be authenticated. This is to ensure that program images are not executed without being authenticated.

The application must be protected against unauthorized access by an approved authentication model which is at a level commensurate with the application's risk classification (based on the results of the Information Security Risk Assessment).

Accounts for City agency applications may not be shared because loss of accountability introduces a number of vulnerabilities. Shared passwords tend to be written on notice boards and post-it notes. Typically, this leads to "information leak," which is a ripple effect and very difficult to control. Applications may not permit simultaneous logon attempts from a single user unless there is an explicit and documented business requirement to do this. Audit logs also tend to lose value if accounts are shared as actions cannot easily be attributed to an individual. For the same reason, guest accounts must be removed and each account must be linked to a system profile which must include information about the user such as full name, location, privileges and role.

User account management is further discussed in the City's *Information Security Directive: User Account Management*.

2.2.4.1 High Privilege Accounts

City agency operators must be issued accounts which have sufficient high-privileges to perform their job function. The ultimate supervisor or system manager account must be retained for emergencies.

Privileged accounts must be protected with a minimum ten character password. These passwords must be stored in a physically secure environment (e.g. signed envelope, locked away). Their management must be under the following segregated control scheme:

- one set of people must deal with password creation;
- one set of people must deal with password access/release; and
- one set of people must deal with actual password use.

Passwords for high privilege accounts must only be released on the authority of an authorized issuer, whose signature must be checked against a list of authorized signatories. For emergency access, passwords could be released to pre-authorized personnel, but issue must subsequently be authorized by an authorized issuer at the earliest opportunity.

Passwords must be reset after use by the holder (not the user), recorded and placed back in the secure location.

Allocation of privileges to specific user accounts must be undertaken so that no one user has the sufficient combination of privilege to act as sole supervisor.

Supervisor or system manager (privileged) accounts may not be used for regular operational use as they have all possible privileges and their use is unaccountable.

2.2.5 Third Party Access

As Intranet/Extranet services become more important to the operating of the City, remote access by external parties is likely to increase. City agency assets must be protected against this threat by appropriate levels of control.

Third parties must be restricted to appropriate services and data. Interfaces must only permit authorized communications protocols, commands and services and must be restricted to present only the information related to that third party.

Data transfer between third parties must be initiated by a City agency system. In other words, information must be pulled into City agency systems rather than pushed by the third party.

2.2.6 Protection Against Unauthorized Access

Accounts must be automatically disabled after five login failures, requiring the administrator to explicitly reset the account before it may be used again. Persistent login failures must be written to the audit log and reviewed regularly by City agency information security personnel or Information Technology (IT) personnel. Operating system facilities, as well as, logging facilities built into the application must enable properly structured audit log reviews.

The City agency users' last logon time and date must be displayed each time they log on. This gives the users the chance to check that their account has not been used without their knowledge.

Systems under management remotely from a management station must raise an alert if accessed by their local terminal.

All application sessions must be terminated when the application is shutdown or if the application crashes, requiring re-authentication to continue processing. The business owner may consider restricting authentication outside of normal working hours depending on the required level of availability and the perceived risk.

Simultaneous sessions per user ID from different workstations may not be permitted except where a justifiable business need can be demonstrated.

Announcements given by the system prior to authentication may not invite the user to login or reveal information about the application or about the City agency. From a legal standpoint, attackers can claim that they were invited to break into the system, if the login screen states, "Welcome." Announcements given by the system prior to authentication may not provide any indication of what the application does as this could provide an attacker with valuable information. Nor may it identify the City agency. Only the following message must be presented prior to any authentication request processing:

Access to this computer is prohibited unless authorized. Accessing programs or data unrelated to your job is prohibited.

Unattended workstations must be secured to prevent unauthorized use of accounts. Authenticated sessions must time-out after a predefined period of inactivity, requiring the user to re-authenticate. A recommended minimum time is fifteen minutes. This would normally be implemented by the operating system. Where users need to observe the application's output for long periods of time without direct input, the application session must drop into 'read-only' mode, requiring re-authentication to make changes to any data. Read-only mode may include scrolling through reports and access to non critical functions. It may not be appropriate to implement this control on trader workstations.

2.3 Client Security

The application's underlying environment must comply with all available platform specific security standards and be based on standard City agency builds. Logical access controls must be in place on the client operating system to restrict access to local processing.

Validation logic must be placed in the application interface to ensure validity of input data. This means that all data entry fields must have an appropriate underlying data type. Input validity checks, including range checking and checks against static data, must be performed at the point of entry. Checks must be applied to fields rather than forms, such that the user is requested to re-enter that field immediately after entry.

Mandatory data entry fields must be used to ensure referential integrity. As a minimum, the user may not be able to leave blank a field that will be used as a key. Referential integrity rules must be applied to deletion or amendment requests such that the request is denied if actioning the request would violate referential integrity rules (i.e. the rule may not simply be used to trigger an error message).

Pull-down lists must be used in favor of manual data-entry fields and options must be based on static data wherever possible. Where the user has the privilege to add new options to a pull-down list, semantic checks must be in place to ensure consistency of data. Where the user has the privilege to add/remove or amend options from a pull-down list, range checking and referential integrity checking must be in place to ensure integrity of data.

Input data must be validated against static data, where possible. An override facility must be provided for field validity checks where the check is intended as a guide rather than a rule. Facilities for changing the parameters used for range checking, including pull-down options, must be available to the system administrator. The administrator must also have the facility to change parameters for syntactic and semantic checking.

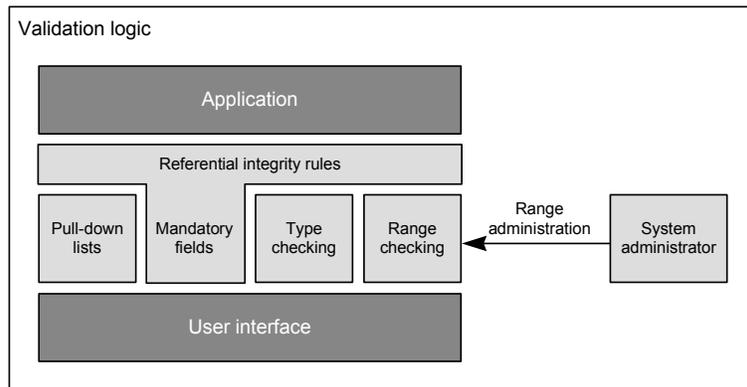


Figure 5. Validation logic

Applications may allow the administrator to take over the user session using a remote control facility. If such a facility is required, the workstation must authenticate the management system before it allows itself to be controlled. Then, activity must be logged and the remote activities must execute under the privileges of the management systems, rather than the privileges of the current user. Access to systems from a management system may not be able to circumvent defined logical access controls on that system.

2.4 Server Security

Applications may allow the administrator to take over the user session using a remote control facility. If such a facility is required, the workstation must authenticate the management system before it allows itself to be controlled. Then, activity must be logged and the remote activities must execute under the privileges of the management systems, rather than the privileges of the current user. Access to systems from a management system may not be able to circumvent defined logical access controls on that system.

- Removal of unnecessary system or administrative software;
- Adequate restrictions on system software and operating system configuration files;
- Removal of any hidden options for system administration use;
- An approved anti-virus agent;
- An approved event monitoring agent;
- Approved configuration and default permission;
- Appropriate service packs and patches;

The application server must reside in a physically secure location, preferably in a locked cabinet in a secure data center.

For applications with client-server architecture, the application may not assume that users will always use the client software to connect to the application. A suitable layer of security must exist at the server end of the client-server relationship to prevent the user from gaining inappropriate privilege by connecting to the application server directly (e.g. using Telnet).

Access to database query languages (e.g. SQL), must be restricted to the database administrator. Users may not have direct access to any query tools. Rather, a set of relevant reports must be made available. That is, users may not be able to write their own queries or reports because if there is a need for a report, it must be written by a professional software engineer and made available to all users. Database reports and queries must be subject to the same level of testing as any software component. As a baseline, report output must be checked for accuracy and a minimum of documentation made available to users.

2.5 Fault Tolerance and Contingency

The maximum level of fault tolerance within the base configuration must be enabled. The City agency must avoid single points of failure. Disk storage must utilize failure tolerant techniques such as shadowing, mirroring, duplexing or RAID type technology.

For systems which are critical according to the results of the Information Security Risk Assessment, application processes, including individual transactions, must be replicated to a mirror system, which would act as a contingency system in the event of failure. All application level client processes must be automatically authenticated by the server using an approved Public Key Infrastructure (PKI) scheme, if available. PKI is further discussed at the City's *Information Security Directive: Public Key Infrastructure*.

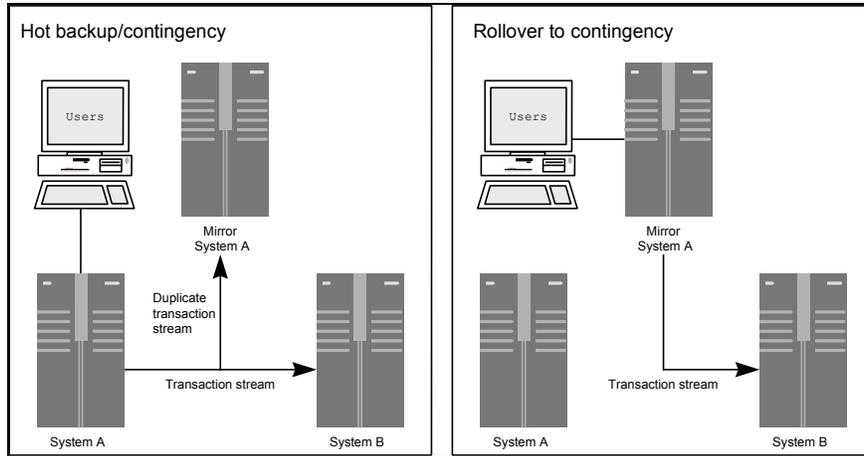


Figure 6. Redundancy

A Disaster Recovery Plan (DRP) must be developed by the City agencies and regularly tested and matched against the relevant Business Resumption Plan. Business Continuity is discussed further at the *Information Security Directive: Business Continuity*.

The same security controls that apply to the production environment must be applied to the contingency environment, both before and after roll-over to contingency.

2.6 Backup and Recovery

All managed data stores, City agency system data and configuration files must be backed up on a regular basis at a frequency agreed with the information owner. In the event of a data corruption or a physical problem (e.g. a bad disk), it is important that data files, as well as, configuration files, executable software images and account details, can be restored.

High confidentiality information on backup media must be encrypted or otherwise physically secured to prevent unauthorized disclosure.

Refer to the City's *Information Security Directive: Business Continuity* for more information.

2.7 Application Output

All physical output must be protected against disclosure. Information systems are typically configured to restrict access to data based on the user's role and privileges. These controls are not available on printed output so an alternative method of protecting the information is required. As a minimum, all reports must include the name of the report, the name of the user, beginning and end of report banner pages and page numbers. Sensitive reports (those which contain confidential data) must include a privacy warning banner and must prompt the user when printing has finished. No reports must be produced where there is no relevant data to be reported.

2.8 Data Integrity

Data which can be referred to by a number of systems must be protected against unauthorized modification and controls must be in place to ensure its accuracy. Corrupt or missing data could have a significant impact on the systems that use it. Data repositories must be subject to the same level of control as all the applications that use them.

Data must be held in common repositories and protected by a suitable access control mechanism. These repositories must be securely managed and subject to change controls, including full documentation, according to a standard convention.

For applications which are critical (according to the results of the Information Security Risk Assessment)—and which rely on data stored in common depositories, the repositories must be replicated so as not to form a single point of failure for any of the applications that use them.

2.9 Transaction Security

Transactions must be protected against failure (availability), modification (integrity), fabrication (integrity) and disclosure (confidentiality).

Security controls must be applied to whole transactions throughout processing. All transactions utilizing messaging services must include appropriate controls to ensure peer application processes are authentic and that processing across those entities takes effect in an appropriately secure manner. Message sequence numbers must be used to prevent fabrication, repeated messages or to prevent out-of-sequence messages from being processed. In this event, an alarm must be raised to the administrator. Numbering messages or transactions makes them more difficult to spoof.

All transactions must be logged to facilitate database reconstruction. This would normally be part of the database build, although the facility would need to be enabled. Transaction logs must be protected against unauthorized disclosure and modification by limiting access to the log files.

A security domain is the logical collection of application components and user entities under a single security administration. All the components of a distributed application must exist in a single logical security domain.

For critical systems, which are identified by an Information Security Risk Assessment, each element of a distributed transaction must be cryptographically protected for integrity or confidentiality (as appropriate) from source to destination. Controls must be in place to validate and acknowledge transactions. Where possible, transactions must be digitally signed using public key encryption technology. For more details on encryption, refer to the City's *Information Security Directive: Encryption*.

2.10 Information Pollution

Information pollution is the ripple effect that occurs when inaccurate or corrupt data flows between systems. This often happens in large organizations where many systems are linked and automated data feeds flow between systems without an appropriate level of control.

To avoid information pollution, the City agency must implement the following directives:

- Batched input must be subject to the same controls as manual input.
- Field checks must be performed on the same data fields and the batch must be manually checked and released. If this is not possible, a summary report must be produced and reviewed regularly.

A data corruption or inaccuracy can pollute the workflow like a virus.

Here is an example:

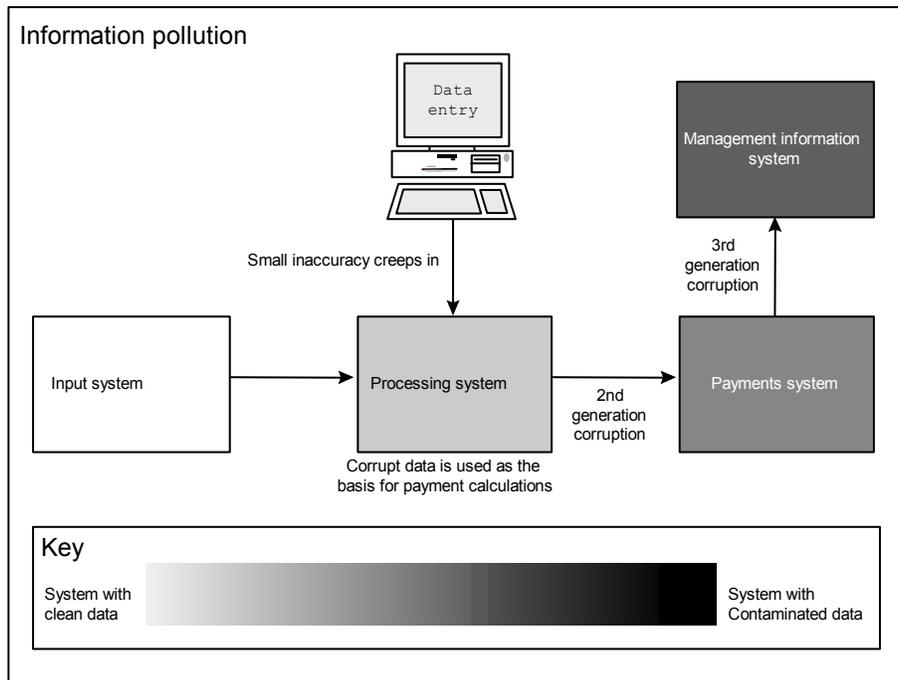


Figure 7. Information Pollution

2.11 Workflow Transactions and City Agency Business Processes

The implementation of a City agency business process or the Information Technology (IT) component of a City agency business process must be controlled to ensure the complete and correctly authorized processing of that information through the full process cycle. Correlation with the business process and the IT process must be maintained. All implementations of City agency business processes using transaction based information processing must be fully documented in the context of that City agency business process.

Critical workflow messages must be protected against unauthorized disclose or modification using cryptographic techniques (e.g. SSL). For more details on encryption, refer to the City's *Information Security Directive: Encryption*.

2.12 Application Interfaces

Sessions between applications must be mutually authenticated and privileges assigned to that authenticated session dependent on membership of privilege groups. Specifically, systems must authenticate the identity of the systems they communicate with during processing or data transfer. Automated reconciliation procedures must be in place at both ends of the application-to-application interface.

The actual interface (i.e. network) link from other systems must be secured according to available network security standards. Connections to external networks must be explicitly authorized and must take place through a firewall. Controls must be in place to ensure that information received from the Internet, or from systems that take their data from the Internet, is filtered or otherwise protected against information pollution. As a baseline, data from non-trusted systems or sites must be crosschecked prior to assimilation.

Application to application logical links must be subject to mutual strong cryptographic authentication. Information systems classified as critical may not provide data to systems classified as non-critical unless the information provided is explicitly classified as non-critical.

Interfaces from external systems must provide a level of assurance of the authenticity and accuracy of the data received. Information may not be relied upon for City agency business processing unless its origins are known and its source trusted.

Equally, information passed through interfaces to external systems must be protected against unauthorized modification and disclosure. Information fed to external systems must be classified as critical and appropriate controls must be applied.

Information may not be received by a critical system from a non critical system, unless the non critical system is demonstrably compliant with enhanced controls, as defined by CISAFE Information Security directives or standards.

Information may not be provided to systems with a higher Information Security Risk Assessment classification or to systems that are not demonstrably compliant with CISAFE Information Security directives and standards.

2.13 Interfaces to External and Supplier Systems (Extranets)

Communications links between City agency systems and external parties, including external entities and suppliers must be controlled in accordance with their business criticality. All external connections must be mediated by a firewall, with appropriate restrictions in place. That is, sessions must be restricted only to appropriate services and an explicit IP routing table must be in place.

All user sessions and application entities must be authenticated, preferably using strong authentication techniques. All data must be encrypted from point-to-point and digitally signed using an approved encryption mechanism.

2.14 Cryptography and Encryption Directives

Information classified as high criticality according to the results of the Information Security Risk Assessment must be encrypted when outside of the physical or logical access control system. This may include application level encryption, as well as, network level encryption.

Only approved cryptographic algorithms, protocols and third party products must be used. All encryption algorithms used must be explicitly approved by CISAFE. This also applies to the selection and use of cryptographic protocols for key management, key distribution, entity authentication, message authentication, non-repudiation and various modes of encryption.

Public key technology can be used to digitally sign a message in order to prove the identity of the transmitter. Messages can be hashed and an acknowledgment message sent back to the originator. This technique is called non-repudiation (i.e. the intention being that the recipient cannot claim that they did not receive the message). This system only works if the physical identity of the person issuing the public key is known, which is why advertised public keys must be protected from unauthorized modification. Certification authorities certify public keys as authentic to assure the identity of the owner.

As technology evolves and high speed processing becomes cheaper, encryption technology becomes more susceptible to brute force attack whereby the attacker tries every possible encryption key until the correct key is obtained, thereby allowing the message to be read. This is why encryption keys need to be sufficiently long to make it computationally unfeasible to determine the key for as long as the message needs to remain confidential. The longer the key, the longer it takes to break it. Keep in mind, the time taken to break a key continues to shorten as technology evolves and as fast machines become cheaper.

The way that encryption keys are managed is at least as important as the strength of the encryption algorithm used and the key length. Keys must be protected against unauthorized modification. Keys must be randomly generated and protected against disclosure. In the case of key exchange, the data encryption key must be different to the message authentication key and must be changed for each message. It is also important to ensure that users cannot encrypt information without making the encryption keys available in their absence. Encryption keys must be held under an internal secure key recovery scheme which must include dial control and auditing.

Encryption and Public Key Management controls are described further in the City's *Information Security Directives: Encryption and Public Key Infrastructure*.

2.15 Denial of Service

Denial of services attacks affect the availability of systems and tend to be the most difficult to prevent. Typically, there will be a number of known vulnerabilities associated with each platform at any given time. Attacks tend to be coded into easy-to-use modules, which invariably appear on the Internet for general consumption. When the manufacturer finds out about the vulnerability, they must issue a patch or a software upgrade to plug the hole. Patches and software upgrades must be applied in a timely manner as part of the change control process and in compliance with the City's *Information Security Directive: Change Control*.

In order to limit the effect of denial of service attacks, the City agency must build performance monitoring into the service structure. A deviation from the agreed response time must be treated in the same way as system failure and appropriate contingency must be invoked.

2.16 Audit / Management Trails

Audit/Management trail functionality is available in most operating systems that dynamically record activity. The review of audit trails must be segregated from normal administration functions, as must security administration. Typically, CISAFE would review the security logs and audit trails as part of their event monitoring activity, although those logs must also be available to the system administrator. A City agency approved security agent must be deployed to interrogate system logs.

Audit logs must be protected against unauthorized disclosure and modification with appropriate file permissions and kept on-line for at least thirty days. It is advisable to take this information off-line regularly as it tends to consume disk space rapidly. Ideally, audit log data must be written to an external system or storage unit via a one-way link. This has the advantage of not filling up storage space on the production system and also prevents users from modifying or destroying data.

The off-line retention of audit logs must be guided by audit, City agency business and regulatory requirements. As a guideline, it is suggested that audit logs must be held on-line for thirty days and off-line for three months. Particular rules apply to systems that hold personal data. For these systems, specific advice must be sought from CISAFE. The City agency must require application level logging for transaction reconciliation purposes. Low-level application hooks must be placed within the application that facilitates the development of audit tools to capture internal information. The use of such tools and access to such hooks must be secured against unauthorized use. Typically, this information would be available through the application interface and would be restricted to authorized personnel. Where applications interact and interface to other applications, it may be necessary to correlate that information as part of the review. In this case, the audit logs must identify the system(s).

2.17 Configuration Management and Change Control

Unauthorized and unscheduled changes can impact system performance, present security vulnerabilities and complicate their own replication if the system crashes. A well-controlled change control and configuration policy is a City agency business requirement. Change control must be in place to ensure that software fixes are rolled out in a controlled way and that changes to user privileges do not impact the production environment.

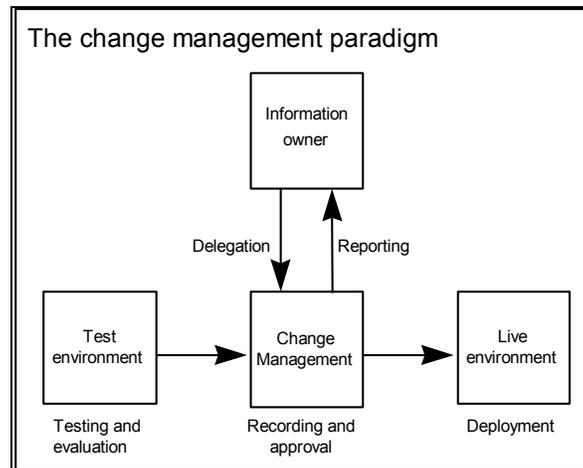


Figure 8. The Change Management Paradigm

For this reason, configuration files must be held on the application server rather than at the client workstation. Configuration files specific to the user must be held in the user's home directory on the application server or another central server. If configuration files need to reside on the client workstation, they must be incorporated into the user's standard build.

Automated configuration management systems are available. These systems record the configuration of application systems at different levels of granularity while maintaining the overall configuration. Tools are also available that allow the administrator to compare the application to a benchmark software image.

As a baseline, all unauthorized changes to system software or configuration files must be audited and all software development resources, including libraries, source code and executables, must be held under the control of a software configuration management system.

Remote reconfiguration or remote operation commands must only be acted upon subject to cryptographic authentication or at least through an initial cryptographic authentication exchange to establish the session. Management communications incorporating sensitive information, such as passwords, must be encrypted to prevent unauthorized disclosure.

The management of a system may not decrease the level of security control. Applications must be constructed to allow secure management. All management messages (e.g. commands and requests) must be authenticated to some degree. The identity of the source, as well as, the content of the message, must be authenticated.

Change Management controls are further discussed in the City's *Information Security Directive: Change Control*.

2.18 Object Orientation

Security controls must be applied to objects that comprise the application as well as the application itself. All object libraries must be secured by an appropriate access control mechanism. All production objects must reside in a suitable object repository and must be subject to change control and reuse of objects must be controlled via this repository.

2.19 Data Warehousing

Entity Relationship modeling (ER) is a logical design technique that seeks to remove the redundancy in data and provide a model for storing data. Dimensional modeling (DM) is the name of a logical design technique often used for data warehouses. It is different from, and contrasts with, ER. Dimensional modeling presents data in a standard framework. Instead of multiple joins across tables, data is presented in dimensional models, each with one table and a multipart key, called the fact table, and a set of smaller tables called dimension tables.

More information, including security controls for data marts and data mining tools, will be included in the next release of this directive.

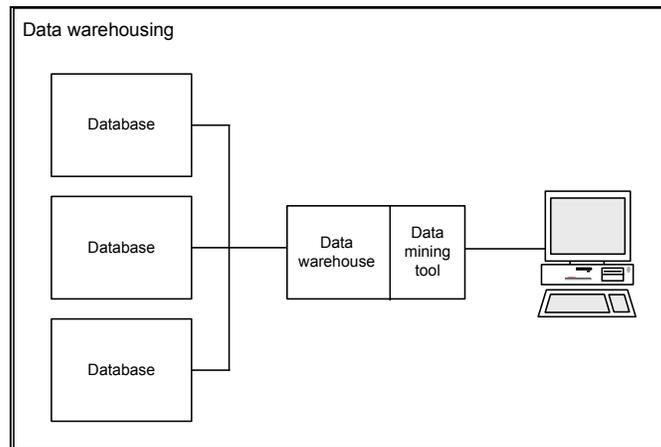


Figure 9. Data Warehousing

2.20 Common Security Environments

Common security APIs (Application Program Interface) must be used to integrate security services into the application. Use of APIs must be controlled using application authentication and authorization. Apart from that, the application must use security facilities available in the underlying Operating System.

2.21 Third Party Software and Vertical Applications

Vendor support of City agency business applications must be authorized by the appropriate information owner and be established so as to adequately contain that access to the system concerned for approved support activity. Vendor access must be provided through a secure network interface point (i.e. configured to strongly authenticate the vendor and to ensure that their access is restricted to relevant systems).

Access or network controls on the target system must prevent the vendor from attempting access to other City agency systems from the target system. The vendor must be given a dedicated support account rather than a standard high privilege account. On top of that, all use of the dedicated support account must be monitored.

All off-the-shelf software must be supported by a current vendor-support contract so that City agencies always have recourse must problems emerge. Off-the-shelf software must be checked for compatibility with all relevant standard builds before being purchased.

Third-party software must be subject to the same controls and must adhere to the same Information Security directives and standards as all City agency applications. CISAFE can assist in a review of potentially business-critical software prior to procurement and deployment.

Software may not be downloaded direct from the Internet in the instance that the software would be unsupported and/or may contain bugs or malicious code. In addition, applications may not mandate a significant change to the workstation or server configuration.

The City agencies may not use software that is not supported by vendors. There may be unforeseen problems with the software including subtle bugs and underlying vulnerabilities. All production software must be licensed. Shareware, freeware and evaluation software may not be used, even if it appears to have adequate functionality. Third party software must be evaluated prior to procurement.

2.22 Documentation

Documentation is often overlooked, especially when project deadlines are tight or when software is evolved rather than designed. Lack of documentation presents a significant information risk in that software becomes a static black box. The classic problem occurs when the original developer, who is also the second line support, leaves the organization. Typically, the software cannot be redeveloped or supported properly when it falls over, as all software does. Suddenly, the business is left without an application which they did not realize they relied on. A minimum level of documentation must therefore be available. Program designs must be available and code must be commented. The City agencies must make available the operating procedures to all operators.

With respect to full production systems, Service Level Agreements (SLAs) must be in place between the City agency information owner and all internal parties that support the application or its environment. This gives the City agency business recourse if there is interruption of service.

Relevant documentation must be made available to users to facilitate use of the software. It is important to draw the distinction between what facilities the system provides (in City agency business terms), how to use it (in the form of individual procedures), and how the system works (a technical guide).

3. Application Design Controls

3.1 Development Environment

The City agency application development team must deploy a software development methodology (e.g. waterfall, incremental, or spiral) that must be approved by the City agency management. The software development methodology must be documented and provide for User Acceptance Testing (UAT).

Access to software development resources must be restricted to authorized developers only under the direction of the project or production support manager. Amendments to resources must be logged and old versions of resources must be kept for at least six version iterations.

3.2 Use of CASE

Computer Aided Software Engineering (CASE) refers to any automated tools that assist with the development lifecycle. Typically, a CASE tool would convert design into code. Security controls must be considered at the design stage for any application, although this is especially important if CASE is to be used.

A level of manual checking must be introduced to ensure the validity of generated code, including version updates. Where CASE tools are used to reverse engineer an existing application, an additional level of manual checking must be in place to ensure validity of code and the application must be formally tested prior to deployment.

CISAFE is available to assist in the evaluation of information security aspects of CASE tools intended to be used to develop critical applications.

3.3 Application testing

The software development methodology is often critical to the success of a project. However, if a system came to the production environment without being fully tested, errors could creep into data causing significant financial loss to the business.

As a guiding principle, software must be adequately functionality-tested prior to user acceptance testing and deployment into the production environment. The testing procedure must include a facility to review errors and amendments throughout the development lifecycle.

Prototyped applications must be formally tested prior to live use (i.e. there must be discrete development and deployment phases). This could be in the form of parallel processing, where the existing system or procedure was used in parallel with the new application.

Testing must be performed on a dedicated test system away from the production environment. Live data must be sufficiently modified if it is to be used for testing. This would enable complete testing without risk to the production environment or any live data.

User Acceptance Testing (UAT) is an important part of the software development process. It allows the sponsor of the system to evaluate it. Clearly, users need to feel comfortable using the system and need to

develop their skills before the system goes live. On top of that, minor problems need to be ironed out before the system goes to production. UAT must include stress and volume testing and the backup and recovery plan must also be tested.

City agency business critical applications must be more formally tested prior to user acceptance testing or deployment. Typically, a formal test plan would be constructed and adequate slack would be built into the project plan for redevelopment.

Copies of live data used for testing must be desensitized. As a minimum, names and other identifiers must be removed from personal data. Production data may not be provided to third parties and all copying of live data must be recorded, including the reason it was copied.

3.4 Security Testing

This section only applies to applications classified as critical by the results of the Information Security Risk Assessment.

Critical systems must be penetration tested prior to going live to ensure that their security arrangements are adequate. The schedule and scope of the penetration testing must be agreed upon with the information owner and performed by technical staff who are not part of the development team. The testing must include the objective of testing and whether the Information technology (IT) custodian or security review staff detected the attack. The results of the penetration testing must be reviewed by the City agency information owner and CISAFE.

3.5 User Interface Ergonomics

3.5.1 Interface Design

Application interfaces must be designed to be intuitive and consistent. If not, poor interface design could affect the user's decision-making process and therefore integrity of data. Too many options, inconsistencies throughout the interface or text, which is difficult to read, may cause an error to creep into the critical workflow.

Usability must be evaluated as part of the User Acceptance Testing (UAT) phase because it is very difficult to guess a user's reaction to an interface. Applications must be evaluated for usability, ease of understanding and intuitiveness. There must be enough slack built into the project plan to allow for redevelopment after UAT.

The application interface must be predictable and intuitive. For example, the ESCAPE key may not be used to confirm actions as the user might expect ESCAPE to mean quit. The classic test for interface usability is to give the user little or no instructions and no hand holding, and simply to observe their behavior. The results of the test may be used to help design the application interface.

Operations, function keys, icons and menu options must have a consistent meaning throughout the application. Options that change functionality between menus are confusing to the user.

Complex operations must be supported with on-screen instructions which follow a standard format and use consistent language throughout the application. User memory-load must be minimized such that instructions remain on the screen throughout the operation. This is commonly called hand-holding. Error messages and user dialog must be easy to understand, simple and positive (Figure 10).

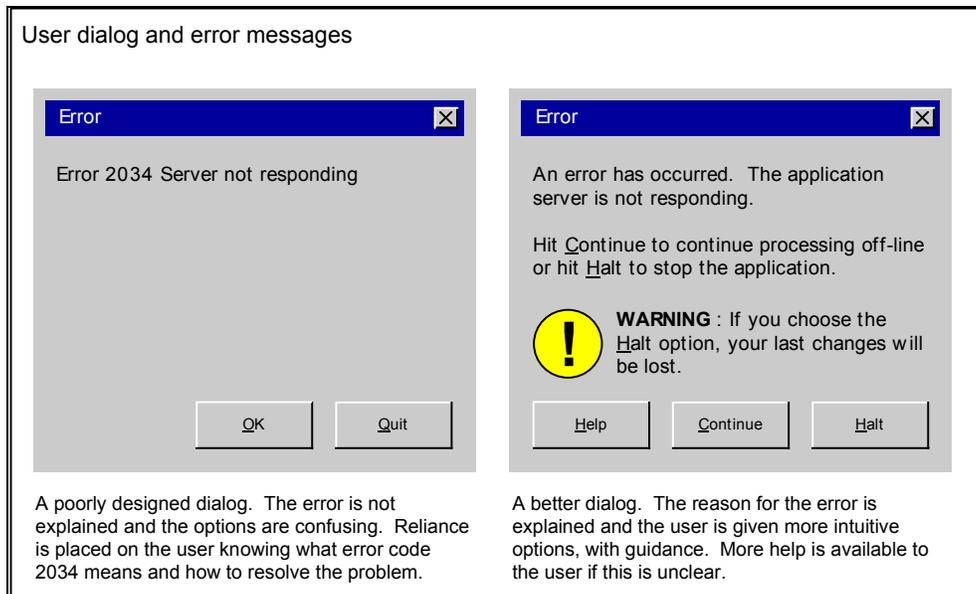


Figure 10. Dialog Boxes

3.5.2 Interface Controls and Restrictions

An “undo” function must be available for relevant actions. Where an undo function cannot be implemented and where inadvertently using the requested function would cause significant damage to data, an “are you sure?” error message must explain the implications of using that function and request confirmation. The “are you sure?” message tends to be overused, especially by popular “user friendly” vertical applications. If the user is presented with this dialog too often, there is a temptation to ignore it.

All screens must have a consistent look and feel, including fonts and colors used, within each application context. This has the benefit of providing the user with visual cues, as well as giving the overall feeling of quality. For the same reason, all messages directed to the user must be clear and consistent. Error messages must be clear and free of codes and must report as much detail as possible about the error. Error messages must include the cause of the error, the record or operation that the error occurred on and what the user must do to recover. Because City agency staff has a diverse range of first languages, simple and direct wording is advised.

The user must be able to customize reports, change the font size and add icons to toolbars, where appropriate, but may not be allowed to affect the functionality of any command or function. While users expect to be able to customize their environment, it is not advisable to allow the user to make the font the same color as the background.

Synthesized speech may not be used to communicate sensitive information. Apart from annoying other users, it is difficult to ensure that “spoken” information is not overheard.

4. Application Administration

4.1 Roles and Least privilege

A role is a logical definition of a user's job function and associated privileges within the application context. Roles allow privileges to be assigned to users more easily using the concept of user groups. Role based systems tend to be easier to manage, easier to administer and tend to have fewer authorization problems. The following directives are an overview of the role based systems concepts.

Access to application functions, system commands and data must be allocated to groups rather than individual users IDs. Each role must have a number of groups associated with it, forming a hierarchical model.

A full definition of users roles and their associated privileges on each system must be documented and held in a central location, preferably on a central directory server. This makes management easier and allows periodic checking. Account request forms for the application must include a role field, which the requester would use to request privileges, rather than indicating specific privileges.

If a central directory server is not being used, all users and their associated roles and privileges must be fully documented in a security plan. This plan must be explicitly approved by the City agency information owner and subject to regular review by CISAFE. This is not as arduous as it may first appear. The roles must be defined initially and users associated with an appropriate role at creation time.

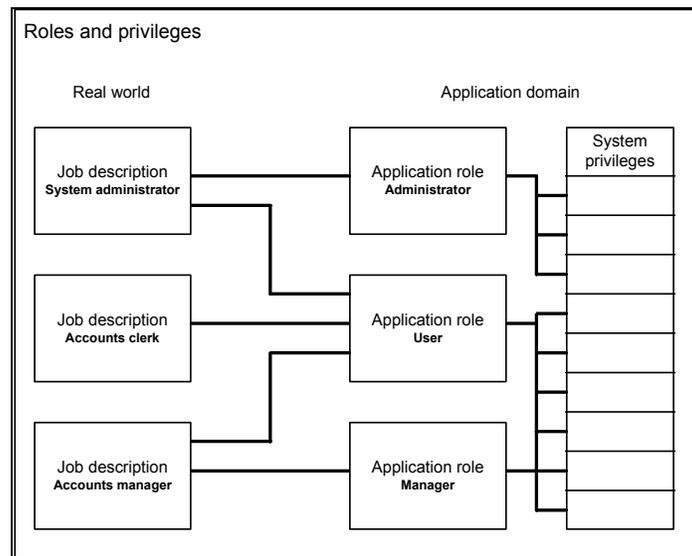


Figure 11. Roles and Privileges

Each user must only have the appropriate functionality and information required to complete their duties. The concept of least privilege is the concept of explicitly denying all rights and only granting those that are required as part of the user's role (i.e. the default must be "no"). Unfortunately, the reverse is often applied when administrators try to remove potentially dangerous privileges. This approach rarely works well.

Application Security Directive	Directive: D.4.4
Issued: April 29, 2003	Page 25 of 34

Users must be trapped into menu structures and prevented at the application level from accessing functionality or data objects which are not required as part of their role. Users may not be able to break out of the application environment or navigate to a command line because it would be difficult to control the environment. Access to data must also be restricted at the system level, preferably using the Operating System's built-in authorization functionality.

Access to users in remote or public locations must be specifically considered and the very minimum of privilege allocated to those users. If possible, read-only access must be allocated. Typically, remote access would also be more stringently controlled than local access.

Temporary or contracted users must be allocated accounts with a limited lifetime, such that the account expires on the day they leave the organization.

Access to system utilities, operating system software and any operating system command line interfaces must be restricted to the system administrators group. Administrative commands must be accessed via a user interface. Access to security administration facilities must be restricted to the security administrators group. Users may not be able to delegate their permissions or group membership to any other user.

4.2 Segregation of Duty

Traditionally, the City agency system administrator has been viewed as the overseer. This meant that the task of keeping the system running, assigning rights, disseminating passwords and of monitoring the system for attacks was all rolled into one. In a modern government environment, the City agency information owner owns these systems and has a requirement to monitor and control the administrator's activity like any other user. For this reason, system administration, security administration and security monitoring must be defined as distinct groups. In this model, it is important for the security administration group to be restricted to account management and for the security monitoring group to be restricted to monitoring software and audit logs.

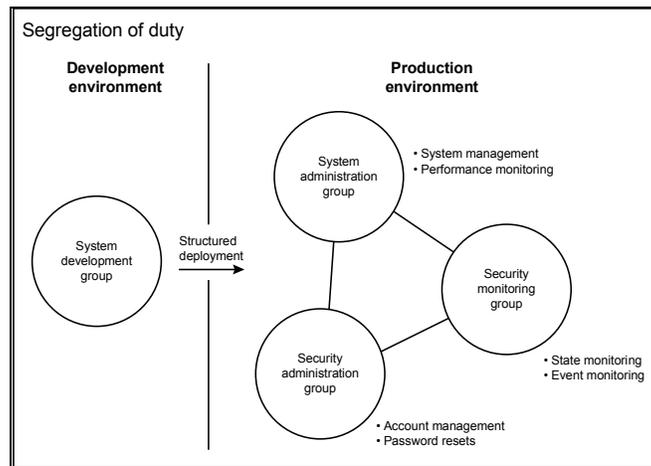


Figure 15. Segregation of Duties

Users must be prevented from performing more than one function on the same critical transaction (e.g. segregate "create" and "release"). Modification or creation of high integrity information and release of highly confidential information must be under segregated control.

Development and support must be defined as separate roles and permissions must be granted accordingly. This particularly applies to third-party or vendor support, where the application is directly supported by an external entity. The development and live systems must be separate and software must be ported to the live system in a controlled way (i.e. via change control). If developers are given full access to live systems, there may be a temptation to make ad-hoc changes to the live system on-the-fly thereby bypassing change controls. If a bug was introduced into the live system, data could be subtly affected before the problem was diagnosed. In this scenario, the system would be unavailable until the problem was fixed. The situation compounds if developers leave the organization. If the system and its configuration are not fully documented, the system becomes a liability.

User support must be performed by a dedicated support team, rather than the developers, as the skills required are quite different. Typically, the business owner would demand a service level agreement and support model, including agreed hours of cover. The development team may not be geared up to meet this requirement.

Application Security Directive	Directive: D.4.4
Issued: April 29, 2003	Page 27 of 34

Where segregation of duties cannot be enforced within the application context, then procedures must be in place which clearly define each party's role and associated privileges.

4.3 Security Administration

Security administration includes account creation/deletion, password resets and assignment of roles and permissions, commonly called authorization.

All requests for new accounts, requests to delete existing accounts or requests to change a users' privileges must be explicitly authorized by the City agency information owner or a nominee (i.e. the group that own the risk presented by creating a new account must be knowingly accepted by the City agency information owner prior to the account being created). For this reason, requests may not be accepted simply because they have been signed by a senior person.

5. Monitoring

5.1 Event Logging

Event monitoring is the process of monitoring a system for actual break in attempts and inappropriate or unauthorized activity. An independent daily audit review of activity on the system must be performed by the City agency and a summary report published to the information owner. Events monitored must include:

- Excessive failed logon attempts;
- Logon out of working hours;
- Unsuccessful attempts by users to change their own password;
- Unsuccessful attempts to access resources;
- Administrator or highly-privileged account activity;
- Security administrator activity;
- Use of third party accounts;
- Additions, deletions and modifications of users;
- Completeness of audit trails; and
- Monitor software changes and enhancements;

All logs must include a date, time stamp and workstation ID. Logs must be retained for as long as required on-line and for three months off-line. Logs relating to critical applications must use an authentic time source.

5.2 State Monitoring

State monitoring is the process of reviewing systems for deviation from security standards and unauthorized reconfiguration. Independent daily, weekly and monthly monitoring exercises must be performed by City agency security personnel and a summary report published to the appropriate system administrator. The City's *Directives* and *Standards* must be used as a basis for state monitoring activity.

The system administrator must implement any fixes recommended by the state monitoring report in a timely manner and report all changes to the City agency management.

6. Appendix A

6.1 Purpose

This *Information Security Directive: Application Security* defines the minimum baseline controls to be implemented for application security. It is intended to provide direction and security standards to City agency personnel who are developing and deploying computer applications.

This directive supports the City's *Citywide Information Security Policy* and is complimented by other detailed directives and standards that provide additional information. These directives and standards are referenced where appropriate.

6.2 Who Must Use This Directive

This directive applies to all City employees, contractors and consultants who develop and maintain City agency computer applications.

It is assumed that knowledgeable technical professionals will be implementing this directive. Detailed control procedures are not included in this document, but must be provided by the appropriate personnel to document supporting detailed operational procedures.

6.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

6.4 Document Convention

The conventions listed in the table below are used in this document.

Item	Convention	Example
Text entered by the user	Bold Courier New	Enter YES or NO
Text displayed by the system	Courier New	The system displays the following message: Process Complete.
Buttons, menus, menu items	bold Arial	Click OK to continue.
Field names	bold Arial	Select the Enable option.
Filenames	Courier New	Transfer the Webagent.conf file.
Path names and file locations	Courier New	Navigate to c:\tmp.
Keys	Uppercase	Press ENTER.
Single-click of left mouse button	<	< OK .
Single-click of right mouse button	>	> [Desired icon]
Double-click of left mouse button	<<	<< My Computer
Command to close the window	☒	☒
Selection from the Windows taskbar	Bold Arial items with an underlined character	Select <u>P</u>rograms

7. Appendix B -- Areas of Responsibility for Implementation of this Document

7.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policies, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

7.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

7.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the CIO (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Application Security Directive	Directive: D.4.4
Issued: April 29, 2003	Page 32 of 34

The TSC is responsible for supporting the *Citywide Information Security Policy*, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

7.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

7.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

Application Security Directive	Directive: D.4.4
Issued: April 29, 2003	Page 33 of 34

8. Glossary of Application Terms

This section provides common application related terms and definitions. For more general security terms, refer to the "Glossary of Information Security" section in the City's *Citywide Information Security Policy*.

None

9. References

- *Citywide Information Security Policy*
- *Information Security Directive: Authentication*
- *Information Security Directive: Business Continuity*
- *Information Security Directive: Change Control*
- *Information Security Directive: Encryption*
- *Information Security Directive: Host and Server Systems*
- *Information Security Directive: Public Key Infrastructure*
- *Information Security Directive: User Account Management*

The City of New York

Policy on Limited Personal Use of City Office and Technology Resources

This Policy, which has been approved by the Department of Information Technology & Telecommunications, the Department of Investigation, the Conflicts of Interest Board, and the Law Department, governs the limited personal use of the City of New York's ("City") office and technology resources by City employees. An agency may adopt agency-specific standards and procedures that are stricter, but not less strict, than this Policy.

I. GENERAL POLICY

City employees are permitted limited personal use of the City's office and technology resources if the use is not prohibited pursuant to this or another applicable agency policy, does not interfere with or otherwise impede the City's operations or employee productivity, and involves no more than a minimal additional expense to the City. City employees may engage in the personal use of the City's office and technology resources permitted by this Policy only at times that do not conflict with the employee's official duties and responsibilities and the employee is not required to perform services for the City.

The opportunity that the City is extending to its employees to make limited personal use of the City's office and technology resources is only a privilege and may be revoked or limited at any time. Moreover, this privilege is subject to monitoring and other restrictions that may from time to time be announced. This privilege does not create a right for any person to use any City property or resources for non-City purposes. Limited personal use of the City's office and technology resources is at the sole risk of the employee, and the City is not responsible for any loss or damages resulting from such personal use.

II. DEFINITIONS

- 1. "Office and technology resources"** includes but is not limited to: information technology, personal computers and related peripheral equipment, software, library resources, telephones, mobile telephones, pagers and other wireless communications devices, facsimile machines, photocopiers, Internet connectivity and access to Internet services, and email.
- 2. "Information technology "** means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

3. "Minimal additional expense" means that an employee's personal use of the City's office and technology resources is limited to those situations where the City is already providing equipment or services and (1) the employee's use of such equipment or services will not result in any additional expense to the City or, (2) the use will result in only normal wear and tear and will employ only small amounts of electricity, ink, toner or paper or, (3) the City has created mechanisms for employees to reimburse the City for the costs associated with their personal use and the employee makes such a reimbursement for his or her personal use. Examples of minimal additional expenses include occasionally making a photocopy, using a computer printer to print out a few pages of material, making a brief personal telephone call, sending a personal email message, or limited use of the Internet for personal reasons. Examples of mechanisms created for employees to reimburse the City include applicable agency policies regarding employees' reimbursement of the City for personal use of mobile phones and of long distance telephone services.

4. "Personal use" means activity that is conducted for purposes other than accomplishing official work related activity. Personal use under this Policy does not include any use that is unlawful, violates the City's Conflicts of Interest rules or other applicable rules and regulations, or is specifically prohibited by this Policy or another applicable agency policy.

III. UNAUTHORIZED PERSONAL USES

Employees are required to conduct themselves appropriately in the workplace and to refrain from using the City's office and technology resources for activities that are unauthorized by this Policy, another applicable agency policy, or applicable law, rule or regulation. Unauthorized personal use of the City's office and technology resources includes, but is not limited to, the following uses, all of which are prohibited:

- Any personal use of the City's office and technology resources that could cause congestion, delay, or disruption of service to any of the City's office and technology resources. For example, electronic greeting cards, video, sound, digital images or other large computer file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams can also degrade the performance of the entire network.
- Any personal use of the City's office and technology resources as a staging ground or platform to gain unauthorized access to other systems or in furtherance of unauthorized computer use.
- Any personal use of the City's office and technology resources in the creation, copying, transmission, or retransmission of chain letters, petitions or other unauthorized mass mailings regardless of the subject matter.

- Any personal use of the City's office and technology resources for activities that are inappropriate to the workplace or are prohibited by applicable law, rule, regulation or agency policy.
- Any personal use of the City's office and technology resources for the creation, downloading, viewing, storage, copying, or transmission of any material that is: obscene, sexually explicit or sexually oriented; hate speech; threatening; defamatory; known to be fraudulent; or ridicules others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation.
- Any personal use of the City's office and technology resources for furtherance of a non-City business or non-City employment, including, without limitation, consulting for pay, sales or administration of business transactions (not including personal finances), or sale of goods or services, including assisting relatives, friends or other persons in such activities.
- Any personal use of the City's office and technology resources to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited political activity.
- Any personal use of the City's office and technology resources to post agency information to external newsgroups, chat rooms, bulletin boards or other forums without explicit authorization.
- Any personal use of the City's office and technology resources in the unauthorized acquisition, use, reproduction, transmission, or distribution of any information, computer software or data, including, without limitation: private or confidential information about any individual, business or other entity including, but not limited to, medical information; copyrighted, patented or trademarked material or material with otherwise legally protected intellectual property rights; proprietary data; or export controlled software or data.
- Any unauthorized modification of the City's office and technology resources, including, but not limited to, loading personal software or making configuration changes.
- Any personal use of City office supplies, including, but not limited to, paper, pens and postage, other than a minimal use of supplies incident to the limited use of photocopiers, computers, telephones and facsimile machines allowed by this Policy.

IV. PROPER REPRESENTATION

It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in their official capacities as City employees when they are using the City's office and technology resources for non-City purposes. If there is a possibility that

such a personal use could be reasonably interpreted to be made on behalf of the City, the employee may not use the City's office and technology resources.

V. PRIVACY EXPECTATIONS

City employees do not have a right of privacy while using any of the City's office and technology resources, whether for official or personal purposes, at any time, including while accessing the Internet or using email. Any use of the City's office and technology resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous. To the extent that employees wish that their personal activities remain private, they should not use the City's office and technology resources for such activities.

By using the City's office and technology resources, whether for official or other purposes, City employees consent to the disclosure of the contents of any files or information maintained on or passing through the City's office and technology resources and of any logs or other records of the use of such equipment, including, without limitation, billing records.

By using the City's office and technology resources, whether for official or other purposes, City employees consent to the monitoring and recording of any such use with or without cause, including, but not limited to, records of access to the Internet and email usage.

Individual agencies may employ monitoring tools approved by agency senior management to ensure the proper use by their employees of the City's office and technology resources. Agency heads or their designees may access any electronic communications that are made using the City's office and technology resources.

VI. SANCTIONS FOR UNAUTHORIZED USE

Unauthorized use of the City's office and technology resources may result in: (1) loss of use or limitations on use of office and technology resources; (2) financial liability for the cost of such use; (3) disciplinary or other adverse personnel actions, up to and including dismissal; and/or (4) civil and/or criminal penalties.

VII. REIMBURSEMENT PROCEDURES

Employees are required to follow their respective agency's applicable reimbursement procedures for personal use of the City's office and technology resources.



**CITYWIDE INFORMATION SECURITY
ARCHITECTURE, FORMULATION & ENFORCEMENT
(CISAFE)**

**DEPARTMENT OF INVESTIGATION
CITY OF NEW YORK
CONFIDENTIAL**

Information Security Directive

**Electronic Communications – Version 1.
D 4.3**

April 29, 2003

Table of Contents

1	Overview of the Electronic Communications Directive	1
2	Allowable Use.....	2
2.1	Ownership	2
2.2	Allowable Users.....	2
2.2.1	<i>City Agency Users</i>	2
2.2.2	<i>Public Users</i>	2
2.2.3	<i>Transient Users</i>	2
2.3	Acceptable Uses.....	3
2.4	Access Restriction	5
3	Use of Specified Services	6
3.1	Web Pages	6
3.2	E-mail.....	6
3.3	Facsimile	7
4	Privacy and Confidentiality.....	8
4.1	Access without Consent	8
4.2	Privacy Protections and Limits	10
4.2.1	<i>Privacy Protections</i>	10
4.2.2	<i>Privacy Limits</i>	11
5	Securing the Electronic Communications	12
5.1	Security Mechanisms	12
5.2	Authentication.....	12
5.3	Authorization.....	12
5.4	Encryption.....	12
5.5	Backups and Disaster Recovery	12
5.6	Retention and Disposition.....	13
5.7	Audit Trail	13
6	Securing Specified Services.....	14
6.1	E-mail.....	14
6.1.1	<i>External E-mail Connectivity</i>	14
6.2	Facsimile	16
6.3	Voice Mail	16
6.4	Video Conferencing	17
7	Appendix A.....	18
7.1	Purpose	18
7.2	Who Must Use This Directive	18
7.3	Information Security Risk Assessment.....	18
7.4	Document Convention	19
8	Appendix B -- Areas of Responsibility for Implementation of this Document	20
8.1	CISAFE.....	20
8.2	DoITT.....	20
8.3	Technology Steering Committee	20
8.4	City Agency and Unit Management.....	21
8.5	Internal Audit	21

Electronic Communications Directive	Directive: D.4.3
Issued: April 29, 2003	

9 Glossary of Electronic Communications Terms 22

10 References 24

10.1 City Agency Policy and Directives 24

10.2 State of New York Statutes 24

10.3 Federal Statutes and Regulations 24

1 Overview of the Electronic Communications Directive

The City encourages the use of electronic communications for sharing information and knowledge and for conducting City agency business. City agencies must support and provide interactive electronic communications services and facilities for telecommunications, mail, publishing, and broadcasting. This document establishes directives on privacy, confidentiality, and security in electronic communications through voice, video, and data networks. This directive applies to all—

- Electronic communications resources owned or managed by City agencies
- Electronic communications resources provided to the City through contracts and other agreements with the City
- Contents of the electronic communications and the electronic attachments and transactional information associated with such communications
- Users and uses of City electronic communications resources
- City electronic communications records in the possession of City employees or other users of the City's electronic communications resources

This directive applies only to electronic communications records in electronic form. It does not apply to printed copies of electronic records or printed copies of transactional information. However, electronic communications records in either printed or electronic form are subject to federal and state laws and must comply with City policies, including retention and disclosure policies. This directive clarifies the applicability of existing law and the *Citywide Information Security Policy* and directives to all forms of electronic communication.

2 Allowable Use

City agencies must encourage the use of electronic communications resources and make them widely available to City agency employees. Nonetheless, the use of electronic communications resources are limited by the same restrictions that apply to all City property and by constraints necessary to provide reliable operation of electronic communications systems and services. To satisfy these restrictions and constraints, the City agency must reserve the right to deny access to its electronic communications resources. In general, the City agency may not be the arbiter of the contents of electronic communications. However, the City agency must protect users from receiving offensive electronic communications.

2.1 Ownership

This directive does not address the ownership of intellectual property stored on or transmitted through City electronic communications resources. Law and the City's *Information Security Directive: Copyright Compliance* govern ownership of intellectual property. The laws and directives apply to records in paper, digital format, or any other format.

Electronic communications records pertaining to the business of a City agency are considered the property of the City agency. This is true whether or not the City agency owns the electronic communications resources, systems, or services used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or otherwise record them.

City agency electronic communications resources, systems, and services are the property of the City agency. These include all components of the electronic communications physical infrastructure and any electronic communications address, number, account, or other identifier associated with or assigned by the City agency to individuals, units, or functions.

2.2 Allowable Users

2.2.1 City Agency Users

As authorized by City agency management and for purposes in accordance with the section "Acceptable Use," all City agency employees and affiliates, including those in contract or license relationships with a City agency, must be eligible to use City agency electronic communication resources and services.

2.2.2 Public Users

Persons and organizations that are not City agency users may only access City agency electronic communication resources or services under programs sponsored by the City or by a City agency for purposes in accordance with the Section "Allowable Use."

2.2.3 Transient Users

Users whose electronic communications merely travel through City agency facilities as a result of network routing protocols are not considered "users" for the purposes of this directive.

2.3 *Acceptable Uses*

Use of City agency electronic communications resources is allowable, subject to the following conditions:

Purpose. Electronic communications resources may be provided by a City agency in support of the City agency's mission.

Non-Competition. City agency electronic communications resources may not be provided to individual consumers or organizations outside the City agency except by approval of the City agency management. The services provided to these individuals or organizations must support the mission of the City agency and may not be in competition with commercial providers.

Restrictions. The City agency electronic communications resources may not be used for:

- Unlawful activities
- Commercial purposes not under the support of the City agency
- Personal financial gain
- Personal use inconsistent with the uses described in this section
- Uses that violate the City's *Information Security Directive: Copyright Compliance*
- Uses that violate the Conflict of Interest Board regulations

Representation. Users of electronic communications resources must abide by City and City agency policies on the use of the City or City agency's name, seals, and trademarks. Users of electronic communications resources may not represent, give opinions, or make statements on behalf of the City or any City agency, unless appropriately authorized to do so.

Endorsements. Users of City agency electronic communications resources must abide by City and City agency directives regarding endorsements. References or pointers to any non-City entity contained within City agency electronic communications may not imply City agency endorsement of the products or services of that entity.

False Identity and Anonymity. Users of City agency electronic communications resources shall not, either directly or by implication, use a *false identity* (for example, the name or electronic identification of another). However, a supervisor may direct an employee to use the supervisor's identity to transact City agency business for which the supervisor is responsible. In such cases, an employee's use of the supervisor's electronic identity does not constitute a false identity.

The City agencies must develop additional procedures for defining the circumstances under which pseudonyms and anonymous electronic communications are permitted.

A user of City agency electronic communications resources may use a *pseudonym* (that is, an alternative name or electronic identification for oneself) for privacy or other reasons, so long as the pseudonym clearly does not constitute a false identity. A user of City agency electronic communications resources may remain *anonymous* (that is, the sender's name or electronic identification is hidden) except when publishing web pages and transmitting broadcasts.

Electronic Communications Directive	Directive: D.4.3
Issued: April 29, 2003	Page 4 of 24

Interference. City agency electronic communications resources may not be used for purposes that could directly or indirectly cause excessive strain on any electronic communications resources or could cause unwarranted or unsolicited interference with others' use of the resources.

Users of City agency electronic communications services may not:

- Send or forward electronic mail chain letters or their equivalents
- "Spam" (that is, exploit electronic communications systems for purposes beyond their intended scope with widespread distribution of unsolicited electronic communications)
- "Letter-bomb" (that is, send an extremely large message or multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic communications systems and services)
- Intentionally engage in other practices, such as "denial of service attacks," that impede the availability of electronic communications services

Personal Use. Users of a City agency electronic communications facility or service may use that facility or service for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, the use does not:

- Directly or indirectly interfere with the City agency's operation of electronic communications resources
- Interfere with the user's employment or other obligations to the City agency
- Burden the City agency with noticeable incremental costs (City agencies must develop procedures addressing the reimbursement process when noticeable incremental costs for personal use are incurred.)

A City agency may have to disclose specified public records in compliance with law. In response to requests for such disclosure, it may be necessary to access electronic communications records that users consider personal. The City agency is not responsible for any loss or damage incurred by an individual as a result of personal use of City agency electronic communications resources.

Electronic Communications Directive	Directive: D.4.3
Issued: April 29, 2003	Page 5 of 24

Accessibility. All electronic communications intended to accomplish the business tasks of the City agency must be accessible to users with disabilities in compliance with law and City agency policies. Alternate accommodations must conform to the law and City directives.

Intellectual Property. The contents of all electronic communications must conform to the law and the City's *Information Security Directive: Copyright Compliance*, including laws and policies regarding copyright, patents, and trademarks. When the content and distribution of an electronic communication would exceed fair use, as defined by the federal *Copyright Act of 1976*, users of City agency electronic communications resources must secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.

2.4 Access Restriction

Access to and use of City agency electronic communications services or electronic communications resources, when provided, is a privilege accorded at the discretion of the City agency. This privilege is subject to the normal conditions of use, including procedures for initiation and termination of access. The manager of the individual electronic communications resource must establish these procedures.

In addition, access to and use of City agency electronic communications services or electronic communications resources may be wholly or partially restricted or rescinded by the City agency without prior notice and without the consent of the electronic communications user under the circumstances described in the Section "Access without Consent."

Restriction of access and use under such conditions is subject to established City agency procedures or, in the absence of such procedures, to the approval of the appropriate City agency management. Electronic communications resource providers may, nonetheless, restrict access to City agency electronic communications systems and services on a temporary basis as needed in emergency or compelling circumstances in order to control the emergency or prevent damage or loss. In compliance with the *Digital Millennium Copyright Act*, the City agency reserves the right to suspend or terminate the access to City agency electronic communications systems and services of any user who repeatedly violates copyright law.

3 Use of Specified Services

The City agency electronic communication systems must be used according to the directives established in the previous section, "Allowable Use." The following additional conditions apply for the use of web page publishing, e-mail, and facsimile:

3.1 Web Pages

The City agency must develop and document procedures to ensure that the following requirements are met for publishing web pages:

- *Identification.* Web pages may not be posted anonymously at addresses within a City agency domain (for example, www.nyc.gov). City agencies, in coordination with the City's Office of New Media, must establish procedures for identifying the City agency unit, program, and individual responsible for a web site.
- *Official City Agency Web Pages.* The City agencies must designate certain web pages as official City agency web pages. They must also develop mechanisms to identify which web pages do not represent the City agency. Any identification used to denote official web pages may not be used for other web pages.
- *Personal Web Pages.* The establishment of personal web pages is subject to approval by the City agency management. When personal web pages are allowed, the City agencies must establish standards that will enable users to recognize that the page represents the individual rather than the City agency.

3.2 E-mail

City agency electronic communications systems must be used for City agency business activities. Incidental personal use is permissible as long as it:

- Does not consume a noticeable amount of system resources
- Does not interfere with worker productivity
- Does not preempt any business activity

City agency electronic communication systems may not be used for charitable endeavors, private business activities, or amusement and entertainment purposes. Regardless of the circumstances, e-mail users are accountable for the content generated from their individual accounts.

E-mail users may not give access to their mailbox to other users unless it is required for business purposes (for example, a manager may delegate mailbox access to his or her administrative assistant). Authorized information sharing mechanisms such as message forwarding or public directories on local area networks must be used for data sharing.

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users must exercise judgment when forwarding messages. If possible, the e-mail systems administrators must disable blanket forwarding of messages to parties outside the City agency. Sensitive information may not be forwarded to any party outside the City agency without the prior approval of City agency management.

3.3 Facsimile

If fax machine operators can view the faxes, public fax routing services may not be used for sensitive information.

4 Privacy and Confidentiality

The City agency recognizes that principles of freedom of speech and privacy hold important implications for the use of electronic communications. The City agency respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that City agency records are accessible for the conduct of the City agency's business.

A City agency may not routinely inspect, monitor, or disclose electronic communications without the consent of the holder (that is, the electronic communications user). Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this directive, the City agency may deny access to its electronic communications services and may inspect, monitor, or disclose electronic communications under very limited circumstances as described in sections "Access Restriction" and "Access Without Consent." City agency employees may not seek out, use, or disclose personal information without authorization. In addition, they must take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise.

City agency contracts with outside vendors for electronic communications services must explicitly reflect and be consistent with this directive and other City directives related to privacy.

4.1 Access without Consent

Whenever possible, the City agency must obtain the electronic communication holder's consent prior to any inspection, monitoring, or disclosure of the contents of the holder's City agency electronic communications records. Exceptions to this directive can be made when—

- Required by and consistent with the law
- There is substantiated reason to believe that violations of law or of the *Citywide Information Security Policy* and directives have taken place
- Failure to act might result in significant bodily harm, significant property loss or damage, loss of important evidence of one or more violations of the law or of the *Citywide Information Security Policy* and directives, or significant liability to the City agency
- Failure to act during critical operations-related circumstances could seriously hamper the ability of the City agency to function

When, under the circumstances described above, the contents of electronic communications are inspected, monitored, or disclosed without the holder's consent, the following directives must be used:

- *Authorization.* Normally, inspection, monitoring, or disclosure of electronic communication contents must be authorized in advance and in writing by responsible City agency management personnel. Exceptions may be made in emergency or compelling circumstances, when time is of the essence and there is a high probability that delaying action would almost certainly produce bad results. Without authorization, inspections must be kept at a minimum, and the least action necessary must be taken to resolve the situation.
- *Emergency Circumstances.* Following an unauthorized inspection, monitoring, or disclosure, appropriate authorization must be sought without delay.
- *Notification.* At the earliest possible opportunity that is lawful and consistent with City agency Directives, a responsible authority or designee must notify the affected individual of the actions taken and the reasons for the actions taken.
- *Compliance with Law.* Actions taken under the paragraphs "Authorization" and "Emergency Circumstances" must be in full compliance with the law, including the laws listed in the "Reference" section, and the *Citywide Information Security Policy* and Directives. Advice of City agency management must always be sought prior to any action involving electronic communications stored on equipment not owned or housed by the City agency or whose content is protected under the federal *Privacy Act of 1974*.
- *Recourse.* City agencies must implement procedures for appeal of decisions regarding non-consensual access to electronic communications (whether under normal or emergency circumstances).
- *Annual Report.* In an annual report of non-consensual access to electronic communications, City agencies must identify the —
 - Number of requests for non-consensual access
 - Number of requests granted on emergency basis
 - Number of requests granted after approval
 - Number of requests denied
 - Reasons for the requests

This report must consist of summary numbers with no information about individual cases. The City Agency management must review the annual report and publish it.

4.2 Privacy Protections and Limits

4.2.1 Privacy Protections

Personal Information. Both federal and state laws provide privacy protection for the collection and use of information that personally identifies an individual. These laws apply to information collected and disseminated by electronic means just as they apply to records stored on paper and other media. A written release must be obtained prior to posting, broadcasting, or distributing an individual's information, picture, or statement.

Employee Information. The City agency must determine what employee information may and may not be released.

Electronically Gathered Data. Except when otherwise provided by law, users of City agency electronic communications systems and services must be informed whenever personal information other than transactional information will be collected and stored automatically by the system or service. It is recommended that the City agency provide mechanisms that enable users to terminate an electronic communications transaction without leaving personal data. In no case shall electronic communications that contain personal information, including data automatically collected by the use of "cookies" or other agents, be sold or distributed to third parties without the explicit permission of the individual. Any other distribution of such information shall be consistent with the *Citywide Information Security Policy*.

Telephone Conversations. In compliance with federal law, unless a court has given explicit approval, audio or video telephone conversations shall not be recorded or monitored without advising the participants. Emergency services must record 911-type emergency calls in accordance with federal and state laws and regulations. Participants must be informed when a call is being monitored or recorded for the purpose of evaluating customer service, assessing workload, or other business purposes permitted by law. City agencies that monitor or record telephone calls shall provide an alternative method of doing business with the City agency to clients who do not wish to be part of a monitored telephone call.

4.2.2 Privacy Limits

Public Records. Records of electronic communications pertaining to the business of a City agency, whether or not created or recorded on City agency equipment, are City agency records subject to disclosure under law or as a result of litigation.

Possession of City Agency Records. City agency employees are expected to comply with City agency requests for copies of records that pertain to the business of the City agency or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on City agency electronic communications resources.

Unavoidable Inspection. During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of City agency electronic communications resources and services. On these and other occasions, systems personnel might observe the contents of electronic communications. Except as provided elsewhere in this directive or by law, they are not permitted to seek out the contents or transactional information where not germane to the foregoing purposes or to disclose or otherwise use what they have observed.

Such unavoidable inspection of electronic communications must be limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to route an otherwise undeliverable electronic communication to its intended recipients. Except as provided above, systems personnel may not intentionally search electronic communications records or transactional information for violations of law or this directive. However, they must report violations discovered inadvertently in the course of their duties.

Back-up Services. Upon request, operators of City agency electronic communications resources must provide information about back-up procedures to users of those services.

5 Securing the Electronic Communications

The City agency must provide secure and reliable electronic communications services as described below.

5.1 Security Mechanisms

Unless otherwise authorized by provisions of this directive, no person must breach or attempt to breach any security mechanism used by the City agency to protect electronic communications services or facilities, nor any records or messages associated with these services or facilities.

5.2 Authentication

Electronic communications service providers must be knowledgeable of the technologies supported by the City agency and must implement authentication mechanisms in accordance with the City's *Information Security Directive: Authentication*. User accounts must be assigned whenever possible and managed according to the City's *Information Security Directive: User Account Management*. Each user account must be unique, and if the users have passwords, the passwords must be in accordance with the City's *Information Security Directive: Password Management*.

5.3 Authorization

Electronic communications service providers must implement and employ authorization technologies commensurate with the security requirements of the service, application, or system.

5.4 Encryption

Electronic communications records that contain sensitive data must be encrypted during transit across communications networks. Encryption must follow the City's *Information Security Directive: Encryption*.

Records subject to disclosure under law or required to be accessible for defined periods of time must be stored in an unencrypted format.

5.5 Backups and Disaster Recovery

To safeguard important data from damage, the City agency must develop sound backup procedures according to the City's *Information Security Directive: Archiving and Retention*. For example, all official City agency electronic mail messages, including those containing a formal management approval, authorization, delegation or handing over of responsibility, or similar transaction, must be copied, archived, or otherwise backed up and protected.

Furthermore, the providers of City agency electronic communications services must implement recovery practices adequate to ensure rapid recovery from security intrusions and service interruptions. They must do so in accordance with the City's *Information Security Directive: Business Continuity*.

5.6 Retention and Disposition

There is no single retention period for electronic messages. The value of electronic messages is based upon their informational content. Messages that are deemed to be records need to be retained for the same length of time that they would be retained if they were printed. Usually, the record status of an electronic record or message will be determined by the individual employee who created or received it. City agency employees are encouraged to acquaint themselves with the City's *Information Security Directive: Archiving and Retention*. It is a statutory requirement that all records be appraised and scheduled for disposition. If an existing City agency-wide schedule cannot be applied, then units within the agency must prepare a records schedule.

Electronic records must be maintained in a useable format throughout the approved retention period. As upgrades occur, electronically maintained records must be migrated to new software and storage media. If the electronic record is printed and retained in paper form, all envelope information must be printed and retained with the record.

As soon as the approved retention period has expired, electronic records must be deleted. Deleting records systematically and promptly limits City agency risks and significantly reduces space requirements for electronic records.

Approved retention times must also be applied to the backup tapes containing the copies of the electronic records. If the records continue to be maintained on the backup tapes beyond the approved retention time periods, the information still remains accessible and subject to discovery.

5.7 Audit Trail

The providers of electronic communications services must implement and employ cost-effective audit technologies and practices to help identify security violators and speed up recovery from security violations. The use of such audit technologies and practices may not conflict with other provisions of this directive, in particular those found in the section "Privacy and Confidentiality."

6 Securing Specified Services

The City agency electronic communication systems must secure the electronic communication services as described above in the section “Securing the Electronic Communications.” The following additional controls must be implemented for e-mail, facsimile, voice mail, and video conferencing.

6.1 E-mail

Using electronic mail (e-mail) to carry City agency information without additional controls may jeopardize the integrity and confidentiality of City agency information. Therefore, the City agency must implement the following controls:

- Redundant or default accounts must be removed from the e-mail systems.
- E-mail services may be used to carry sensitive data provided that the encryption and signing options are enabled (refer to the City’s *Information Security Directive: Encryption* for more details).
- E-mail user agents may not interpret or automatically execute content without user permission. They must be configured to ensure that they are not able to automatically launch e-mail attachments.
- If possible, filters must be used to—
 - Look for browser-based attacks, which exploit holes in HTML-aware email readers and web browsers
 - Check for attempted buffer-overflow attacks in malformed mail headers
- Anti-span mechanisms must be used, wherever possible, to block spam e-mail by detecting typical spam practices, such as incorrect “Reply To” addresses or “From” headers containing incorrect domains.

6.1.1 External E-mail Connectivity

Communication of City agency information via an external mail connection must occur through a managed secure gateway. The gateway must be used for mail exchange only. The number of gateways must be kept to an operational minimum, and the following controls must be implemented:

- Connectivity to the mail gateway must be direct, and City agency networks and systems may not be directly connected to those of third parties unless a firewall is in place.
- The gateway must ensure that the message information does not reveal information about the structure of City agency networks.
- Incoming mail must only be processed if destined for valid City agency addresses.
- The gateway must run on a physically secure server dedicated to the gateway function and may not offer any external interactive access. There must be no network routing or bridging between the internal and external networks except via a Mail Transfer Agent. Public switched external connections must, where possible, be initiated by the City agency mail gateway (that is, dial-out rather than dial-in connections).

- E-mail transfers via the gateway must take place through an e-mail screening that quarantines—
 - Messages with a binary executable attachment (such as, EXE, SYS, OVL, COM, DLL) including those enclosed, encoded, or zipped
 - Files that are greater than a predefined size based upon capacity limits
 - Messages containing a recognized virus. To ensure maximum effectiveness, the virus scanner on the gateway must be from a different vendor from (or in addition to) any City agency standard anti-virus software present on internal workstations.

Quarantine events must be followed by e-mails to the sender, the recipient, and an e-mail administrator advising them of the event.

- If customer or third-party relationships are to be conducted via external e-mail, then the customer must be notified that such communications are open and insecure unless explicitly protected. The City agency's legal department must be consulted about any appropriate agreement that needs to be framed in this context.
- E-mail directory information may not be made available outside the City agency. Specific e-mail addresses may be provided to outsiders on a need-to-know basis.
- Inbound mail to users no longer associated with the City agency will be forwarded to a nominated person in the intended recipient's former business area.
- The gateway must offer the facility to append outgoing messages with the following, or a similar approved, disclaimer. Alternatively, the disclaimer may be added to the e-mail user agent software:
 - Any opinions, expressed or implied, presented are solely those of the author and do not necessarily represent the opinions of the City agency.*
- Unless specifically instructed otherwise (at the discretion of the City agency's management), the gateway must pre-append all incoming messages with:

This message has originated from an open public network and cannot be wholly relied upon to be authentic, unless explicitly protected (that is, digitally signed and/or encrypted).

6.2 Facsimile

Fax services may not be used to carry sensitive information without implementing at least the following controls:

- Incoming and outgoing business fax processing must be recorded via confirmation reports.
- Fax gateway and servers must be configured to prevent unauthorized entry into the City agency's networks or systems.
- Fax servers must be configured to send or receive faxes only and not to offer dial-in network access to the attached network.
- Originator details on fax machines or servers must be set correctly.
- Every fax must include a disclaimer notification, which may vary according to City agency, such as:

This fax is intended only for the use of the addressee named above and may contain confidential information. If you are not the addressee, we apologize for any inconvenience to you. Please call us immediately, and we will arrange with you for the return of this fax at our expense. You may not copy this fax, rely on it, or disclose it to any other person. To do this may be illegal.
- Fax machines must be located in office environments where access is restricted.
- Layered security mechanisms (such as fax encryption features or specified devices) must be implemented to add confidentiality or integrity protection to fax services and use.

6.3 Voice Mail

The City agency voice mail facilities and resources must be protected from unauthorized use and reconfigured upon installation to disable default usage options as follows:

- All user voice mailboxes must be protected by a user-specific and definable Personal Identification Number (PIN) with a minimum of six digits. When PINs are allocated to users, they must be random, rather than a fixed default, and they must be set to expire after issue to new users. Furthermore, the system must enforce mandatory PIN changes every six months.
- System administrator PINs must be changed at system installation, subject to regular change, and allocated to appropriate authorized personnel.
- Whenever possible, passwords must be suppressed from feature phones, system printers, and call logging facilities.
- Mailbox access must never provide the option to obtain an outside dial tone.
- Mailboxes must never be allocated or activated in bulk against the Private Branch Exchange (PBX) extension range, but specifically as business authorized and requested, with procedures in place to align maintenance with staff movement (for example, mail boxes must be deleted promptly when an employee departs).
- Guest and default mailboxes must be removed from the system.
- Only system administration personnel must be able to broadcast a message to all mailboxes.

Electronic Communications Directive	Directive: D.4.3
Issued: April 29, 2003	Page 17 of 24

- If the remote maintenance and diagnostic port is used, it must be secured by a barrier device that authenticates the user.

6.4 Video Conferencing

The City agencies must implement controls over video conferencing facilities to prevent interception and eavesdropping, such as:

- Video conference or personal video call facilities must be configured not to auto answer.
- Encryption facilities must be available to secure video conferencing or video calls and prevent interception by unauthorized parties.
- Logging must be enabled.

7 Appendix A

7.1 Purpose

The City recognizes that the principles of freedom of speech and privacy establish important criteria for the use of electronic communications. This directive reflects these firmly held principles within the context of the City agency's legal and City obligations. The purpose of this directive is to:

- Establish guiding principles for privacy, confidentiality, and security in electronic communications
- Ensure that City agency electronic communications resources are used for purposes appropriate to the City's mission
- Inform the City agencies about the applicability of laws and City policies to electronic communications
- Ensure that electronic communications resources are used in compliance with those laws and City policies
- Prevent disruptions to and misuse of City electronic communications resources, services, and activities

This directive cannot be considered a comprehensive or definitive explanation of all the laws that apply to electronic communications.

This directive supports the *Citywide Information Security Policy* and is complemented by other directives and standards, which are referenced where appropriate.

7.2 Who Must Use This Directive

This directive applies to all City employees, contractors, and consultants who are responsible for managing the operation of and access to any part of a City agency's electronic communication systems and services.

It is assumed that knowledgeable technical professionals will be implementing this directive. Detailed operational and control procedures are not included in this document but must be developed by the appropriate personnel.

7.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

7.4 Document Convention

The conventions listed in the table below are used in this document.

Item	Convention	Example
Text entered by the user	Bold Courier New	Enter YES or NO
Text displayed by the system	Courier New	The system displays the following message: Process Complete.
Buttons, menus, menu items	bold Arial	Click OK to continue.
Field names	bold Arial	Select the Enable option.
Filenames	Courier New	Transfer the Webagent.conf file.
Path names and file locations	Courier New	Navigate to c:\tmp.
Keys	Uppercase	Press ENTER.
Single-click of left mouse button	<	< OK .
Single-click of right mouse button	>	> [Desired icon]
Double-click of left mouse button	<<	<< My Computer
Command to close the window	☒	☒
Selection from the Windows taskbar	Bold Arial items with an underlined character	Select <u>P</u>rograms

8 Appendix B -- Areas of Responsibility for Implementation of this Document

8.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

8.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

8.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Electronic Communications Directive	Directive: D.4.3
Issued: April 29, 2003	Page 21 of 24

The TSC is responsible for supporting the *Citywide Information Security Policy*, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

8.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

8.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

9 Glossary of Electronic Communications Terms

This section defines common terms specific to electronic communications. For more general security terms, refer to the “Glossary of Information Security” section in the *Citywide Information Security Policy*.

City agency record	A “record” includes any information kept, held, filed, produced or reproduced by, with, or for a City agency in any form or media, including, but not limited to, reports, statements, examinations, memorandum, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, images, photos, letters, microfilm, computer tapes or disks, rules, regulations, or codes.
compelling circumstances	Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of City policies, or significant liability to a City agency or the City.
electronic communications	Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. For purposes of this directive, an electronic file that has not been transmitted is not an electronic communication.
electronic communications records	Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communication systems or services. This definition of electronic communications records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.
electronic communications resources	Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.
electronic communications systems or services	Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups. The system may be either explicitly denoted as a system for electronic communications or may be implicitly used for such purposes.
electronic communications service provider	Any unit, organization, or staff with responsibility for managing the operation of and controlling individual user access to any part of a City agency’s electronic communications systems and services.

emergency circumstances

Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

holder of an electronic communications record

An electronic communications user who, at a given point in time, is in possession (see definition below) or receipt of a particular electronic communications record, whether or not that electronic communications user is the original creator or a recipient of the content of the record.

possession of electronic communications record

An individual is in possession of an electronic communications record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is deemed, for purposes of this directive, to be in the possession of that addressee. Systems administrators and other operators of City agency electronic communications services are excluded from this definition of possession with regard to electronic communications not specifically created by or addressed to them. Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

transactional information

Information, including electronically gathered information, needed either to complete or to identify an electronic communication. Examples include, but are not limited to: electronic mail headers, summaries, addresses and addressees, records of telephone calls, and IP address logs.

10 References

10.1 City Agency Policy and Directives

- *Citywide Information Security Policy*
- *Information Security Directive: Copyright Compliance*
- *Information Security Directive: Authentication*
- *Information Security Directive: Encryption*
- *Information Security Directive: Remote Access*
- *Information Security Directive: Internet Acceptable Use*
- *Information Security Directive: Change Control*
- *Information Security Directive: Archiving and Retention*
- *Information Security Directive: Business Continuity*
- *Information Security Directive: Risk Assessment*

10.2 State of New York Statutes

- *NYS Department of State Personal Privacy Protection Law* (<http://www.dos.state.ny.us/coog/pppl.html>)

10.3 Federal Statutes and Regulations

- *Freedom of Information Act* (http://www.epic.org/open_gov/foia/us_foia_act.html)
- *Electronic Communications Privacy Act of 1986*
- *Digital Millennium Copyright Act of 1998*
- *Telecommunications Act of 1996*
- *Federal Communications Commission Rules and Regulations*



**CITYWIDE INFORMATION SECURITY
ARCHITECTURE, FORMULATION & ENFORCEMENT
(CISAFE)**

**DEPARTMENT OF INVESTIGATION
CITY OF NEW YORK
CONFIDENTIAL**

Information Security Directive

**Encryption Directive – Version 1.
D 2.18**

April 29, 2003

Table of Contents

1.	Encryption Directive Overview	1
2.	Cryptography Outline.....	2
3.	Electronic Authentication	3
3.1	Public-Key Cryptography for Authentication.....	3
3.2	Secret-Key Encryption for Authentication.....	4
4.	Data Encryption	5
5.	E-mail Encryption	6
6.	Traffic Encryption.....	7
7.	Key Management Controls	8
7.1	Key Management Life Cycle	8
7.1.1	<i>Key Generation</i>	<i>8</i>
7.1.2	<i>Key Sizes</i>	<i>9</i>
7.1.3	<i>Implementation</i>	<i>9</i>
7.1.4	<i>Key Distribution.....</i>	<i>9</i>
7.1.5	<i>Key Back Up and Recovery.....</i>	<i>9</i>
7.1.6	<i>Key Escrow</i>	<i>10</i>
7.1.7	<i>Key Usage</i>	<i>10</i>
7.1.8	<i>Key Termination.....</i>	<i>10</i>
7.1.9	<i>Key Archival.....</i>	<i>10</i>
8.	Appendix A.....	11
8.1	Purpose	11
8.2	Who Must Use This Directive	11
8.3	Information Security Risk Assessment.....	11
8.4	Document Convention	12
9.	Appendix B -- Areas of Responsibility for Implementation of this Document.....	13
9.1	CISAFE.....	13
9.2	DoITT.....	13
9.3	Technology Steering Committee	13
9.4	City Agency and Unit Management.....	14
9.5	Internal Audit	14
10.	Glossary of Encryption Terms	15
11.	References	19
11.1	City Policy and Directives	19
11.2	Federal Statutes and Regulations	19

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 1 of 19

1. Encryption Directive Overview

Communication and transaction security starts with authentication and encryption. Encryption, or encoding data into an unreadable form to ensure privacy, is used for authentication of individuals or computers, such as in Web-based transactions, for securing the exchange of e-mail messages and securing information between a Web browser and a Web Server. In particular, digital signatures, which can be generated quickly and bind a document or message to the owner of a particular key, can also be used for authenticating messages.

This directive provides direction to the City agencies for the use of encryption for City agency business.

2. Cryptography Outline

Cryptography is the branch of applied mathematics that concerns itself with protecting information that is readable ("plaintext") by transforming it (encrypting it) using a cryptographic function ("cipher") into an unreadable format ("cipher text"). The cipher takes two inputs: a key and the plaintext message content. The recipient of the encrypted message submits the cipher text and a key to a cipher and produces the original message.

Cryptographic systems can be broadly classified into:

- *Secret-key systems* (also known as symmetric-key or private-key) which employ an algorithm using the same key to encrypt and decrypt messages, such as the Data Encryption Algorithm (DEA), the RC4, the RC6, and the Advanced Encryption Standard (AES).
- *Public-key systems* (also known as asymmetric-key) which employ an algorithm using two different but mathematically related keys, such as the Rivest, Shamir, and Adleman (RSA) algorithm, the Digital Signature Algorithm (DSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA). The originator's private key is used for creating a digital signature or transforming data into a seemingly unintelligible form. Another key (public key) is used for verifying a digital signature or returning the message to its original form. Each person's public key is published while the private key is kept secret (never shared).

Public-key cryptography depends on mathematical operations that are computationally intensive, and can not be used efficiently to encrypt bulk data in the way many applications require. On the other hand, secret-key systems are excellent performers that can be used to do the kind of bulk encryption necessary in an online application. Therefore, it is recommended to use public-key cryptography in the initial authentication step to exchange a secret key and then use secret-key cryptography to encrypt and decrypt the data.

3. Electronic Authentication

Common authentication methods, such as passwords, are vulnerable to several threats. These threats include masquerade, password compromise, and replay attacks. However, when electronic authentication supported by cryptography is deployed, many of these issues are resolved. The term "electronic authentication" means a cryptographic or other secure electronic technique that allows the user of the technique:

1. to authenticate the identity of or information associated with a sender of a document;
2. to determine that a document was not altered, changed, or modified during its transmission to a recipient;
or
3. to verify that a document received was sent by the identified party claiming to be the sender.

Both public-key and private-key cryptography can be used for electronic authentication.

3.1 Public-Key Cryptography for Authentication

Public-key cryptography can be used for electronic authentication in the form of digital signatures. A digital signature is extra data appended to a message. This extra data is used to identify and authenticate the sender and message data using public-key cryptography.

Authentication based on public-key cryptography has an advantage over many other authentication schemes in that no secret information has to be shared by the entities involved in the exchange. A user (claimant) attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter that is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

In particular, to verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. A public-key certificate or certificate is a credential that vouches for the bind between a key pair and the identity of the owner of the key. It is signed by the private key of the issuing Certificate Authority (CA) and can be verified using the CA's public key. It contains the identifiers for the key pair owner, the public half of the pair, the start and end dates of its validity, and its intended purpose, use and limitations. The certificates of several of the most popular CAs are embedded in most Web browsers.

A CA is a third-party organization or company that vouches for the association between a public key and another person or entity. The CA may be a principal such as the management of a company, a government agency or an independent third party operating as a fiduciary and for a profit. The principal requirement for a CA is that it must be trusted by those who will use the certificate and for the purpose for which the certificate is intended. The necessary trust may come from its role, independence, affinity, repudiation, contract, or other legal obligation. For more information on CAs and key management, refer to the City's *Information Security Directive: Public Key Infrastructure (PKI)*.

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 4 of 19

On October 1, 2000, the *Electronic Signatures in Global and National Commerce (ESIGN) Act* officially went into effect in the United States. It states that electronic signatures, which encompass digital signatures, retinal scans and digitized signatures, are as valid and legal as handwritten signatures. This enables companies and individuals to create contractual relationships and binding transactions and records over the Internet that cannot be denied enforcement because they were purely electronic.

City agencies interested in digital signing need to understand the business risk associated with deployment of public-key systems and to take the necessary security precautions to protect these systems. Therefore, a City agency interested in digital signing must do the following:

- develop a policy and practices statement that describes the use of digital signatures;
- describe the degree of trust that can be associated with a signature; and
- define how digital signatures can be used and who can use and rely on them.

Furthermore, users of digital signatures need to understand the significance of signing and the need to protect their private signing key. City agencies must ensure that the public-key systems that are supported by them provide these capabilities.

3.2 Secret-Key Encryption for Authentication

Secret-key systems typically take a password and convert it into a secret key using a one-way hash function. One of the most popular authentication systems used today is called Kerberos. The basic model for authentication in Kerberos allows a client and a server (e.g., a browser and a Web server) to mutually authenticate each other with the help of a trusted third party (a Kerberos authentication server). The major advantage of such a model is that a centralized authentication server can be used to authenticate clients and servers for a large number of applications spread across a distributed environment. Another advantage is that the passwords themselves never cross the network, not even in an encrypted form.

Using secret-key encryption for authentication is recommended for City agencies that have a centralized point of administrative control. However, the City agencies must consider the fact that a secret-key system, such as Kerberos, requires an online centralized authentication server that stores a database of every user's (client and server) secret keys. This makes the server a tempting and available target for attack and possible single point of failure.

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 5 of 19

4. Data Encryption

Since City agency communications systems may not be secure, City agency employees may not transmit sensitive information over any communication system unless it is transmitted using approved security procedures and practices (e.g. encryption, secure networks, and secure workstations).

The following are data encryption directives:

- Users of City agency computing resources are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks.
- The City agency must make available software and protocols that provide robust encryption, as well as the capability for properly designated City agency officials to decrypt the information, when required and authorized under this directive.
- These products must be endorsed by the City agency and DOI/CISAFE. Users of City agency computing resources who are encrypting information are encouraged to use only the endorsed software and protocols.
- The City agencies must ensure that a staff member is allowed to encrypt data only with the permission of his/her supervisor.

Users who elect not to use endorsed encryption software and protocols on Information Technology (IT) systems are expected to decrypt information upon official, authorized request.

5. E-mail Encryption

There are many risks associated with sending unsecured e-mail. E-mail can fall prey to malicious software tools used for scanning and intercepting mail traffic. These tools may be used by unauthorized people to tamper with e-mails so that the message reaching the recipient is not the one originally sent by its author. Furthermore, the sender's name and address can be used to send false e-mail messages. The results of such practices to a City agency could be embarrassing and costly.

The use of encryption gives rise to e-mails that are demonstrably authentic and unaltered, as well as, private and non-reputable (i.e. the sender cannot deny being their originator). An encryption package consists of data-scrambling technology that allows users to e-mail information across a network without reservations. Through encryption, a message is encoded so that only its intended recipient can decrypt it. This way, if a message is scanned or intercepted, it cannot be read. The two main forms of e-mail encryption are Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).

The City agency must choose one of the following options for the implementation of e-mail encryption based on its business needs:

- *Client-based.* Involves implementing the software at the client level. It requires installation of the encryption software on each machine in the corporate network. Every user has his/her own key pair and the public keys have to be distributed to each sender whose message is to be encoded and also handle the decoding of each message received. In this case, if e-mail is encrypted and is sent outside the City agency network, it cannot be scanned for malicious content by the anti-virus software installed at the firewall level. To ensure appropriate anti-virus protection, the City agency management must decide whether to allow the encryption of e-mail messages that contain sensitive information only within the City agency or also to outside parties.
- *Server-based.* The e-mail server (not the user) automatically encrypts all outgoing mail and all e-mail messages reaching the server are automatically decrypted, meaning that each user receives a legible text message. All City agency users share the same key pair held by the e-mail server. The public key can be shared through a City agency-wide message automatically added to all outgoing mail. This enables all senders to encrypt messages to the City agency and helps cater to the legal liability of the unprotected transmission of confidential or sensitive data.

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 7 of 19

6. Traffic Encryption

Depending on the sensitivity of a City agency Web Site, which can be determined by the results of the Information Security Risk Assessment, public-key cryptography, in particular the Secure Socket Layer (SSL) protocol, must be used for authentication of City agency Web sites to Web browsers.

The Secure Sockets Layer (SSL) protocol provides encrypted connections so that information can move across the intranet or Internet with confidence that it will not be intercepted or modified in transit. SSL defeats most attempts to eavesdrop, forge or otherwise tamper with data in transit. It is appropriate to use SSL to protect passwords, intellectual property and other information on a City agency Web site which may not travel across a network unencrypted.

The City agency Web servers must use server certificates signed by respected Certificate Authorities and support 128-bit encryption.

Regardless of SSL, the City agencies may not collect and store highly sensitive or confidential information on a City agency Web server. While SSL encrypts a Web browser's connection to a City agency Web site, it does not protect information stored on a Web server. That is, the files in the Web server are not encrypted and are therefore more vulnerable.

7. Key Management Controls

Key management is the application of security policies, directives and standards discipline using technology and procedures to symmetric (secret-key) algorithms for data encryption, data integrity and message authentication. Asymmetric keys refer to asymmetric (public-key) algorithms for key exchange and digital signatures.

The City agencies must follow general key management security directives. These directives include:

- symmetric keys and asymmetric private keys must be kept secret;
- asymmetric public keys must be managed with data integrity and authentication, typically in the form of a public key certificate according to the City's *Information Security Directive: Public Key Infrastructure*;
- cryptographic software and hardware must be operated in a secure, lights-out environment with limited access by authorized personnel under dual control; and
- controls must be implemented specific to the key life cycle as described next.

7.1 Key Management Life Cycle

Cryptographic keys have an inherent life cycle with planned obsolescence. The City agencies must implement procedures to secure the key management life cycle as described in the following sections.

7.1.1 Key Generation

Key generation is the process where keys are initially created. The City agencies must implement key generation according to the following directives:

- All keys must be generated using a random or pseudo random number generator. Most browsers (e.g. Navigator, Internet Explorer) use a FIPS 140-1 certified software pseudo random number generator. Almost all cryptographic hardware (e.g., Luna PCMCIA cards) uses hardware random number generators. For the current list of FIPS 140-1 certified vendor products, refer to <http://csrc.nist.gov/cryptval/140-1/1401val.htm>.
- All asymmetric keys must be generated using a bona fide prime number generator. Refer to ANSI X9.80 for further details. Many prime number generators (e.g. Entrust, Netscape) are based on the RSA BSAFE toolkit, which was developed by leading cryptographers.
- Keys must be generated according to the size (typically specified in bits) appropriate to the Information Security Risk Assessment. The strength of symmetric keys is based upon the time it takes to perform an exhaustive key search of the possible key space. The strength of asymmetric keys is based on the difficulty of "hard" mathematical problems (e.g. factoring for RSA 4, discrete logarithms for DSA) where the amount of work is estimated and compared to performing the equivalent of performing an exhaustive search.

7.1.2 Key Sizes

Given the current technology, symmetric keys less than 80-bit must be considered “weak” symmetric keys whereas 128-bit keys or higher is considered “strong” symmetric keys.

Furthermore, 512-bits asymmetric RSA keys must be considered “weak” whereas 768-bits or higher asymmetric RSA keys must be considered “strong”. Note that ANSI X9 standards mandate a minimum of 1024-bit RSA keys and 160-bit keys for all discrete log algorithms (e.g. DSA, ECDSA, Diffie-Hellman) for digital signatures and key management protocols.

However, it is important to recognize that the corresponding key management controls are independent of the key size. Therefore, “weak” keys only reduce the overall security strength and do not reduce the operational overhead or significantly speed up cryptographic processing.

7.1.3 Implementation

Cryptography can be implemented in software on a general purpose computer or in specialized cryptographic hardware called a Tamper Resistant Security Module (TRSM). Software implementations radically increase the risk of key compromise as the symmetric or asymmetric private keys occur as clear text in the unprotected memory of the computer. Specifically, software cryptography violates the security of secret keys. Conversely, a TRSM is specifically designed to protect cryptographic keys.

7.1.4 Key Distribution

Key distribution and activation is the process whereby keys are distributed from their generation site to their usage site. The City agencies must implement the following controls for key generation:

- Keys must be deployed in the fewest locations that are operationally practical. This is based on the concept of compartmentalizing damage in the event of a key compromise. Keys must only be deployed where necessary.
- Keys must be securely deployed in acceptable form using verifiable key exchange mechanisms.

7.1.5 Key Back Up and Recovery

Key back-up and recovery is the process whereby keys are securely stored for purposes of key recovery due to inadvertent key loss (e.g. equipment failure). The City agencies must implement the following controls for key back up and recovery:

- Keys must be securely stored with all access under dual control with proper authorization duly recorded in an event journal.

7.1.6 Key Escrow

Key escrow is the process where keys are securely stored for purposes of data recovery due to City or governmental requirements. The owner of the key may be unaware that the key is being accessed. The City agencies must implement the following controls for key escrow:

- keys must be securely stored in acceptable form with all access under dual control with proper authorization duly recorded in an event journal; and
- escrowed keys subsequent to retrieval, having been out of the control of a City agency, must be considered compromised at the end of the data recovery period and must be terminated whenever possible.

7.1.7 Key Usage

Key usage is the process whereby keys are securely used in a production environment. The City agencies must implement the following controls for key usage:

- keys must only be used for their intended purpose as determined at the time of key generation;
- since misuse of keys can expose a system to certain types of attacks, cryptographic equipment may be used to enforce key separation (e.g. key variants, control vectors); and
- keys must be used only during their intended life time.

7.1.8 Key Termination

Key Termination is when all instances of a key are deleted with the possible exception of key archival. The City agencies must implement the following controls for key termination:

- Upon termination, each instance of the key is destroyed and documented in the event journal.

7.1.9 Key Archival

Key Archival is the process whereby a single instance of a key is stored securely for the purposes of validating any past transactional data. The City agencies must implement the following controls for key generation:

- archived keys must be securely stored in acceptable form with all access under dual control with proper authorization duly recorded in an event journal;
- archived keys must never be installed in production systems; and
- careful consideration must be used during the re-installment of archived keys, since it could expose a system to certain types of attacks.

8. Appendix A

8.1 Purpose

Encryption can be used to maintain confidentiality and protect data from unauthorized access. It can also be used to prove the authenticity of a message's originator. The City promotes the use of strong encryption which enhances the privacy of communications and stored data while preserving the City's and law enforcement's right to be able to gain access to evidence as part of a legally authorized search or surveillance. The purpose of this document is to establish directives for the appropriate use of encryption by City agencies.

This directive supports the *Citywide Information Security Policy* and is complemented by other detailed directives and standards that provide additional information. These directives and standards are referenced where appropriate.

8.2 Who Must Use This Directive

This directive applies to all City employees, contractors and consultants who use encryption for City agency business.

It is assumed that knowledgeable technical professionals will be implementing this directive. Detailed control procedures are not included in this document, but must be provided by the appropriate personnel to document supporting operational procedures.

8.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

8.4 Document Convention

The conventions listed in the table below are used in this document.

Item	Convention	Example
Text entered by the user	Bold Courier New	Enter YES or NO
Text displayed by the system	Courier New	The system displays the following message: Process Complete.
Buttons, menus, menu items	bold Arial	Click OK to continue.
Field names	bold Arial	Select the Enable option.
Filenames	Courier New	Transfer the Webagent.conf file.
Path names and file locations	Courier New	Navigate to c:\tmp.
Keys	Uppercase	Press ENTER.
Single-click of left mouse button	<	< OK .
Single-click of right mouse button	>	> [Desired icon]
Double-click of left mouse button	<<	<< My Computer
Command to close the window	☒	☒
Selection from the Windows taskbar	Bold Arial items with an underlined character	Select <u>P</u>rograms

9. Appendix B -- Areas of Responsibility for Implementation of this Document

9.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

9.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

9.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 14 of 19

The TSC is responsible for supporting the *Citywide Information Security Policy*, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

9.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

9.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

10. Glossary of Encryption Terms

This section provides common encryption terms and definitions. For more general security terms, refer to the Glossary of Information Security section in the *Information Security Policy*.

Advanced Encryption Standard (AES)	Encryption algorithm for securing sensitive but unclassified material by US Government agencies.
Certificate or Public-Key Certificate	A set of data that unambiguously identifies an entity, contains the entity's public key and is digitally signed by a trusted third party (Certification Authority).
Certificate Authority (CA)	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.
Cipher	Any method of encryption text (concealing its readability and meaning). It uses both a key (a variable that is combined in some way with the unencrypted text) and an algorithm (a formula for combining the key with the text).
Ciphertext	The text that results from encrypting plaintext.
Claimant	An entity that is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange (e.g. a smartcard (claimant) can act on behalf of a human user (principal)).
Cryptography	The branch of applied mathematics that concerns itself with protecting information that is readable ("plaintext") by transforming it (encrypting it) using a cryptographic function ("cipher") into an unreadable format ("cipher text").
DEA	Data Encryption Algorithm, a symmetric algorithm defined in the ANSI standard X3.92 and in the Data Encryption Standard FIPS PUB 46
Decryption	The process of converting encrypted data back into its original form so it can be understood.

Digital Signature Extra data appended to a message that identifies and authenticates the sender and message data using public-key cryptography.

DES Data Encryption Standard, the official title of FIPS PUB 46.

Digital Signature Algorithm (DSA) Proposed in August of 1991 by NIST. The DSA has become a U.S. Federal Information Processing Standard (FIPS 186) called the DSS(Digital Signature Standard). It is the first digital signature scheme recognized by any government. The DSS is a signature scheme with appendix and explicitly requires use of SHA-1(the Secure Hash Algorithm).

Elliptic Curve Digital Signature Algorithm (ECDSA) The elliptic curve analogue of the DSA (also called DSS) signature method. Defined in the ANSI X9.62 standard, it incorporates the use of a hash function. Currently, the only hash function defined for use with ECDSA is the SHA-1 message digest algorithm.

Electronic Authentication A cryptographic or other secure electronic technique that allows the user of the technique to authenticate the identity of or information associated with a sender of a document, to determine that a document was not altered, changed, or modified during its transmission to a recipient; or to verify that a document received was sent by the identified party claiming to be the sender.

Encryption The conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

Entity Any participant in an authentication exchange; such a participant may be human or non-human and may take the role of a claimant and/or verifier.

Hash Function An algorithm which creates a digital representation or "fingerprint" in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it.

Key A variable value that is applied using an algorithm to a string or block of unencrypted text to produce encryption text and vice versa. The length of the

key generally determines how difficult it will be to decrypt the text in a given message.

Plaintext Ordinary readable text before being encryption into cipher text or after being decrypted.

Pretty Good Privacy (PGP) A technique for encrypting messages developed by Philip Zimmerman. PGP is based on public-key cryptography.

Principal An entity whose identity can be authenticated.

Private key A cryptographic key used with a public-key cryptographic algorithm, which is uniquely associated with an entity and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.

Public key A cryptographic key used with a public-key cryptographic algorithm, uniquely associated with an entity and which may be made public. It is used to verify a digital signature and it is mathematically linked with a corresponding private key.

Public-key cryptography Using a public key and a private key to protect information, where each person's public key is published while the private key is kept secret (never shared). Messages are transformed or "signed" using the originator's private key and can be verified using his or her public key by anyone.

Public Key Infrastructure (PKI) An architecture that is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings and provide other services critical to managing public keys.

RC4 Stream cipher algorithm designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation.

- RC6** Block cipher algorithm designed by Ron Rivest in collaboration with Matt Robshaw, Ray Sidney and Yiqun Lisa Yin from RSA Laboratories. The algorithm makes essential use of data-dependent rotations.
- RSA algorithm** A public-key cryptosystem based on the factoring problem. RSA stands for Rivest, Shamir and Adleman, the developers of the RSA public-key cryptosystem and the founders of RSA Data Security (now RSA Security).
- Secret- key Cryptography** Using the same key for encryption and decryption of data.
- Secure/MIME (S/MIME)** New version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.
- Signed data** Data on which a digital signature is generated.
- Tamper Resistant Security Module (TRSM)** A physical device having physical barriers and/or logical controls to prevent the exposure of cryptographic keying material.
- Verifier** An entity that either is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

Encryption Directive	Directive: D.2.18
Issued: April 29, 2003	Page 19 of 19

11. References

11.1 City Policy and Directives

- *Citywide Information Security Policy*
- *Information Security Directive: Public Key Infrastructure*
- *Information Security Directive: Risk Assessment*

11.2 Federal Statutes and Regulations

- *Electronic Signatures in Global and National Commerce (ESIGN) Act*



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

IDENTITY MANAGEMENT

THE POLICY

ALL ACCESS TO CITY OF NEW YORK SYSTEMS MUST BE AUTHORIZED AND BASED UPON INDIVIDUAL IDENTIFICATION AND AUTHENTICATION.

AGENCY RESPONSIBILITY

- 1) Each agency is responsible for the management of its user identities. This includes identity validation/registration, authentication, authorization, provisioning/de-provisioning and management of identities.
- 2) Management approval is required before a user is authorized to use any City computing resources.
- 3) Users who are not City employees, but who are in a current contractual relationship with the City may have access to City computing resources if they have a valid non-disclosure agreement in effect and their sponsor approves their access.

IDENTITY LIFE CYCLE

- 4) Users must be positively and individually identified and validated prior to being permitted access to any City computing resource.
- 5) Users will be authenticated at a level commiserate to the data classification of the information being accessed.
- 6) Access permissions must be defined in accordance with a user's actual functional work requirements.
- 7) User accounts will be created and de-provisioned in a timely manner. Inactive user accounts will be de-provisioned according to the **Citywide Information Security Password Policy**.

CITYWIDE IDENTITY STORE

- 8) Each agency must establish connectivity to the Citywide Directory.
- 9) Each agency is responsible for managing their identities within the Citywide Directory/Identity Vault
- 10) Applications will be required to participate in the consolidation of external identities to the Single Identity Vault.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

PASSWORD CONTROLS

- 11) The password settings of user accounts must comply with the ***Citywide Information Security Password Policy***.

DOITT

DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Information Security Directive

Incident Response – Version 1.
D 2.8

April 29, 2003

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	

Table of Contents

1 Overview of the Incident Response Directive.....	1
2 Incident Outline.....	2
2.1 Definition.....	2
2.2 Indications.....	2
2.3 Categories.....	3
2.3.1 System Privileges.....	3
2.3.2 System Compromise.....	3
2.3.3 Information	4
2.3.4 Unauthorized Compromise Access.....	4
2.3.5 Denial of Service.....	4
2.3.6 Misuse of IT Resources Probes.....	5
2.3.7 Hostile Probes.....	5
2.3.8 Other IT Security Concerns.....	5
2.4 Priority Levels.....	6
3 Incident Response Process.....	7
3.1 Considerations.....	8
4 Incident Response Teams.....	9
5 Incident Response Procedures.....	10
5.1 Handling Incident Information.....	11
5.2 Incident Logging.....	11
6 Appendix A.....	12
6.1 Purpose.....	12
6.2 Who Must Use This Directive.....	12
6.3 Information Security Risk Assessment.....	12
7 Appendix B -- Areas of Responsibility for Implementation of this Document.....	14
7.1 CISAFE.....	14
7.2 DoITT.....	14
7.3 Technology Steering Committee.....	14
7.4 City Agency and Unit Management.....	15
7.5 Internal Audit.....	15
8 Glossary of Incident Response Security Terms.....	16
9 References.....	17

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 1 of 16

1 Overview of the Incident Response Directive

Despite an organization's best efforts, an information technology (IT) security incident may occur. When an incident occurs, the incident response process helps the affected organization respond to the event and resume normal operations as quickly as possible. Throughout the incident response process, the organization must have adequate controls to ensure that the following goals are achieved:

- Determine the scope of incident
- Maintain and restore data and evidence
- Maintain and restore services
- Determine how and when the incident occurred
- Determine the causes of the incident
- Prevent escalation and further incidents
- Prevent negative publicity
- Penalize or prosecute the attackers

The purpose of this document is to provide directives for responding to security events that adversely affect the security and operational integrity of the City agency's information systems.

This directive addresses all types of incidents known as of the revision date of this document. These incidents may include-

- An intruder gaining unauthorized access to the City agency's systems
- A virus infecting the City agency's systems
- City agency resources becoming unavailable because of a denial of service (DoS) attack
- An authorized user attempting to gain access or gaining access to unauthorized resources
- A malicious attempt to break into the City agency's systems

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 2 of 16

2 Incident Outline

2.1 Definition

An incident is an adverse event or situation that poses a threat to the integrity, availability, or confidentiality of systems or data. Some results of an incident may include-

- Failure or compromise of security controls
- Attempted, suspected, or actual alteration, destruction, or misappropriation of information
- Waste, fraud, abuse, damage, or loss of City agency IT property or information

2.2 Indications

A computer security incident can occur at anytime. Traditionally, most hacker and “cracker” incidents have occurred during off hours, because hackers do not expect system managers to be watching their systems then. However, some types of attacks, such as worm and virus incidents, can occur at any time. Therefore, time and distance considerations are very important in responding to the incident.

Certain indications that an incident may have taken place deserve special attention. These include-

- Repeated or inexplicable system crashes
- New, unidentified user accounts or high activity on an account that has had no activity for months
- System accounting discrepancies (for example, in a UNIX system, the file /usr/admin/lastlog decreasing in size)
- Data modification or deletion (for example, files vanishing)
- Attempts to write to privileged system files
- Denial of service (for example, a system manager and all other users becoming locked out of a UNIX system that has been changed to single-user mode)
- Unexplained poor system performance
- Irregular actions (for example, “GOTCHA” being displayed on a computer screen)
- Suspicious queries (for example, many unsuccessful login attempts from another node)
- Suspicious browsing (for example, someone becoming a root user on a UNIX system and accessing successive files in one user account after another)

This list is not all-inclusive. Any type of aberrant system behavior may be indicative of an attack.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 3 of 16

2.3 Categories

Both defining and tracking categories of incidents provide statistical data that can help management allocate resources to improve the City agency's IT security posture. To understand the nature and extent of threats to IT resources, the incidents must be categorized based on the severity of the risk to the system or network. Incident categories must include:

- System compromise
- Information compromise
- Unauthorized access
- Denial of service
- Misuse of IT resources
- Hostile probes
- Other IT security concerns

2.3.1 System Privileges

The term system privileges denotes the ability to do one or more of the following:

- Make modifications to the computer's operating system, system audit logs, system configurations, account privileges, account passwords, data files, software, or applications
- Add or delete accounts
- Install or delete software and applications
- Alter a system's security controls outside the abilities normally authorized for an individual's account

This is not an all-inclusive list.

2.3.2 System Compromise

The following are acts that may represent a system compromise:

- An account or application with system privileges is used without prior authorization or approval
- A vulnerability in the system is exploited, and system-level access to accounts is gained
- A valid account is used to increase its own privileges and is successfully exploited to gain access to accounts with system privileges

This is not an all-inclusive list.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 4 of 16

2.3.3 Information Compromise

The following are acts that may represent an information compromise:

- A valid account is used without authorization and access is gained to password files, data, applications, or accounts that are protected or restricted, but access is not gained to system-level accounts
- A vulnerability in the system is successfully exploited to gain access to password files, data, applications, or accounts that are protected, but access is not gained to system-level accounts
- The physical theft of assets provides access to password files; protected or restricted data; licensed applications or software; or restricted applications, software, or code

This is not an all-inclusive list.

2.3.4 Unauthorized Access

The following are acts that may represent unauthorized access:

- A valid account is used without authorization to attempt access to password files, data, applications, or other accounts outside the user account's authorizations to view otherwise protected or restricted information
- A vulnerability in the system is successfully exploited, allowing access to data, applications, accounts with system privileges or password files, or information that is otherwise protected or restricted

This is not an all-inclusive list.

2.3.5 Denial of Service

The following are acts that may represent a denial of service:

- A system's ability to perform its normal functions is impaired because it has been inundated with activity originating from one or more sources
- Resources, such as power, network access, or routing tables, are deliberately modified to cause a system not to be able to perform its normal functions
- Malicious code (for example, viruses, Java applets, ActiveX, Trojan horses, logic bombs, or worms) interferes with a system to a significant degree
- Assets are physically taken or destroyed, but no password files, protected or restricted data, applications, restricted software, or code are compromised

This is not an all-inclusive list.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 5 of 16

2.3.6 Misuse of IT Resources

The following are acts that may represent the misuse of IT resources:

- An authorized account is used in violation of federal laws or the Citywide Information Security Policy regarding the proper use of IT resources
- Resources or privileges higher than those allocated or assigned are obtained without authorization
- Unlicensed software or applications are installed

This is not an all-inclusive list.

2.3.7 Hostile Probes

The following are acts that may represent hostile probes:

- Exploits are run against a system that, if successful, would result in a system compromise, information compromise, or unauthorized access
- Exploits are run against a system that, if successful, would impair a system's ability to perform its normal functions
- Information from one or more systems is illicitly gathered or is attempted to be illicitly gathered

This is not an all-inclusive list.

2.3.8 Other IT Security Concerns

The City agency must identify personnel responsible for information security. These personnel must identify other questionable events that are not included in the above-mentioned categories. Examples of other questionable events include: suspicious network activity, excessive junk mailing, mail spoofing, and hoaxes.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 6 of 16

2.4 Priority Levels

It is important to prioritize the actions that must be taken during an incident well in advance of any possible occurrence. At times, an incident may be so complex that it is impossible to do everything at once to respond to it. Therefore, setting priorities is essential. Although priorities may vary based on circumstances, the following serve as starting points for defining the City agency's response:

- Priority 1 – Protect human life and people's safety. Human life always has precedence over all other considerations.
- Priority 2 – Protect classified and highly sensitive data while gathering evidence.
- Priority 3 – Protect other data, including proprietary, managerial, and other data, because loss of data is costly in terms of resources
- Priority 4 – Prevent damage to systems. Such damage can result in costly downtime and recovery.
- Priority 5 – Minimize disruption of computing resources. In many cases, it is better to shut down or disconnect a system from the network than to risk damage to data or systems.

An important consideration in defining priorities is that once human life and institutional security considerations have been addressed, it is more important to save data rather than system software and hardware. Although it is undesirable to have any damage or loss during an incident, systems can be replaced. The loss or compromise of data, however, is usually not an acceptable outcome.

3 Incident Response Process

Incident response consists of asset managers' real-time decisions and actions to minimize incident-related effects on their assets. These decisions and actions, based on available evidence from the incident, must mitigate any residual security risk. Figure 1 depicts a typical incident response process.

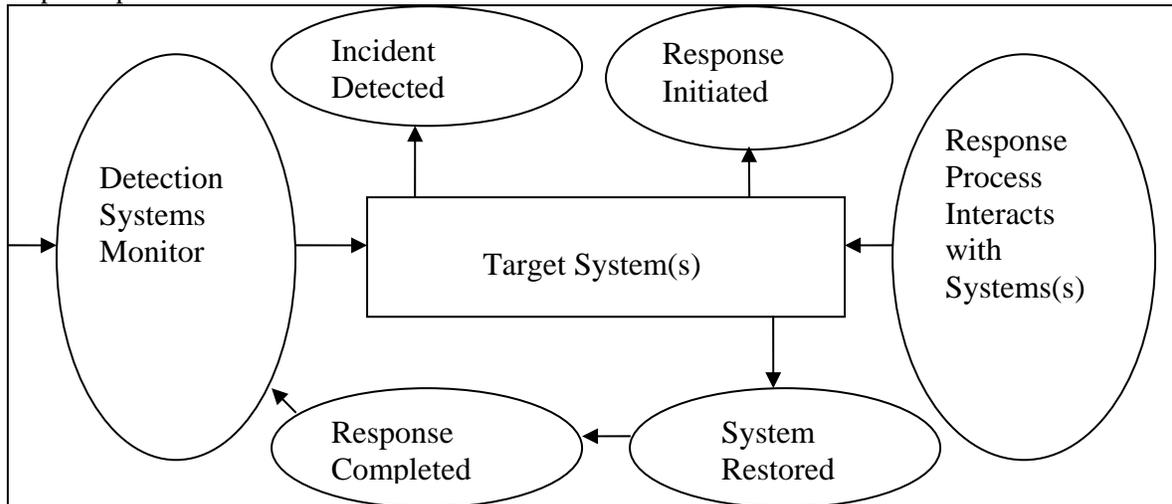


Figure 1. Typical Incident Response Process

Detection Systems Monitor. Intrusion detection systems (IDSes) or other types of detection systems monitor the status of City agency systems in order to identify and respond to malicious activity targeted at computing and networks resources. For more details on intrusion detection, refer to the City's Information Security Directive: Intrusion Detection.

Incident Detected. The City agency performs an initial analysis and determines that an incident has occurred and whether the incident is security-critical.

Response Initiated. Information is passed from an IDS or other type of detection system to the City agency's personnel or automated systems as the basis for a response.

Response Process Interacts. The response activities of the City agency's personnel interact with the target environment to restore it to a degraded, mirrored, or improved state. The considerations described in the next section must be taken into account.

System Restored. The system is restored as a result of the incident response activities. The restored system may be in one of the following states:

- Degraded – The system is restored, but some of the system attributes remain in a degraded or damaged state. This may be an intermediate step to mirrored or improved restoration.
- Mirrored – Using backups, the system is restored to its exact pre-incident state.
- Improved – The system is restored and enhanced to address the vulnerability that was exploited during the incident.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 8 of 16

Response Completed. The system is restored, and a post-mortem analysis is conducted to prevent future occurrences of the incident or improve future performance in similar incidents.

3.1 Considerations

Certain factors can influence and affect incident response. The City agency's incident response team must take into account the following considerations when responding to an incident.

About the incident:

- What assets have been damaged by the incident?
- Has this incident occurred before?
- How did the incident occur? Was it caused by a malicious or a non-malicious source?
- How trustworthy is the incident information source?
- Can the incident be correlated with other information?
- Was the incident detected as a result of a defensive action (for example, a trap)? Is there a well-defined plan for this type of incident?

About the effects of response actions:

- What would be the effect of modifying system functionality? Common response modifications are-
 - Shutting down all system operations. This must be done only in the most extreme cases to ensure that it does not accomplish the denial of service task intended by the intruder.
 - Cutting off all inbound service. This must be used to respond to flooding spoofs where the source of intrusion is unknown. This action may also produce a denial of service effect.
 - Cutting off inbound service access from the reported source address of the intrusion.
- What would be the effect of initiating active defensive strategies such as traps or trace-back? Is it acceptable?
- Is the proposed response legal and compliant with relevant policy?
- Who must be involved in the response?

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 9 of 16

4 Incident Response Teams

The City agency must identify a City Agency Security Incident Response Team (CASIRT). This team must coordinate and support the responses to security incidents that involve sites within a defined constituency. Depending on the size of the City agency, the

CASIRT must include a member of the upper level management, human resources management (for internal incidents), technical staff, security engineers, and lead information systems security personnel.

Everyone who uses the City agency's IT resources must report any known or suspected IT security incidents to the designated CASIRT. The City agency personnel involved in the incident response process are also responsible for providing any needed information to CASIRT.

The City agency must identify a City Agency Emergency Response Team (CAERT). This team must evaluate the security incidents that CASIRT has identified as emergencies. CAERT and CASIRT must coordinate efforts during and after the emergency situation. CAERT must be empowered to make decisions and to request resources required to investigate, contain, and resolve the computer security emergency situation.

The City agency must develop procedures for the CASIRT and CAERT teams. These procedures must be documented and published internally. Published procedures must include the teams' contact information to ensure that all users know how to notify the teams in case of a security incident.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 10 of 16

5 Incident Response Procedures

The City agency must develop incident response procedures that outline the steps of the City agency's incident response. These procedures must address the following areas:

- Incident Detection:

- The integrity of the monitoring systems must be verified, and the logging systems must be checked to ensure that they have not been breached.

- If an unusual or malicious activity has been detected, the criticality of the event must be determined and, if required, the City agency CAERT must be notified.

- If an incident has occurred, the CAERT must be summoned, the CAERT membership must be documented, and a CASIRT member must contact a CAERT member to provide a telephone number through which CASIRT can receive information updates.

- During the incident triage process, a decision must be made as to whether the possibly compromised system must be shut down immediately to contain the damage, or whether the system must remain in operation until the CAERT assembles. This decision must take into account the possibility of a "dead man's switch" or other malicious code that, if the system is shut down or disconnected, may be introduced and cause greater damage.

- Incident Containment:

- If the incident has been deemed an emergency, the CAERT must determine the appropriate course of action from the following options for containment: shut down the compromised system, disconnect the compromised system, or disable system services. Depending on which action is taken, it may be necessary to contact other parties. A list of such parties must be maintained for each application running in the City agency systems or dependent on the City agency systems.

- Incident Resolution

- Weaknesses in the system must be eliminated (for example, all passwords on all systems to which the intruder may have had access must be changed through forced expiration). All compromised systems, executable programs (including application services), and binary files must be reinstalled, and all changes made by an intruder must be removed. Any remaining system and network vulnerabilities must be identified.

- The exact means and modality of the attack must be determined to ensure that the vulnerability is eliminated from all other systems.

- The CASIRT and CAERT, in cooperation with the City agency management, must decide when to return systems to operation.

- All unusual and suspicious activities must be monitored at a critical level. Redundant systems must be checked for further damage, and the backup capabilities of critical systems must be ensured.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 11 of 16

- Incident Prevention

- A post mortem analysis must be conducted, a review meeting must be held with the City agency CASIRT, and an Incident Report must be generated.

- Threat and vulnerability findings resulting from the incident must be communicated to all other City agencies to prevent the same attack from being perpetrated against another City agency.

- The affected system and network assets must be re-inventoried to determine whether assets have been updated, modified, or added to systems or networks as a result of the incident resolution stage.

- System and network administrators must assist legal, audit, and other investigations, as appropriate, with technical reporting and incident notes.

5.1 Handling Incident Information

All electronic communications regarding incidents must be handled in a secure manner through the use of secure messaging technology. Examples of personnel authorized to possess incident information include the system administrators, City agency management, City agency security officer (if applicable), CASIRT, CAERT (in case of an emergency incident), and CISAFE. To keep information within prescribed channels, individuals with knowledge of an incident must exercise caution. Failure to do so may impede or even circumvent the City agency's chance of obtaining a conviction if a computer crime is discovered.

5.2 Incident Logging

Logging of information is critical in situations that may eventually involve federal, state, or local law enforcement authorities and a criminal trial. The implications of each security incident are not always known at the beginning or even during the course of an incident. Therefore, a written log must be kept for all security incidents that are under investigation. The information must be logged in a location that cannot be altered by others. Manually written logs are preferable, since online logs can be altered or deleted. The types of information that must be logged are-

- Dates and times of incident-related communication, such as phone calls (for example, timestamp)
- Dates and times that incident-related events were discovered or occurred
- How much time was spent working on incident-related tasks
- People who have been contacted by the City agency or who have contacted the City agency
- Names of systems, programs, or networks that have been affected

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 12 of 16

6 Appendix A

6.1 Purpose

This directive is designed to provide guidance to the employees and administration of the City in responding to computer security incidents. A computer security incident is defined as any event that compromises some aspect of computer or network security.

An incident response process ensures the protection of the City's business processes, intellectual property, and competitive advantage through rapid response to electronic security emergencies. Through early detection, an incident response process can provide containment, timely resolution, and preventive measures in dealing with a computer security incident.

This directive supports the Citywide Information Security Policy and is complemented by other directives and standards, which are referenced where appropriate.

6.2 Who Must Use This Directive

This directive applies to all City employees, contractors and consultants, who use City computing resources and are engaged in the support of the City's information systems. The management of Information Technology security incidents is a primary business risk management objective and requires the attention of management and key support staff.

It is assumed that knowledgeable technical professionals will be implementing this directive.

Detailed control procedures are not included in this document, but must be provided by the appropriate personnel to document supporting operational procedures.

6.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's Information Security Directive: Risk Assessment) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications.

DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 13 of 16

7 Appendix B -- Areas of Responsibility for Implementation of this Document

7.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

7.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

7.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 14 of 16

The TSC is responsible for supporting the Citywide Information Security Policy, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

7.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

7.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 15 of 16

8 Glossary of Incident Response Security Terms

This section defines common terms specific to incident response security. For more general security terms, refer to the Glossary of Information Security section in the *Citywide Information Security Policy*.

City Agency Security Incident Response Team (CASIRT)

A team that coordinates and supports the response to Security incidents that involve sites within a defined constituency (for example, a City agency).

City Agency Emergency Response Team (CAERT)

A team that-
Evaluates security incidents that have been deemed emergencies

- Coordinates efforts during and after the emergency situation.

The CAERT is empowered to make decisions and to request the resources required, investigate, contain, and resolve the electronic security emergency situation.

Incident

An adverse event or situation that poses a threat to the integrity, availability, or confidentiality of data or systems that result in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of City of New York IT property or information.

Information

Anything spoken, overheard, written, stored electronically, copied, transmitted, or held intellectually concerning the City's agency's business, information systems, employees, business partners or any aspect of the operations of the administration.

Vulnerability

A characteristic of a piece of technology that can be Exploited to perpetrate a security incident.

Incident Response Directive	Directive: D.2.8
Issued: April 29,2003	Page 16 of 16

9 References

- *Citywide Information Security Policy*
- *Information Security Directive: Risk Assessment*
- *Information Security Directive: Intrusion Detection*



**CITYWIDE INFORMATION SECURITY
ARCHITECTURE, FORMULATION & ENFORCEMENT
(CISAFE)**

**DEPARTMENT OF INVESTIGATION
CITY OF NEW YORK
CONFIDENTIAL**

Citywide Information Security Policy

**Citywide Information Security Policy - Version 1.1
P 1**

April 30, 2003

Table of Contents

1.	Overview	1
1.1	Introduction.....	1
1.2	CISAFE Mission Statement.....	1
1.3	Scope.....	2
1.4	Document Taxonomy	2
2.	Policy Statement	4
2.1	Information Classification and Control.....	4
2.2	System Access Control	5
2.3	Information Security in the Systems Development Life Cycle.....	5
3.	Roles	6
3.1	DOI	6
3.2	DoITT.....	6
3.3	Technology Steering Committee	6
3.4	City Agency and Unit Management.....	7
3.5	Information Owners	7
3.6	Information Custodians.....	8
3.7	Users	8
3.8	Independent Review.....	8
3.9	Internal Audit	9
4.	Enforcement	10
4.1	Violations	10
4.2	Penalties.....	10
5.	Appendix A	11
5.1	Information Security Risk Assessment.....	11

1. Overview

1.1 Introduction

The City of New York (the "City") relies on its information technology systems to meet its operational, financial, and informational obligations. Accordingly, City information technology systems, and the information and communications that are stored, processed, and presented on these systems ("Information Assets"), constitute vital City property that must be protected from misuse, and operated and maintained in a secure environment.

Pursuant to the June 24, 1981, Mayoral Directive 81-2 Electronic Data Processing Security ("Mayoral Directive 81-2"), the Department of Investigation ("DOI") is responsible for establishing citywide standards to ensure the security of the City's electronic data processing systems, and their compliance with approved policy. In the two decades since Mayoral Directive 81-2 was promulgated, there have been significant developments and changes affecting the City's information assets' management, including the development of the Internet, e-mail communications, and increased access to both of these resources. As a result, the City's information assets are now constantly exposed to security risks that did not previously exist.

DOI, to meet its responsibilities under Mayoral Directive 81-2, has established the Citywide Information Security Architecture, Formulation, and Enforcement Unit ("CISAFE").

1.2 CISAFE Mission Statement

CISAFE is responsible for the creation, development, and enforcement of consistent and cost effective security procedures, standards, and controls to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information which is processed through the City of New York. CISAFE's mission is aligned with the City's Information Technology Strategy (ITS), which is available on the City Intranet at: <http://cityshare.nycnet>; select DOI/CISAFE from the "Agency Intranet Sites" menu.

DOI has established a *Citywide Information Security Policy*, along with accompanying directives and standards, to safeguard the City's information assets, as required by law, and to meet the City's obligation, to its citizens and others, to deliver City services efficiently, without interruption or delay.

The *Citywide Information Security Policy* requires that each City agency and its units must be responsible for the security of its own information assets, and must adequately protect this information, according to its value and risk factor. This obligation includes, but is not limited to, maintaining the confidentiality, integrity, and availability of this information, as well as ensuring individual accountability for its use.

1.3 Scope

For purposes of this policy and its supporting directives and standards, City information assets shall include all electronic data stored, processed, transmitted, or printed by any City computer system, and such systems' peripheral equipment, networks, or magnetic data.

All City employees, and individuals performing services for the City, whether paid or unpaid, including contractors, consultants, interns, or suppliers, who use or have access to any City information assets, must comply with this policy and its directives and standards.

CISAFE will verify and enforce compliance.

1.4 Document Taxonomy

The chief components of the *Citywide Information Security Policy* and its supporting directives and standards are defined as follows:

Policy – The legal, regulatory, and operational requirements of the City's Information Security program. The *Citywide Information Security Policy* is a mandate with which all City agencies are required to comply.

Directive – The implementation of the *Citywide Information Security Policy* in a specific information technology area. A directive defines the strategic objectives of the *Citywide Information Security Policy* in terms relevant to a specific type of information technology or supporting process.

Standard – The implementation of a directive for a specific hardware, software, or infrastructure component. A standard is product-specific, and describes security controls particular to a vendor's product.

City agencies are expected to develop procedures that describe steps tailored to the operation of their specific software, hardware, and network components to comply with these directives and standards.

The following diagram (next page) depicts the taxonomy used for this model.

DOI/CISAFE Document Taxonomy

Citywide Information Security Policy	
P	1 High Level Information Security Policy

Information Security & Availability	
D	2.1 Risk Assessment
D	2.2 Authentication
D	2.3 User Account Management
D	2.4 Public Key Infrastructure
D	2.5 Virtual Private Networks
D	2.6 Digital Signatures
D	2.7 Intrusion Detection
S	2.7.1 Net Ranger
S	2.7.2 ISS Real Secure
S	2.7.3 Axent Net Prowler
D	2.8 Incident Response
D	2.9 Information Classification
D	2.10 Archiving & Retention
D	2.11 Disposal of Information Assets
D	2.12 Copyright Compliance
D	2.13 Business Continuity
D	2.14 Change Control
D	2.15 Physical Security
D	2.16 Personnel Security
D	2.17 Password Management
D	2.18 Encryption
D	2.19 Wireless Networks

Operating Systems	
D	3.1 Host & Server Systems
S	3.1.1 UNIX
S	3.1.2 OS/390 RACF
S	3.1.3 OS/390 Top Secret
S	3.1.4 AS/400
S	3.1.5 Open VMS
S	3.1.6 Windows NT Server
S	3.1.7 Windows 2000 Server
S	3.1.8 Novell Netware
S	3.1.9 UNISYS
D	3.2 Desktop Systems
S	3.2.1 UNIX
S	3.2.2 Windows

Applications	
D	4.1 Database Management Systems
S	4.1.1 Sybase
S	4.1.2 Oracle
S	4.1.3 DB2
S	4.1.4 MS SQLServer
D	4.2 Source Code Management
D	4.3 Electronic Communications
S	4.3.1 Lotus Domino
S	4.3.2 Microsoft Exchange
S	4.3.3 Eudora Mail
S	4.3.4 Groupwise
D	4.4 Application Security

Infrastructure	
D	5.1 Network Management
S	5.1.1 SNMP
D	5.2 Domain Name Services
S	5.2.1 UNIX
S	5.2.2 NT
S	5.2.3 Windows 2000 Server
D	5.3 Hubs, Routers & Switches
S	5.3.1 Cisco
S	5.3.2 3Com
S	5.3.3 Bay
D	5.4 Firewall Configuration
S	5.4.1 Cisco PIX
S	5.4.2 Raptor
S	5.4.3 Checkpoint Firewall-1
S	5.4.4 Border Manager
S	5.4.5 Cyberguard
S	5.4.6 Cisco IOS
S	5.4.7 IBM Firewall for AIX
S	5.4.8 TIS Guantlet
D	5.5 Web Applications
D	5.6 Internet Acceptable Use
D	5.7 Internet Connectivity
D	5.8 Internet Perimeter Architecture
D	5.9 Telephony / PBX
D	5.10 Anti-Virus
D	5.11 Directory Services
S	5.11.1 Netware Directory Services
S	5.11.2 NT Directory Services
S	5.11.3 iPlanet Directory Server
S	5.11.4 Active Directory
S	5.11.5 Banyan Vines Street Talk
D	5.12 Remote Access
D	5.13 Local Area Network

2. Policy Statement

City information assets shall be safeguarded to ensure their:

- confidentiality;
- integrity;
- availability; and,
- non-repudiation,

so that the City can meet its public, legal, and contractual obligations.

The City requires that:

- City information owners (i.e., agency Commissioners, unit chiefs, etc.) are responsible for defining City information security and control levels at their agencies based on their risk assessment;
- individual users are accountable for their use of City information;
- City information is recorded on a secure medium, and procedures are employed, so that all City information transactions can be reconstructed pursuant to DORIS regulations; and,
- periodic, independent reviews are conducted by DOI/CISAFE, of the management and use of City information.

2.1 Information Classification and Control

All City information shall have a designated owner (Information Owner), and be classified according to the requirements stated in the Information Classification Directive. These requirements address:

- Infrastructure; and,
- City agency business processes.

City Information Owners shall ensure:

- that appropriate security policies, directives, and standards are implemented with respect to the City information elements that they own, either directly or through appointed custodians; and,
- that the level of security and control applied to the protection of specific City information or processes is commensurate with its sensitivity, value, and critical factor (e.g. confidentiality, integrity, availability, authenticity, accountability, and non-repudiation), according to a defined classification process.

2.2 System Access Control

In order to implement effective Citywide access control:

- each City agency must impose access controls on all City information systems and processes;
- all City information systems must provide appropriate logging to provide a user activity audit trail;
- City information owners are responsible and accountable for determining access rights to City information;
- each City information system must present a system logon banner stating user access requirements; and,
- City information users are allowed access to City information for City business needs only.

2.3 Information Security in the Systems Development Life Cycle

Information security risk analysis and management must be integral to the City information systems' development, implementation, and maintenance processes. The information security requirements for any City information application shall be in compliance with the *Citywide Information Security Policy*, directives, and standards promulgated by DOI/CISAFE. In order to facilitate the integration of security in the Systems Development Life Cycle:

- project risk analysis shall be included in all application development projects, to assess and determine the risks associated with new or modified software; and,
- all new hardware and/or third-party software must be in compliance with the applicable *Citywide Information Security Policy*, directives, and standards established by DOI/CISAFE.

3. Roles

3.1 DOI

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective information security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

3.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT is also responsible for review of the agencies' connectivity requests to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

3.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors, and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology issues.

The TSC is responsible for supporting the *Citywide Information Security Policy*, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

3.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to DOI and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this guideline.

3.5 Information Owners

Information Owners are responsible for:

- defining the City agency business critical factor level of their City information;
- identifying and approving the level of security and control required to adequately safeguard the sensitivity, value, and critical factor level of their City information and, when necessary, to prevent its false repudiation, based on the results of their City agency information security risk assessment;
- ensuring that Information Owners' responsibilities are explicitly defined, and that security and control measures are implemented;
- managing and protecting City information; and,
- ensuring that the electronic data systems on which City information resides and is processed are periodically reviewed for compliance with the governing information security policy, directives, and standards.

When determining the security level and control to apply to City information, an Information Owner must consider how the City information is created and managed, as well as the City agency's City information business critical factor – which is defined by its importance, its sensitivity, its trustworthiness, its availability, and its integrity.

Information Owners are accountable for the access they grant to their City information, and must define, for users, its accessibility, as well as the level and nature of authorization to be applied in the access process.

These determinations must take into account:

- the need to protect the City information, as determined by the City agency information security risk assessment;
- the need to access the City information, as determined by the City agency business requirements;
- the need to retain the City information; and,
- the City information's legal and regulatory requirements.

A City Information Owner may be an individual, a steering committee, a review panel, or an official entity. The use and collection of City information can create new ownership requirements, when information is processed or transferred.

3.6 Information Custodians

Information Custodians (i.e. individuals designated by service level agreement or delegation of responsibility by City Information Owners) are responsible for maintaining the confidentiality, integrity, availability, authenticity, accountability, and non-repudiation of the City information they create or use at levels defined by their Information Owners, and in accordance with this policy and applicable DORIS regulations. Therefore:

- Information Custodians must apprise their Information Owners of risks that may arise as a result of their control and security decisions;
- Information Owners must provide contract language that adequately covers responsibilities of Information Custodians in accordance with this policy and applicable DORIS regulations; and,
- When City information is created and managed by the same user, this user is considered both the Information Owner and the Information Custodian.

3.7 Users

Users shall comply with the *Citywide Information Security Policy*, and relevant directives and standards, when creating, using, and managing City information. Each user will be held individually accountable for his/her actions involving the use of City information and its associated systems.

Users are prohibited from utilizing City-owned computing resources or information for personal business. Furthermore, it shall be a user's responsibility to understand when and why information used to conduct the City's business must be safeguarded with suitable controls, and to seek assistance to implement those controls.

Users who suspect or know of a violation of the *Citywide Information Security Policy* and its related directives and standards, or who believe City information is not properly safeguarded, must report this matter promptly and directly to DOI, in accordance with their responsibilities under Mayoral Executive Order 16 of 1978, as amended.

3.8 Independent Review

Management, use, and control of City information remains, at all times, subject to independent review by DOI. Such review may address the validity of each City agency's information risk assessment results and security classification, and the appropriateness of the information's:

- accessibility;
- safeguards;
- management, including segregation of roles and independent authorization/review of transactions; and,
- procedural recovery arrangements.

3.9 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

4. Enforcement

4.1 Violations

Violations may include any willful or negligent act that:

- compromises the security of City employees, contractors, or consultants, or of the City's information assets;
- exposes the City to an actual or potential monetary loss due to a breach of electronic data or information security;
- allows unauthorized access to, disclosure of, and/or alteration of City information; or
- uses City information in violation of any provision of local, State, or Federal law.

4.2 Penalties

Non-compliance with, or willful violation of, the *Citywide Information Security Policy*, directives, and standards may result in:

- disciplinary action (fines and/or suspension);
- termination of employment; and,
- civil suit and/or criminal prosecution.

5. Appendix A

5.1 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The *Citywide Information Security Risk Assessment* (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. CISAFE proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password Policy

The Policy

All passwords and Personal Identification Numbers (PINs) used to protect City of New York systems must be appropriately configured, periodically changed, and issued for individual use.

Password/PIN Usage and Confidentiality

- 1) Individual users must properly protect passwords and/or PINs for all accounts.
- 2) All passwords and/or PINs must be classified and handled as City of New York Confidential data.
- 3) Passwords and/or PINs unique to an individual must not be shared with other individuals or users.
- 4) Passwords/PINs must not be displayed on the screen at any time.
- 5) Passwords and/or PINs must be changed whenever there is any indication of system or password compromise.
- 6) Any password or PIN management system either must avoid caching the password or PIN or must provide adequate protections and controls if such caching is essential.
- 7) Passwords and/or PINs must always be encrypted when held in storage or when transmitted across any network. Exception: One-time passwords or PINs, or hard-coded passwords or PINs
- 8) Use of a City of New York approved hashing algorithm is considered encryption for the purposes of password or PIN protection. Unencrypted passwords and/or PINs must never be embedded in sign-on utilities. For example, an unauthorized user must never be able to authenticate at sign-on merely by using a function key or by running an available program.
- 9) Unencrypted passwords and/or PINs must not be hard-coded in source code, command files, initialization files, scripts or installation kits.
- 10) PINs shall only be used where a numeric method for authentication is required (e.g., for entry on a telephone keypad); in all other instances, passwords should be used for authentication.
- 11) Administrative passwords must be adequately protected and restricted only to required individuals for system support.
- 12) Screen lock must be activated within fifteen (15) minutes of unattended inactivity.

Password/PIN Length

- 13) Passwords and/or PINs must have a minimum length of eight (8) characters. Exception: Voice mail systems, as well as Blackberry and PDA devices issued by the City must use a password or PIN of at least 4 alphanumeric characters.



Password Complexity

- 14) Passwords must be constructed using at least one alphanumeric and at least one character which is numeric or a special character.

Class Description	Examples
1. Upper Case Letters	A B C ... Z
2. Lower Case	Letters a b c ... z
3. Numerals	0 1 2 ... 9
4. Non-alphanumeric ("special characters", punctuation, symbols)	{ } [] , . < > ; : ' " ? / \ ` ~ ! @ # \$ % ^ & * () _ - + =

- 15) Passwords must not be derived from commonly used words or phrases.
- 16) Users should not select passwords consisting of easily guessed words, such as words found in dictionaries (English and non-English), User IDs, proper names or other names or words readily associated with the individual user, such as dates, nicknames and family names.
- 17) Users should not select passwords, or PINs, that contain personally identifiable numbers, such as the user's telephone extension, Social Security Number, or zip code.

Password/PIN Expiration

- 18) Passwords and/or PINs must be changed at least every ninety (90) days.
- 19) Temporary or initial passwords and/or PINs must be set to expire after initial use. The user must be required to change the password or PIN at the first use.
- 20) Administrative passwords must be changed every sixty (60) days, or when an individual who has knowledge of the password leaves their job function.

Disabling of Accounts

- 21) All accounts that provide access to sensitive, private or confidential Information must be automatically disabled after five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

Default Passwords/PINs

- 22) Any default password or PIN must be changed during or immediately upon the completion of the installation process. The new password or PIN must conform to the requirements defined in this policy.
- 23) Default accounts must be renamed, if possible, to non-obvious names.

Password/PIN Reuse

- 24) User-chosen passwords and/or PINs must not be reused for four (4) iterations.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password/PIN Changes

- 25) Proper proof of identification must be provided before changing a password or PIN.
- 26) Users changing a password or PIN via a system command or screen must prove knowledge of the current password or PIN or be cryptographically authenticated before being allowed to change it.
- 27) The minimum time between user initiated password and/or PIN changes must be at least one (1) day. If a user has recently changed a password and is concerned that the new password may have been compromised, but is unable to immediately change it again in accordance with this provision, the user should contact an administrator of the system in which the password is used to request a password reset.
- 28) Users requesting a new password or PIN or requesting a password or PIN change/reset via a help desk or administrator must prove their identity before the change is initiated.

Password/PIN Delivery

- 29) Delivery of passwords and PINs to a user, either when an account is created or when an administrator resets a password/PIN, requires attention to ensure that delivery is done efficiently and with a regard to security. Passwords must not be transmitted over any City of New York voice, video or data network without appropriate identification and authentication.
- 30) A password must be delivered in a manner that requires the recipient to prove his/her identity before the password is received.

Policy Enforcement

- 31) Administrators are accountable for configuring systems to enforce this policy.
- 32) Where possible, the system must enforce these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, to enforce password complexity, the administrator should run tools periodically to detect weak passwords, and require users with weak passwords to change their passwords.



**CITYWIDE INFORMATION SECURITY
ARCHITECTURE, FORMULATION & ENFORCEMENT
(CISAFE)**

**DEPARTMENT OF INVESTIGATION
CITY OF NEW YORK
CONFIDENTIAL**

Information Security Directive

**Password Management – Version 2.0
D 2.17**

March 18, 2004

Table of Contents

1	Overview of the Password Management Directive.....	1
2	Password Management Policy	2
2.1	Defining Password Security	3
2.2	Choosing a Good Password.....	3
2.3	Password Expiration.....	4
3	Appendix A.....	5
3.1	Purpose	5
3.2	Who Must Use This Directive	5
3.3	Information Security Risk Assessment.....	5
3.4	Blank.....	6
4	Appendix B -- Areas of Responsibility for Implementation of this Document	7
4.1	CISAFE.....	7
4.2	DoITT.....	7
4.3	Technology Steering Committee	7
4.4	City Agency and Unit Management.....	8
4.5	Internal Audit	8
5	Glossary of Password Management Terms	9
6	References.....	10

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 1 of 10

1 Overview of the Password Management Directive

The password is the most vital part of account security. A significant number of computer security incidents involving actual penetration of "secure" systems can be traced back to poorly chosen passwords. In most cases, weak passwords are the first point of attack for an experienced attacker.

Weak passwords can be exposed in a number of ways. These include "password cracking" programs, social engineering, shoulder surfing, or just simple Post-It notes left on top of monitors by employees. It is obvious that an attacker who can discover a user's password can then log on to the system and operate with all of that user's capabilities. This type of attack compromises the audit-related controls because the system assumes that an authorized user is carrying out these activities. As a result, such an attack is usually difficult to detect and can last for months. Depending on the account privilege rights, the damage to the City agency's information integrity, availability, and confidentiality could be substantial.

2 Password Management Policy

All user access must be authenticated, and the authentication process must be in line with the classification of the system based on an Information Security Risk Assessment.

All City agencies must develop and disseminate an agency-specific password policy. This policy must include, at a minimum, the following:

- All system access will be authenticated by passwords.
- Passwords will be a minimum of six alphanumeric characters.
- Passwords must never be displayed on the screen when being entered.
- Users must be forced to change passwords at least every thirty (30) days or when the system is suspected of being compromised.
- Users may not be permitted to change their passwords to any of the past six (6) passwords they have had.
- The system must prevent the selection of easy-to-guess passwords, including, as a minimum, any dictionary word, proper names, repeated text strings, for example, AAAAAAAA, the user ID, or month names. The system must also enforce the requirement that passwords contain at least one numeric character.
- Passwords stored on end systems must be stored with one-way encryption with no facility to read or recover passwords. If a password is forgotten, a new one must be issued or set.
- Passwords may not be hard coded in system scripts, batch files, or other areas.
- When a Security Administrator generates or distributes initial passwords, the unique, "random" initial password must be assigned and provided to the user by a means that protects against unauthorized disclosure of the password.
- New or administrator-provided passwords must be pre-expired, forcing the user to change the initial password on the first use.
- System administrators may not have access to user passwords.
- Password-changing routines must prompt for a re-entry of the new password for verification purposes.
- The user ID must be suspended, pending administrator intervention, after at most three (3) incorrect attempts at logon.
- The use of system-generated passwords is not recommended because such a practice increases the probability that users will write down these difficult-to-remember passwords.
- Password strength must be assessed on all systems on at least a semi-annual basis, using commercially available utilities.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 3 of 10

2.1 Defining Password Security

The user ID identifies users to City agency systems—that is, it tells the system who they are. Passwords authenticate users by providing a second component of the logon process that is presumably known only to valid users. Therefore, the security and integrity of the password is vital to overall security.

Password security from an end-user perspective can be expressed by four simple rules:

1. Keep passwords secret. Don't write passwords down anywhere, for example, on a file, program, or paper, without proper protection.
2. Make sure passwords cannot be guessed by someone who knows you well, for example, someone who has personal knowledge of you or who knows your job function.
3. If there is even a chance that someone else might know your password, change it. It is City agency policy to change passwords every 30 days.
4. Pick good passwords. It is easy to select bad or easily guessed passwords, but it is just as easy to select good ones.

2.2 Choosing a Good Password

Bad passwords are dangerous because they provide the illusion of security while, in reality, they may expose the City agency and the user to significant risk and potential liability.

The following directives must be distributed to the end-user community to guide them in password composition.

In composing passwords, end users **must**:

- Use a password with mixed-case alphabetic characters, digits, and any other characters permitted by the specific system.
- Use a long password (eight characters or more).
- Change passwords at least every 30 days even if not forced by the system.
- Lock the screen with password protection. Screen lock must be activated after five minutes of inactivity.
- Log off properly when done for the day, especially if using public terminals.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 4 of 10

In composing passwords, end users **may not**:

- Use logon names in any form, for example, verbatim, reversed, capitalized, doubled, or modified by adding a prefix or suffix;
- Use, in any form, their first or last name or, more generally, any information easily obtained about them, such as car license plate numbers, telephone numbers, social security numbers, or a spouse's child's, or home street name;
- Use a word contained in any dictionary or any language, spelling lists, or other lists of words, for example, acronyms, place names, car names, names of cartoon heroes, or sequences of letters, such as 'abcdef' or 'qwerty';
- Use a password shorter than 6 characters or with only alphabetic characters or only numbers;
- Use the word "password," "New York," "City," "agency," or other common words associated with the City of New York.

Education with regard to safeguarding passwords and password composition is an integral part of an overall security-awareness program.

2.3 Password Expiration

City agencies must force password expiration by requiring that all users do the following:

- Change the default password immediately after they are given access to a new system or application.
- Change their passwords every 30 days. Appropriate system controls must be set in place to enforce a maximum password expiration of 30 days.

Changing passwords regularly provides a second level of protection against guessed or stolen passwords.

If possible, password expiration must be synchronized between systems to expire passwords on the same date for a given user on all systems. This reduces the chance of users having to remember multiple passwords for multiple systems.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 5 of 10

3 Appendix A

3.1 Purpose

The purpose of this document is to establish directives that support the identification and authentication of a user before allowing that user to access City agency systems or other City resources. This directive helps prevent inappropriate and unauthorized users from accessing systems and applications that contain City of New York information.

This directive supports the *Citywide Information Security Policy* and is complemented by other security directives and standards, which are referenced where appropriate.

3.2 Who Must Use This Directive

This directive applies to all City employees, contractors, and consultants who use City agency computing resources. Password management is a primary business risk management objective and requires the attention of management and key support staff.

It is assumed that knowledgeable technical professionals will be implementing this directive. Detailed operational and control procedures are not included in this document but must be developed by the appropriate personnel.

3.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 6 of 10

3.4 Blank

Page intentionally left blank

4 Appendix B -- Areas of Responsibility for Implementation of this Document

4.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

4.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

4.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 8 of 10

The TSC is responsible for supporting the Citywide Information Security Policy, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

4.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

4.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

Password Management Directive	Directive: D.2.17
Issued: April 30, 2003	Page 9 of 10

5 Glossary of Password Management Terms

This section defines common terms specific to Password Management. For more general security terms, refer to the Glossary of Information Security section in the *Citywide Information Security Policy*.

None

6 References

- *Citywide Information Security Policy*
- *Information Security Directive: Risk Assessment*



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

PERSONNEL SECURITY

THE POLICY

ALL EMPLOYEES, CONTRACTORS, AND CONSULTANTS MUST BE APPROPRIATELY SCREENED, TRAINED, AND SUPERVISED.

JOB POSITION SECURITY REQUIREMENTS

- 1) City Agencies must ensure that:
 - a. Security requirements critical to performance of job responsibilities are clearly defined.
 - b. Job descriptions include all applicable security responsibilities.
- 2) In conjunction with Human Resources background checks must be performed on all employees. Background checks will be performed on contractors and all temporary personnel in accordance with their contract terms.
- 3) In unique situations, the responsible party at the Agency may make exceptions to this requirement providing appropriate supervision is granted while the individual has access to City assets.

MANAGEMENT RESPONSIBILITIES

- 4) All agency managers are responsible for enforcing Citywide and agency level information security policies.
- 5) Compliance with information security requirements should be reflected in individual's performance evaluations.

USER RESPONSIBILITIES

- 6) All City employees, contractors, consultants, temporary personnel, clients, and vendors are responsible and accountable for safeguarding and preventing the unauthorized disclosure, modification or destruction of information assets entrusted in their care.
- 7) Users must follow the access and handling requirements identified in local information security policies.
- 8) All employees and contractors must relinquish all City of New York assets upon termination of contract or employment. This includes but is not limited to; copies of information received and/or created, identification badges, and computing devices.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

CONFIDENTIALITY AGREEMENT

- 9) All City personnel with access to City Critical Information assets must sign a confidentiality agreement which forbids the disclosure of such information to parties within or outside of the City who do not have a business need.
- 10) All non-City personnel (temporary contract employees, contractors, vendors/consultants and/or the vendor/consultant Company on their behalf, and third-party users) must sign a non-disclosure agreement to receive access to any City Critical Information.
- 11) Confidentiality and/or non-disclosure agreements must be reviewed periodically, and/or whenever there are changes in terms of employment or the contractual agreement.

USER SECURITY TRAINING

- 12) Each new employee is required to attend an orientation specific to their City agency. The orientation must explain the agency's information security policies. A record must be maintained that every person with access to City business information acknowledges that he/she:
 - a. Has read and understands the information security policies.
 - b. Understand his/her responsibilities to comply with the policies which affect that person's job responsibilities.
 - c. Understands the consequences of an infraction.

DISCIPLINARY PRACTICE

- 13) Each Agency, in conjunction with their Human Resources and Legal Departments, must develop and implement a formal disciplinary practice for noncompliance with information security policies.
- 14) Disciplinary practice may involve action up to and including termination for serious violations and repeated offenses.
- 15) Criminal or civil liability may apply to any individual who knowingly violates security requirements.
- 16) Individuals who violate the City Information Security Policies may have their access removed or suspended. Contractors will have their company notified and legal action taken. The action taken in each situation will be decided between the Information Owner and the Agency Head.

DOITT

DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Information Security Directive

Physical Security- Version 1.

D 2.15

April 30, 2003

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	

Table of Contents

- 1 Overview of the Physical Security Directive.....1**
- 2 Physical Access Controls.....2**
 - 2.1 Baseline Building Controls.....2
 - 2.2 Additional Building Controls.....3
 - 2.3 Data Center Controls.....3
 - 2.4 Server Controls.....4
 - 2.5 Workstation Controls.....4
 - 2.6 Portable Computer Controls.....4
 - 2.7 Supporting Infrastructure Controls.....4
- 3 Environmental Protection Controls.....5**
 - 3.1 Physical Layout and Location.....5
 - 3.2 Fire Protection.....5
 - 3.3 Heating, Ventilation, and Air-Conditioning.....5
 - 3.4 Electric Power Systems.....6
 - 3.4.1 Backup Power for Power Outage Situations.....6
 - 3.4.2 Emergency Power-Off Switches.....6
 - 3.4.3 Emergency Lighting.....6
- 4 Operational Constraints.....7**
- 5 Other Considerations.....8**
 - 5.1 Employee Termination or Change in Job Responsibility.....8
 - 5.2 Insurance.....8
- 6 Appendix A.....9**
 - 6.1 Purpose.....9
 - 6.2 Who Must Use This Directive.....9
 - 6.3 Information Security Risk Assessment.....9
- 7 Appendix B -- Areas of Responsibility for Implementation of this Document.....10**
 - 7.1 CISAFE.....10
 - 7.2 DoITT.....10
 - 7.3 Technology Steering Committee.....10
 - 7.4 City Agency and Unit Management.....11
 - 7.5 Internal Audit..... 11
- 8 Glossary of Physical Security Terms..... 12**
- 9 References..... 13**

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 1 of 13

1 Overview of the Physical Security Directive

Physical security refers to the protection of building sites and equipment and all information and software contained in them from physical threats, such as—

- Natural catastrophes (for example, floods, earthquakes, and tornados)
- Extreme environmental conditions (for example, dangerous temperatures, high humidity, heavy rains, and lightning)
- Intentional acts of destruction (for example, theft, vandalism, and arson)
- Unintentional acts of destruction (for example, spilled drinks, overloaded electrical outlets, and faulty plumbing)
- Accidents

Physical security requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Physical security is a vital part of any security plan and is fundamental to all information security efforts. Without physical security, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to implement.

This document provides guidance on the implementation of physical access controls and environmental protection controls that must be in place for City agencies:

- Data centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

This directive covers all information system (IS) environments operated by a City agency or contracted with a third party by a City agency. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (for example, mainframe, distributed, desktop, and network devices), software, and information.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 2 of 13

2 Physical Access Controls

Physical access controls primarily protect the physical installation and media (magnetic and documented) from damage or theft. City agency building-access controls must be appropriate to the type of information processing that is occurring at the physical location and the criticality of the information as determined by an Information Security Risk Assessment. Consequently, City agency buildings containing designated data centers must employ stricter access controls than those that do not.

2.1 Baseline Building Controls

City agency workspaces must implement the following measures to safeguard the information resources they house (if the City agency only utilizes part of a building, then the points below refer only to the specific City agency run sections):

- Security guards must protect against unauthorized access to the building. Guards must be on duty during all hours of expected building operation and must conduct internal inspections of the building to ensure appropriate security.
- External monitoring of conditions around the building must be conducted. This can be accomplished by external security guard patrols, outside camera monitoring, or a combination of both methods where appropriate. Outside lighting must effectively support building monitoring.
- During hours other than normal business hours, access to building/department entrances must be achieved by a card or token access system.
- All secure areas, including elevators, must be outfitted with controlled-access devices (for example, door locks and magnetic badge card readers).
- A visitor access procedure must be followed when nonemployees gain entrance to the building:
 - Sign in with the security guard in a visitors log that is retained and reviewed
 - Produce photo identification to obtain a visitor's badge from the security guard
 - Wear the visitors badge to inform personnel that a nonemployee is in the area
 - Be accompanied by a City agency employee while in the building
- Property passes must be issued by the property owners and verified by the security guard in order to allow removal of City agency property from the building.
- Physical security devices must remain operational during a power failure and must be inspected and tested on a monthly basis.
- All equipment, media, files, and supplies—including those located in the user areas (for example, office and cubicle work spaces)—must be secured physically at all times to prevent them from being removed from the facility without permission. In particular, media storage—for example, compact discs (CDs), diskettes, tapes, and paper documents, such as files and folders—must be placed in secured areas or cabinets. Offices, file cabinets, and overhead bins must be locked when not in use.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 3 of 13

2.2 Additional Building Controls

The information processed in data centers is usually deemed critical to City agency operations and is generally confidential. Consequently, access controls for a building that houses a data center require a high level of personnel restriction and authentication. Beyond the baseline controls described in the previous section, additional controls must be enforced at City agency buildings that house data centers. These controls include:

- Inspection of incoming and outgoing packages (for example, bags, briefcases, and boxes) to prevent unauthorized materials from entering or leaving the building.
- Advance authorization for all visits by non-data center personnel by data center management, with appointments confirmed by security guards.
- Use of a card access or token system for controlling access to the building during hours other than normal business hours and for recording individual personnel entrance and exit times in an audit log, which must be retained and reviewed regularly
- Measures for securing from tampering all power feeds, communication lines, and other cabling that service the data center

2.3 Data Center Controls

In addition to controlling physical access to buildings that house data centers, City agencies must enforce the following physical access controls for the data centers themselves:

- Card-key access must be enforced so that only authorized individuals may enter the data center.
- Logging of card-key access use must be done to create an audit trail.
- The list of persons authorized for data center access must be reviewed regularly. Card-key access must be terminated immediately after termination of employment.
- Everyone who enters the data center must be properly identified and required to wear an identification badge at all times. In particular, all visitors, building maintenance workers, hardware manufacturer representatives, hardware maintenance staff, software suppliers, and cleaning personnel entering the data center must be signed in, escorted, and supervised when entering the data center or working in it, and they must be signed out when leaving the data center. These individuals may not be permitted to operate any equipment in the data center or be near it without a specific reason or without close supervision.
- Data center employees must have written procedures and training for challenging unfamiliar or unauthorized personnel in or near data center areas.
- Security guard personnel must perform internal monitoring of data center activity (through closed-circuit television). In particular, entrance and exit alarms must warn against unauthorized access attempts. Intrusion-detection alarm systems must be used for installations that may be left unattended. These alarm systems must either be part of 24-hour security control or be connected to a security company or law enforcement agency. Alarm systems must be checked periodically.
- Appropriate physical construction standards that discourage unauthorized access attempts must be in place. These standards must include the following:

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 4 of 13

- True floor-to-ceiling data-center perimeter walls or motion detectors in the drop ceiling (and under the raised floor) to detect unauthorized access attempts
- Absence of external access, such as windows or external hinges, on entrance doors to the data center

2.4 Server Controls

Based on the results of an Information Security Risk Assessment, all servers that process critical applications or data must be located in areas that meet the physical security requirements for data centers.

When a server that processes only non-critical applications and data is located in an area other than a data center, access to it must be physically restricted to authorized personnel (for example, system administrators). The server must be located in a closed area (for example, a locked office) that is free from physical hazards (for example, high traffic, water leaks, and fire risks).

2.5 Workstation Controls

End-user workstations must be located in areas free of physical hazards (for example, high traffic, water leaks, and fire risks). The workstations must be secured via security cabling to prevent unauthorized removal from the premises. Workstations connected to the network must store sensitive information on file-server drives as often as possible. Information stored on floppy disks must be physically secured in a manner appropriate to its sensitivity level.

2.6 Portable Computer Controls

Laptops have a high risk of loss because of portability. Consequently, laptops must be traceable to individual users. Sensitive data, to the extent possible, may not be stored on the unit's permanent disk drive. However, if it is necessary, sensitive data (for example, nondisclosure agreements) must be stored on the disk drive using a PC security or disk encryption package. All laptops must have their system and user passwords enabled.

All laptops must be physically secured via an appropriate security device (for example, security cabling) during any period that the unit is left unattended in a City agency office.

2.7 Supporting Infrastructure Controls

The level of security must be determined on the basis of the results of an Information Security Risk Assessment. Access to facilities that support information processing systems—such as rooms housing telecommunications, emergency power sources (for example, generators and batteries), and air-conditioning units and closed areas where network hubs are stored—must be restricted to authorized individuals. Loss of infrastructure services can jeopardize the continuity of information processing and negatively impact operations as a whole. The physical access controls used for these support systems must reflect the importance of the information processing systems they serve. In most cases, locked doors will suffice to safeguard these support systems.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 5 of 13

3 Environmental Protection Controls

Based on the results of an Information Security Risk Assessment., environmental protection controls ensure that the computing resources are maintained in an environment that ensures the continued operation of the service and reduces the effects of disaster, whether man-made or natural.

3.1 Physical Layout and Location

Any building that contains information processing areas must, at a minimum, conform to local and federal construction regulations, especially regulations that refer to natural catastrophes (for example, fire, flood, earthquake, and hurricane). When selecting a new site, the City agency must consider the presence of such threats and avoid high-risk conditions where possible. In particular, locations with the potential for water damage must be avoided when selecting information processing areas (for example, locations below ground level and those under sewer lines, showers, cafeterias, or where water or drainage malfunctions can occur).

3.2 Fire Protection

Controls must be implemented to minimize the risks and effects of a fire within the information processing areas or spreading from an adjoining area. The degree of automatic fire detection and suppression mechanisms deployed depends on the criticality of the information processing system, based on the results of an Information Security Risk Assessment. Data centers must have installed approved fire-suppression systems or dry-pipe sprinkler systems and heat sensors. Closed-area network server rooms may have only smoke detectors and fire extinguishers. Information processing areas must use fire-detection and suppression equipment. Detection devices must alert appropriate personnel. These employees must be must properly trained for fire emergencies.

3.3 Heating, Ventilation, and Air-Conditioning

The computer environment must be protected from damage caused by water, temperature, and humidity. In data centers, sensors and alarms must be installed to monitor the environment surrounding the computer equipment to ensure that air and water temperatures and humidity levels remain within the limits specified by the equipments' manufacturers. Water sensors must be placed in the floor and ceiling to ensure leakage detection. If proper conditions are not maintained, the City agency must configure alarm systems to summon operations and maintenance personnel to correct the situation before a business interruption occurs.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 6 of 13

3.4 Electric Power Systems

3.4.1 Backup Power for Power Outage Situations

Based on the results of an Information Security Risk Assessment computer systems and their supporting infrastructure (for example, air-conditioning and security-alarm systems) must have a dependable, consistent electrical power supplies that are free from surges and interference that could negatively affect their operation. Backup power is necessary to ensure that computer services are always available and to prevent equipment damage if normal power is lost. An uninterruptible power supply (UPS system) must be in place in case the normal power to the computer systems and supporting equipment is lost. The UPS must be monitored for status at a consistently attended location, must be tested on a weekly basis, and must be part of a preventative maintenance program. Where appropriate, generators and batteries must also be used to ensure the continuation of operations. In areas susceptible to outages of more than 15 to 30 minutes, diesel generators are recommended. Backup power facilities must be tested regularly to ensure reliable functionality.

3.4.2 Emergency Power-Off Switches

In data centers, emergency power-off switches, which shut off all power supplies, must be installed and be readily accessible, with posted notices showing their locations. These switches must be protected from unauthorized physical access.

3.4.3 Emergency Lighting

In data centers and closed server areas, automatic emergency lighting must be provided for use during power outages.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 7 of 13

4 Operational Constraints

The City agency must follow these directives to strengthen the physical access and environmental controls for data centers and other facilities housing IS facilities:

- Cleaning or repair work that requires the storage or use of flammable liquid may not be performed in computer rooms.
- Each City agency must develop a comprehensive disaster recovery plan that is reviewed quarterly and tested annually at a minimum. A copy of the plan must be kept at an offsite storage facility. Refer to the City's *Information Security Directive: Business Continuity* for further details.
- All computer units in a computer room must be controlled, if possible, by a master switch located inside the room, near the room's exit, or immediately outside the room.
- All personnel must be instructed at least every three months on using fire extinguishers, sounding and reporting fire alarms, shutting down computer equipment, removing vital storage media in the event of fire or suspected fire, minimizing the amount of combustible material in the computer room, and dealing with deliberate threats.
- Telephone numbers of the persons or agencies to call in an emergency must be posted in highly visible locations in the computer facilities.
- Data centers must be equipped with covered metal containers for waste materials. Materials that can cause problems (for example, window curtains or reams of paper and other flammable materials) must be eliminated.
- Food or drinks may not be allowed in a data center.
- The facility must have protective covering materials available, such as plastic sheeting, to guard against water damage to equipment, data storage media, and supplies.
- Each City agency building must maintain a current inventory of all information technology resources located there, including equipment, system and application software, furniture, supplies, and any other item essential to conduct business. A copy of this inventory must be kept at an offsite storage facility.
- The City agency must develop, on the basis of this directive, a written policy and procedures manual that contains directives for all aspects of physical security in the facility.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 8 of 13

5 Other Considerations

5.1 Employee Termination or Change in Job Responsibility

If an employee has a change in his or her job responsibility or is terminated for any reason, all items in his or her possession that control physical access to information must be returned. These items can include the following:

- Keys and combinations to safes, control panels, cupboards and filing cabinets, and entrances and doors
- Terminals, PCs, and their passwords (if possible)
- Telecommunications equipment
- Diskette boxes
- Personal authentication devices (for example, SecurID and random password generator)

If keys have not been returned, it may be necessary to replace locks that protect sensitive information. Combination locks must be changed at the discretion of City agency management.

All copyright, licensed, and confidential Information held on magnetic media as data, programs, operating systems, and utilities must be returned, recorded, and checked.

5.2 Insurance

Insurance coverage must complement an effective system of physical security controls. Such coverage is a countermeasure against sabotage and its impact on City agency operations. The following items must be considered, comparing the values of associated assets with the cost of insurance to mitigate losses:

- IS equipment and facilities
- Employee loyalty
- Media reconstruction
- Unexpected expenses
- Business interruption
- Errors and omissions
- Loss of items in transit
- Liability resulting from systems activities

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 9 of 13

6 Appendix A

6.1 Purpose

This document outlines the security measures for ensuring that physical access to City information assets, systems, and media is controlled and protected. Physical access to information processing and storage areas and their supporting infrastructure—communications, power, and environmental systems—must be controlled to prevent, detect, and minimize unauthorized or unintended access (for example, unauthorized information access or disruption of information processing).

This document supports the *Citywide Information Security Policy* and is complemented by other security directives and standards, which are referenced where appropriate.

6.2 Who Must Use This Directive

This directive applies to all City employees, contractors, and consultants who are responsible for the management of physical access to City information assets, systems, and media.

It is assumed that knowledgeable technical professionals will be implementing this directive. Detailed operational and control procedures are not included in this document but must be developed by the appropriate personnel.

6.3 Information Security Risk Assessment

Information Risk Management is the process of identifying risks associated with information processing, and then developing pragmatic security controls and solutions to manage the identified risks appropriately, in line with business' needs. The Citywide Information Security Risk Assessment (ISRA) (refer to the City's *Information Security Directive: Risk Assessment*) process has been developed to manage information security risks associated with operating critical information systems.

The ISRA process will determine the level of criticality for an application or infrastructure component, and hence identify an appropriate level of security controls that must be implemented to mitigate the associated information security risks. Security controls are derived from the Citywide information security policies, directives and standards.

The City seeks to ensure that all its systems are adequately protected against information security vulnerabilities and that an adequate level of accountability is applied to all critical applications. DOI CISAFE, proactively, develops and disseminates security solutions, and security policies, directives and standards, in line with City requirements.

Implementation of security controls, as identified by the ISRA process, is the responsibility of all City agencies and will be monitored for compliance by DOI CISAFE.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 10 of 13

7 Appendix B -- Areas of Responsibility for Implementation of this Document

7.1 CISAFE

The Department of Investigation (DOI) promotes and maintains integrity and efficiency in government operations. Through its Inspectors General and other investigative staff, the Department investigates and refers for prosecution City employees and contractors engaged in corrupt or fraudulent activities or unethical conduct. Investigations may involve any agency, officer, or employee of the City, as well as those who do business with, or receive benefits from, the City. The Department also analyzes and studies various aspects of the operation of City government to identify management practices, operations, and programs that can be improved. The Department provides the Mayor with recommendations for corrective actions to assist City agencies in the design and implementation of strategies to limit opportunities for criminal misconduct and waste.

Pursuant to Mayoral Directive 81-2, the DOI has been charged with responsibility for the design and implementation of a system of Electronic Data Processing Security for the City and its constituent agencies. To accomplish this task DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE).

CISAFE is responsible for the creation, development, and enforcement of consistent and cost-effective security policy, directives and standards to ensure, for the mutual benefit of all concerned, the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City computer systems.

7.2 DoITT

DoITT provides communication services to the City's Agencies and units. DoITT is responsible for the design, engineering, maintenance and testing of the systems infrastructure associated with the City's communication links and maintains the City's connections to the Internet. DoITT also is responsible for review of the above agency connectivity request to provide external DNS services and for coordinating the connectivity. DoITT must perform its services in compliance with this document.

7.3 Technology Steering Committee

Executive Order No. 43 established the City of New York's Technology Steering Committee (TSC) in October 1998. The Office of the Chief Information Officer (OCIO) was created within the Department of Information Technology and Telecommunications (DoITT) to provide the TSC with technical staff to help perform its mandated functions. Among these functions are recommending to the Mayor information technology (IT) spending priorities for all City agencies, developing the citywide IT Strategy, and sponsoring citywide technology initiatives.

In addition, the Office of the CIO seeks to identify information technology best practices found in the public, private, and nonprofit sectors and to implement them citywide as appropriate. In this way, it operates as the citywide clearinghouse for information technology-related issues.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 11 of 13

The TSC is responsible for supporting the *Citywide Information Security Policy*, guaranteeing that information security retains a high profile within the City, and ensuring that key resources are available for the ongoing development, implementation, and review of appropriate policies.

7.4 City Agency and Unit Management

City agency and unit management must review the results of the risk assessment and approve the implementation of recommended security controls to achieve a level of technical and business risks that are acceptable to the City agency, to CISAFE and to DoITT. Furthermore, City agency and unit management are responsible for ensuring that the City agency and unit systems connected via DoITT to the Internet are in compliance with this directive.

7.5 Internal Audit

The City and City agency Internal Audit (IA) departments are responsible for the assurance of controls included in this document. IA may perform periodic audits to verify that the City agency remains in compliance with this document.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 12 of 13

8 Glossary of Physical Security Terms

This section defines common terms specific to physical security. For more general security terms, refer to the Glossary of Information Security section in the *Citywide Information Security Policy*.

data center

A central data processing facility or specialized facility that serves and provides data and other services for an organization. It may contain a network operations center (NOC), which is a restricted-access area containing automated systems that constantly monitor server activity, Web traffic, and network performance and that report even slight irregularities to engineers so that they can spot potential problems before they happen.

Server

A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

uninterruptible power supply (UPS)

A device that is inserted between a primary power source, such as a) commercial utility, and the primary power input of equipment to be protected, such as a computer system, for the purpose of eliminating the effects of transient anomalies or temporary outages.

Physical Security Directive	Directive: D 5.4
Issued: April 30, 2003	Page 13 of 13

9 References

- *Citywide Information Security Policy*
- *Information Security Directive: Risk Assessment*
- *Information Security Directive: Business Continuity*



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Data Classification Policy

The Policy

The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope

This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification

All information at the City of New York and corresponding agencies will be classified at one of four levels; Public, Sensitive, Private, or Confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency's ability to perform its primary business function.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Information Valuation and Categorization

- 1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
- 2) All information assets must be valued and categorized.
- 3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
- 4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Data Steward

- 5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- 6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.
- 7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.
- 8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Information Labeling

- 9) Information within systems or processes must be marked appropriately to ensure that users will be aware of the sensitivity of the information and how it should be protected and controlled. Appropriate marking of mission critical information includes marking it as Public, Sensitive, Private, or Confidential.
- 10) All copies or reproductions maintain the same level of classification as the original.
- 11) Aggregation of data with different classification levels require reevaluation to determine if a new level of classification is needed.
- 12) All personally identifiable information should be classified at a minimum as Private.

Information Protection

- 13) Protective measures must be commensurate to the value of the data contained on the information asset.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 14)** Critical¹ information must be protected and secured during any electronic data transmission or electronic or physical media transfer.
- 15)** Critical information may be transmitted electronically over Citynet² without encryption, although it is strongly encouraged that approved encryption be used when required by regulatory requirements.
- 16)** Critical information may not be transmitted over a public network (such as the Internet) unless it is in an approved, encrypted form.

¹ Data of a higher sensitivity.

² Metro area network utilized by multiple agencies and supported by DoITT.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

PORTABLE DATA SECURITY POLICY

THE POLICY

ALL PORTABLE COMPUTING DEVICES USED TO PROCESS AND STORE CITY OF NEW YORK INFORMATION MUST BE PHYSICALLY PROTECTED AND APPROPRIATE SECURITY MEASURES PROVIDED FOR THE DATA CONTAINED.

ACCESS

- 1) Where the device supports it, the power-on, or security password, must be enabled.
- 2) Some portable computing devices limit password strength. If a password conforming to the requirements of the *Password Policy* cannot be used, then the strongest password permitted by the device should be used. Information classified as "**Confidential**" cannot be stored in the device without encryption.
- 3) Automatic login scripts, which would allow an unauthorized party access to an account without requiring a password, are prohibited.
- 4) Portable computing devices must not be left unattended at any time when remotely connected to Citynet.
- 5) Portable computing devices should be protected in accordance with the value of the information contained in the device.

PROTECTION

- 6) Confidential information must be protected at all times.
- 7) Confidential information can be stored on removable media (e.g., disks, removable drives, tapes, flash memory cards, CDs, USB memory devices) if the data is encrypted. The removable media should be physically protected (e.g., locked in a desk drawer, safe, or kept with the individual).
- 8) Laptop PCs, Smart Telephones, PDAs, etc. that can be physically carried by the user must be protected as one would protect a wallet or similar container that holds one's identity (e.g., driver's license, credit cards, etc.).
- 9) Laptop PCs, Smart Telephones, PDAs, etc. shall not be used to store or transmit information classified as "**Confidential**" (including e-mails and attachments to emails) unless these devices are in compliance with all of the City of New York Information Security Policies.
- 10) If the device is synchronized with a personal computer, the Confidential information transferred should be appropriately protected on the personal computer in accordance with the City's Information Security Policies.
- 11) Up-to-date, anti-virus software must be installed and automatic scanning enabled, when such software is available. All externally obtained media or files should be scanned before any files are opened.

USER RESPONSIBILITIES

- 12) Backup of any data stored on a portable computing device is the responsibility of the user. The backup device is must also comply with the **Citywide Portable Data Security Policy**.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 13) Confidential information must not be accessed on trains or in public places, unless the user has taken all reasonable precautions against inadvertent disclosure to unauthorized individuals.
- 14) Loss of a portable computing device or the loss of removable media that contains "**Confidential**" information must be reported to the individual's manager and to the agency's Chief Information Security Officer as soon as possible, but not later than 24 hours after detection of the loss.

DISCIPLINARY PRACTICE

- 15) When reasonable care has not been exercised in safeguarding a portable computing device, the individual may be subject to disciplinary action and be held responsible for the replacement cost if the device is lost or stolen.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

REMOTE ACCESS POLICY

THE POLICY

REMOTE ACCESS TO CITY OF NEW YORK COMPUTING RESOURCES MUST BE AUTHORIZED AND GRANTED BASED UPON INDIVIDUAL IDENTIFICATION AND PRIOR MANAGEMENT APPROVAL.

MANAGEMENT AUTHORIZATION

- 1) Management approval is required before a user is authorized to use any City networking and computing resources.
- 2) Accounts that permit access to Citynet must only be granted to users who possess an active remote access account.
- 3) Users who are not City employees, but who are in a current contractual relationship with the City, may have access to City networking and computing resources if they have met the requirements of the Personnel Security Policy:
 - a. Consultant remote access must be approved by their sponsor.
 - b. A valid non-disclosure agreement must be signed prior to granting access.

ACCESS MANAGEMENT/AUTHENTICATION

- 4) Users must be positively and individually identified and authenticated prior to being permitted access to any City networking and computing resource.
- 5) Users remotely accessing Citynet must be authenticated using strong authentication mechanisms which comply to the **Citywide Password Policy**.

REMOTE ACCESS

- 6) Remote access (including but not limited to dial-in and VPN) to City resources must be limited to DoITT authorized entry points.
- 7) Modems, or modem type devices on desktops, laptops, and servers are not authorized entry points.
- 8) No computer or computing device shall be connected simultaneously to more than one network.
- 9) The fax modem function must be appropriately configured on all network resources to not answer any incoming call requests.
- 10) Users must disconnect from the remote access connection when not actively in use.
- 11) Users should be disconnected after a maximum of one hour of no user input or activity.
 - a. This does not apply to application program inactivity. The application time-out period will be determined by the application owner.

Issued: Aug, 2007 Final Draft

Remote Access Policy



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

- b.** Users must not use any method acting in their absence to avoid the inactivity disconnect.

USER RESPONSIBILITIES

- 12)** Users are responsible for maintaining the confidentiality of passwords or other authentication mechanisms that are assigned in conjunction with the remote access service. A user's credentials must be classified as restricted information. Individual passwords must never be shared.
- 13)** Any disclosure of a password must be immediately communicated to the DoITT Help Desk or the appropriate agency contact and the password immediately changed.
- 14)** Users must protect the confidentiality and integrity of data that is accessed remotely. This includes, but is not limited to ensuring that City data is either erased from the remote device after use or appropriately protected based on the level of sensitivity of the information.
- 15)** Users have the responsibility of ensuring that all software, files and data accessed from remote locations entering the City's computing environment are properly virus scanned.

PROTECTION OF CITY INFORMATION AND COMPUTING RESOURCES

- 16)** All City of New York owned software and hardware must be returned upon conclusion of a user's employment or contract.



Security Accreditation Process

Scope

All externally accessible applications or internally accessible Citywide applications developed to support City of New York business must be built in a secure fashion. These applications must be reviewed and approved by the Citywide Chief Information Security Officer (CISO). Accreditation must be achieved prior to migrating to the production environment.

Software Development Life Cycle (SDLC)

The development of any application should follow the phases of the SDLC with checkpoints for information security assurance:

1. *Analysis*: determine the data classification
2. *Define*: determine what business functions the application is intended to address
3. *Design*: develop a technology solution leveraging tools, technology, process, and best practices to design the solution
4. *Development*: create code, build hardware, and deploy the application to QA environment.
5. *Test*: Perform unit, system, and user acceptance test cases against the QA environment.
6. *Implementation*: Deploy to production environment

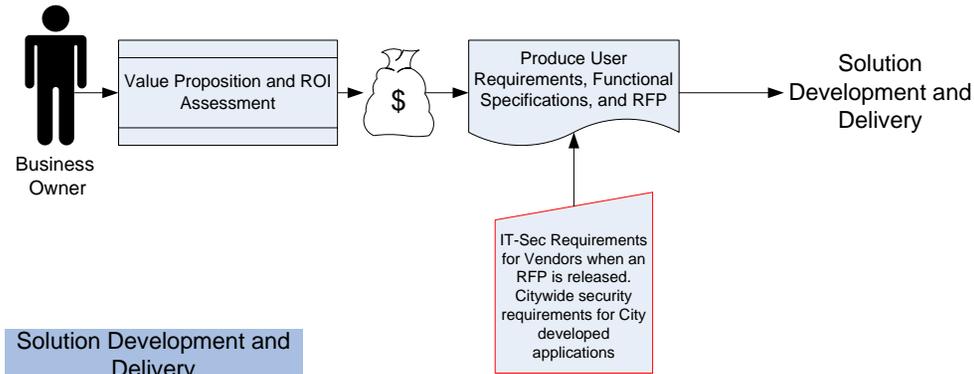
Note: This is based on the DOITT Application Development and Support SDLC presentation.

The following diagram shows depicts the DoITT SDLC and IT Security touch points along the way towards accreditation:

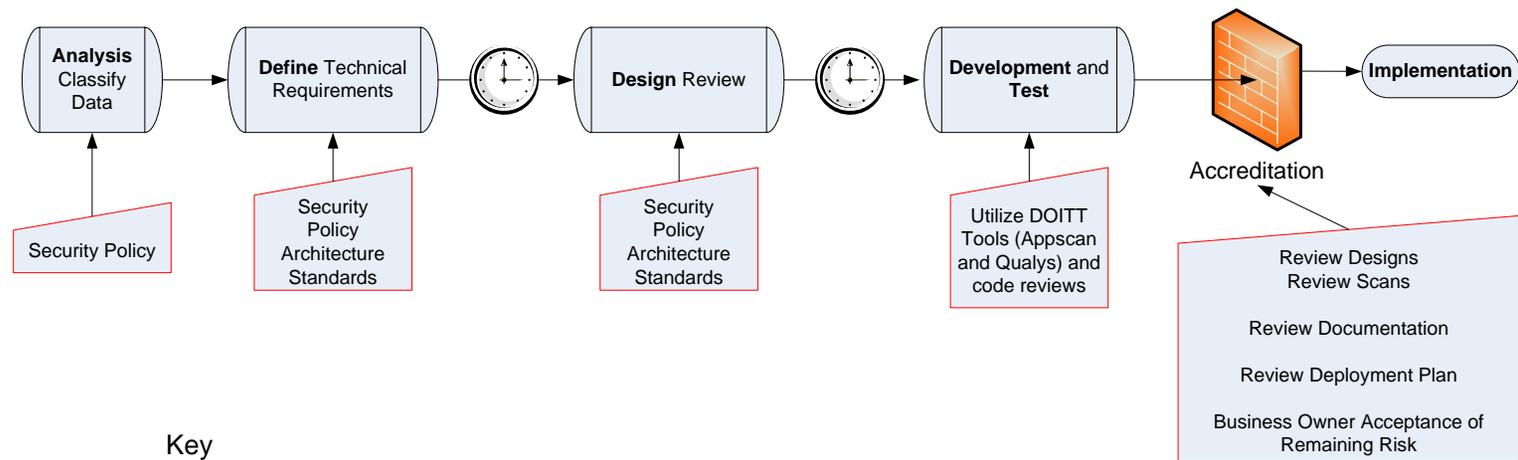


**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

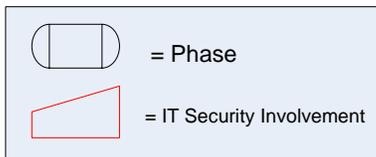
Project Initiation and Planning



Solution Development and Delivery



Key



Note: MEDIUM or HIGH application related risks or Severity 3,4, and 5 host related risks must be addressed. LOW and severity 1 and 2 risks must be addressed or accepted by the business owner.



Accreditation Process Overview

This process has been mapped to the DoITT SDLC as a baseline, but this does not make the process incompatible with agencies or vendors that use other software development methodologies. The seven steps in the process can be overlaid onto any process at any stage. From a practical standpoint, DoITT is not always in the loop from project inception. Therefore this process is designed to always start from the first phase, reviewing already completed work as necessary.

It is important to note that while projects require many meetings and discussions, the actual assessment process will use the application documentation as the authoritative source for information. Clearly written and detailed documentation is the key to ensuring an efficient and timely process.

The following steps describe the accreditation process:

- 1) In the *Analysis Phase*, the business requirements and related data fields are analyzed and classified. Data classification provides a critical foundation for information security decisions. To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust. In this phase, it is important to assess data classification based on the content itself, where it was collected, where it will be stored, and how it will be queried. Input at this stage will determine the initial data classification of the system data and high-level security control requirements. Ultimately, data must be classified by the business owner of the project, with appropriate documented statement, according to the Data Classification policy.

Depending on the data classification and application exposure it may be required to perform an independent third party security assessment of the application in the Accredited phase. This may include ethical hacking, design and code reviews as well as policy compliance reviews. Appropriate budgeting must be allocated at this time in case it is found that a 3rd Party assessment required. Appendix A defines guidelines for determining if a 3rd Party Audit is required.

- 2) During the *Define Phase* DOITT IT Security Engineering (ITSecEng) will look at functional requirements and assist in defining technical requirements for security.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 3) During the *Design Phase*, ITSecEng can provide guidance to the business owner in applying detailed design requirements for security controls to the application design. These requirements will be derived from citywide policies, standards, guidelines, best practices, and the DOITT Citynet Security Reference Architecture.

Some **examples** of these design requirements are:

1. All DMZ hosted applications must support a 3-Tier architecture.
2. Applications that handle Sensitive or Confidential information must use end to end encryption.
3. All passwords must be stored hashed and communicated with encryption.

At this stage, clearly written documentation describing application design, logical and physical environment, data flows, intended users, authentication and authorization parameters as well as security controls build into any part of the application or the environment should be prepared and presented to ITSecEng. This documentation should be updated during the rest of the development cycle. See IT Security Documentation Guidelines for more information.

- 4) In the *Build* and *Test* phases, ITSecEng can assist the developers in tactical design issues. Development and QA teams are encouraged to use peer code reviews, application scanning tools such as Appscan and consultations with the ITSecEng team on any security issues is greatly encouraged and will prevent negative impact to the time line. If a 3rd Party security assessment has been specified, it will be done at this point and the results will be reviewed in the next stage.
- 5) After the application is ready for release ITSecEng will facilitate a system vulnerability assessment and an application vulnerability assessment using Qualys and Appscan to uncover issues. The process is as follows:
- A) The scan(s) will be initiated and the results reviewed. All Medium and High vulnerabilities must be addressed. Low vulnerabilities should be reviewed by the agency applications team. ITSecEng will coordinate with the agency counterparts to remediate identified vulnerabilities. Vulnerabilities will be addressed by:
 - i. Fixing the vulnerabilities
 - ii. Review and confirmation of any false positive(s).
 - B) The project manager will produce an issues log outlining all high and medium vulnerabilities and their resolution.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- C) Scans will be rerun until all Medium or High vulnerabilities are resolved.
 - D) The business owner will provide ITSecEng a written communication stating the acceptance of any LOW or INFORMATIONAL vulnerabilities that were not addressed.
 - E) Results from any 3rd Party assessments will be reviewed and their remediation will be verified.
 - F) ITSecEng will review the final scan(s) and the issues log and provide a written approval of the scan results.
- 6) During the final Accredited phase, the following criteria will be reviewed and presented to the Citywide CISO:

Accreditation Review Criteria

Confirm the following requirements have been met:
1. Data has been classified
2. Data security controls match data classification levels
3. System documentation meets guidelines (See IT Security Documentation Guidelines)
4. Security Architecture complies with CityNet Security Reference Architecture
5. System authentication credentials are stored in the Enterprise directory
6. Proper regulatory and industry standards and applicable laws (such as HIPAA, PCI) are complied with.
7. System names comply with enterprise naming standards
8. System utilized proper enterprise DNS and SMTP services.
9. Qualys scans of all system components are complete and all severity 3,4 and 5 issues have been addressed
10. Results from any 3 rd Party assessments will be reviewed and their remediation will be verified.
11. Watchfire application scans of are complete and all medium and high severity issues have been addressed

- 7) The Citywide CISO will provide an acknowledgment of satisfactory completion of the accreditation process. It is important to note that while successful completion of accreditation process enhances the security posture of the application and the enterprise in general, it in no way certifies the application as 100% secure and in no way transfers any residual security related risks to the IT Security group. Risks to the Availability, Integrity and Confidentiality of the data, the application and its supporting environment reside solely at the business owner of the application.
- 8) The project owner will provide a written acceptance of the security of the application assuming any residual risk. The project owner also agrees to re-



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

accredit the application in case of significant changes, added functionality or changes in data classification levels.

- 9) Citywide CISO will provide final sign-off and the developer will fill out the appropriate security change forms and schedule a window for migration to the production environment.

Exceptions

When consensus cannot be reached between the Business Owner and the Citywide CISO over the risks associated with an accreditation process finding, an exception can be requested. In recognition of the risk management approach in which policy exceptions are applied, an exception from a policy provision may be requested and granted due to unusual and/or exceptional circumstances. The approval process for exception requests shall be as follows:

- The agency desiring an exception to a policy provision shall complete a thorough analysis to determine if the unusual and/or exceptional circumstances will have any potential impact on the security of Citynet, any other City of New York agency, or any customer or partner.
- The agency desiring an exception to a policy provision will also complete an analysis to determine if approval of an exception for the extraordinary circumstances would adversely affect compliance with any legal or regulatory requirements.
- If the Agency determines that there will be no adverse impact or if there is a minimal adverse impact on another party, that agency's commissioner sends their request to the DoITT Commissioner.
- The exception request will be reviewed by the Commissioner of DoITT with input from the Citywide CISO to confirm the impact is acceptable.
- If there is non-concurrence, the final decision to approve the exception rests with the DoITT Commissioner and the Citywide CISO.
- If an exception request is disapproved, it is the responsibility of the requesting City agency to remediate the circumstances that required the exception request.



Appendix A – Determining the need for a 3rd Party Security Assessment

The goal of a 3rd Party Security Assessment is the preemptive discovery of application security vulnerabilities. When determining the need for an assessment, the most important considerations must be the volume and classification of the data and the transactional complexity of the application. The more complex the application, the more potential opportunities exist for a determined adversary to circumvent the application security controls. The value of the data should also be considered. Using this information for context, the Business Owner should consult his agency security lead as well as the DoITT CISO, to determine if a 3rd Party Security Assessment is right for their application.

The Open Web Application Security Project (<http://www.owasp.org>) can provide more background information on application security assessments.



Security Architecture Standard

Purpose

Information security must be an integral and mandatory part of any system or infrastructure designed to provide access to information. It is very difficult to add information security measures after a system has been designed, and the resulting system may not comply with City of New York Information Security policies. This document will define various models and security controls so that a system can be built to interface with the existing architecture.

Scope

All externally accessible applications or internally accessible Citywide applications developed to support City of New York business must be built in a secure fashion. These applications must be reviewed and approved by the Citywide Chief Information Security Officer (CISO). Accreditation must be achieved prior to migrating to the production environment.

Background

Citynet is a Department of Information Technology and Telecommunications (DoITT) operated, trusted network that interconnects city agencies, hosts citywide applications, and provides Internet-based services citywide. DoITT utilizes policies, processes, and technology to protect this network, its applications, its hosts, and the data processed therein. This layered security design comprises the Citynet Security Architecture.

Security Policy

The Citywide Chief Information Security Officer (CISO) has responsibility for ensuring appropriate security controls are applied to protect confidentiality, integrity, and availability of City of New York information systems.

The purpose of policies is to provide guidance for selecting and specifying appropriate security controls for information systems. These policies have been developed to:

- Facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for City systems;
- Facilitate development of City Baseline Security Controls for information systems based on the confidentiality, integrity, and availability requirements;



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- Create a foundation for the development of information system security controls that meet legal requirements, industry best practices, and City objectives.
- Facilitate the development of consistent assessment methods and procedures for testing security controls effectiveness.

Data Classification

The Data Classification Policy provides a critical foundation for information security decisions. To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

All information at the City of New York and corresponding agencies will be classified at one of four levels; Public, Sensitive, Private, or Confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of confidentiality.
- **Private**—This information is for agency use only, and its disclosure would damage the reputation of the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency.

When looking at the information stored or processed by an application, it is important to assess its classification based on the content itself, where it was collected, where it will be stored, and how it will be queried.

For example, a name or address may be publicly available information, if it was collected by a HIPAA application, and is stored in a shared database with other application data that can tie the name to a medical condition, the classification changes. The Citywide Chief Information Security Officer will use this context as part of his decision making.

Security Accreditation Process

All externally accessible applications or internally accessible Citywide applications developed to support City of New York business must be built in a secure fashion. These applications must be reviewed and approved by the Citywide Chief Information Security Officer (CISO). Accreditation must be



achieved prior to migrating to the production environment. See the “**Security Accreditation Process**” document for more information.

Security Zones

Citynet is logically divided into security zones, where corresponding security controls are defined based on security policy, threats and exposure.

1. **Untrusted** – Systems that are unmonitored and unprotected by DoITT security infrastructure.
2. **DMZ** – Systems that are protected and monitored by DoITT security infrastructure, but have some direct exposure to the Internet.
3. **Partner** - External systems that owned by third parties who are bound to abide by Citywide policies.
4. **Trusted** – Internal systems that are part of shared service environments and are protected and monitored by DoITT security infrastructure.
5. **Most Trusted** – Internal LAN segments, connected to Citynet, without any external connections that are protected by firewalls

EXAMPLE: The following systems are classified as such:

1. **Untrusted** - Internet Perimeter
2. **DMZ** – 2-Tier and 3-Tier DMZ
3. **Partner** – Extranet Connections, ISP Agencies, NYCWin
4. **Trusted** – CSC Hosting, Citynet Agencies
5. **Most Trusted** – DOITT LAN, Telephony LAN

Perimeter

A traditional information security paradigm is the “perimeter”. The perimeter logically demarcates between the uncontrolled Internet and internal networks that fall under some level of DoITT control. The Citynet perimeter is defined by the following touch points:

1. Internet connections at Financial Information Services Agency (FISA) and 11 Metrotech Center
2. Extranet connections at 11 Metrotech Center and 2 Lafayette Avenue
3. Site to Site VPN Connections
4. Agency Connections
5. NYCWIN wireless infrastructure
6. Out of band connections

Internet Access

All outgoing Internet access must be authenticated, monitored, and tracked. For authentication, individual agencies may pass their local Internet traffic through an agency proxy. Agencies may also use the DoITT shared proxy servers in the



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

CSC hosting environment. DoITT also maintains a content filter service at the perimeter, which forces all traffic through a content filter to block inappropriate and dangerous internet access. The content filter also controls access for those users who are restricted to viewing specifically authorized websites. There are some agencies who maintain their legacy Internet connections through the DOITT DMZ.

NOTE: The Department of Investigations Inspector General may request these logs in hard or electronic format in support of an investigation.

Citynet Connectivity and Remote Access

There are entities that transact business with the City of New York who need access to Citywide applications and systems. There are 8 main connectivity models that are supported by DoITT:

1. Direct Agency connectivity – The most common Citynet connections are those between the Agencies and Citynet. These connections are facilitated through DoITT routers at key locations throughout the City of New York. There are no access controls on these connections.
2. ISP Agency connectivity – There are some agencies that maintain their own connections to the Internet as well as connections to Citynet. These agencies are separated from Citynet by a firewall since DoITT does not control these ISP connections and cannot maintain the integrity of Citynet without this control.
3. Extranets (System to system connections via dedicated connections)– These include partners such as financial institutions, that maintain dedicated connections (ie. T1) to City financial systems. These dedicated connections terminate on the Internet perimeter and are controlled by rules in the external firewalls.
4. VPN Connections (System to system connections via the Internet)– These include partners such as financial institutions, that require persistent connections to City financial systems. These connections are supported through site to site IPsec VPN tunnels that terminate on the Internet perimeter. DoITT supports a VPN “Edge” device for smaller remote offices that may not have IPsec capable perimeter equipment.
5. Application specific connections – When an external vendor or business partner needs access to a specific extranet or internal application, this access is provisioned through SSL VPN. The SSL VPN allows external parties to connect to DoITT via their standard web browser, eliminating the need for a heavy client to be installed on their workstation. This access type is also used for applications that need to be exposed to a known set of external users.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

6. General purpose remote access – DoITT provisions SSL VPN accounts for employees who need remote access for “telework.”
7. Client to Server connections – When a vendor or other entity needs access to a system that is difficult to support via SSL VPN, client IPsec connections can be used.
8. Government extranet connections - Government extranet connections such as those from NYS terminate in a special DMZ at 2 Lafayette.

DoITT maintains VPN tunnels to many prominent partners such as SIAC and CUNY. Citynet is not to be used to facilitate pass-through connectivity between VPN-connected agencies and other remote resources.

ISP Agency connectivity through the Citywall firewalls is designed to facilitate a controlled subset of traffic exchange. If an agency desires to take advantage of the full offering of DoITT managed services, such as email, server, and desktop support, it must first remove its ISP connection and become an integrated Citynet Agency.

To ensure effective security monitoring, IPsec tunnels should not transit firewalls. In some unique cases, exceptions have been made where tunnels are terminated and reestablished as they cross DoITT firewall boundaries, but these connections are discouraged.

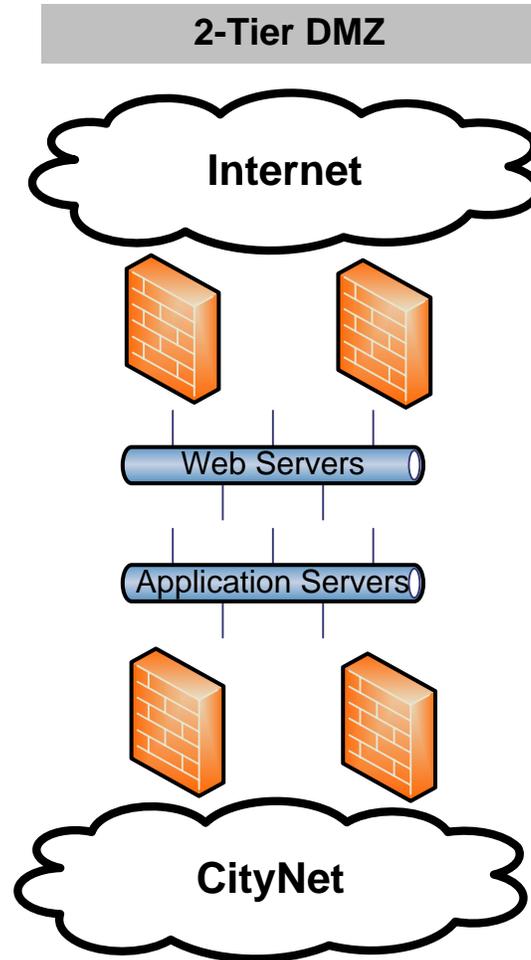
DMZ

A DMZ is a set of logical networks that has direct access to the Internet as well as internal networks. It acts a buffer between the untrusted Internet and the trusted internal networks, allowing select services to be exposed to the Internet while not doing so directly from trusted areas.

Data cannot be stored on servers hosted within the DoITT DMZs.

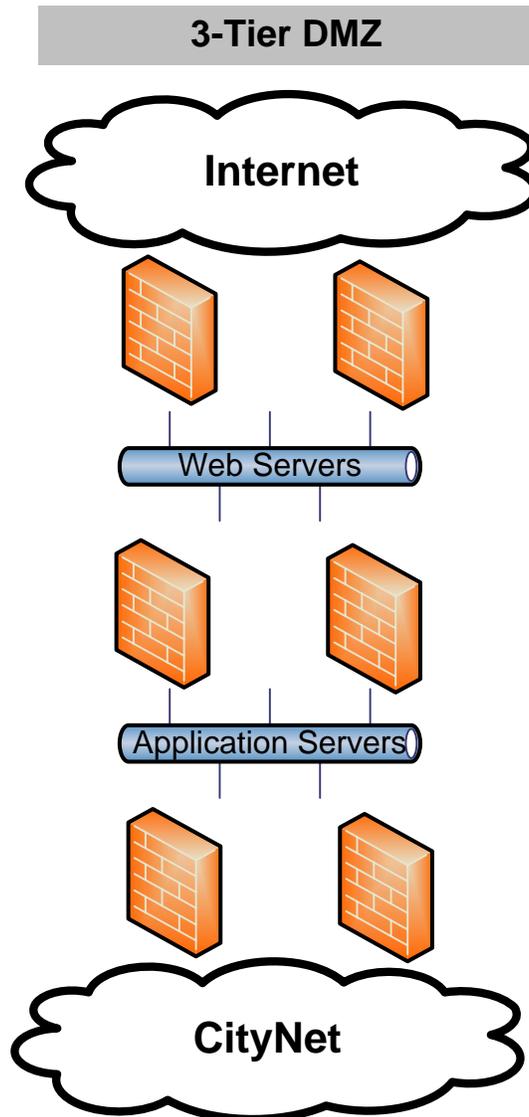


1. DoITT maintains 2 DMZ environments for hosting of Internet facing applications. The 2-Tier DMZ resides at 2 geographically diverse sites for redundancy. Web and App tiers are not separated by firewalls, but are maintained in different VLANs with the App tier using private, non-routable addresses.





2. The 3-Tier DMZ maintains a Web, App, and DB layer separation with 3 firewalls. The 3-Tier DMZ is only built out in 11MTC.

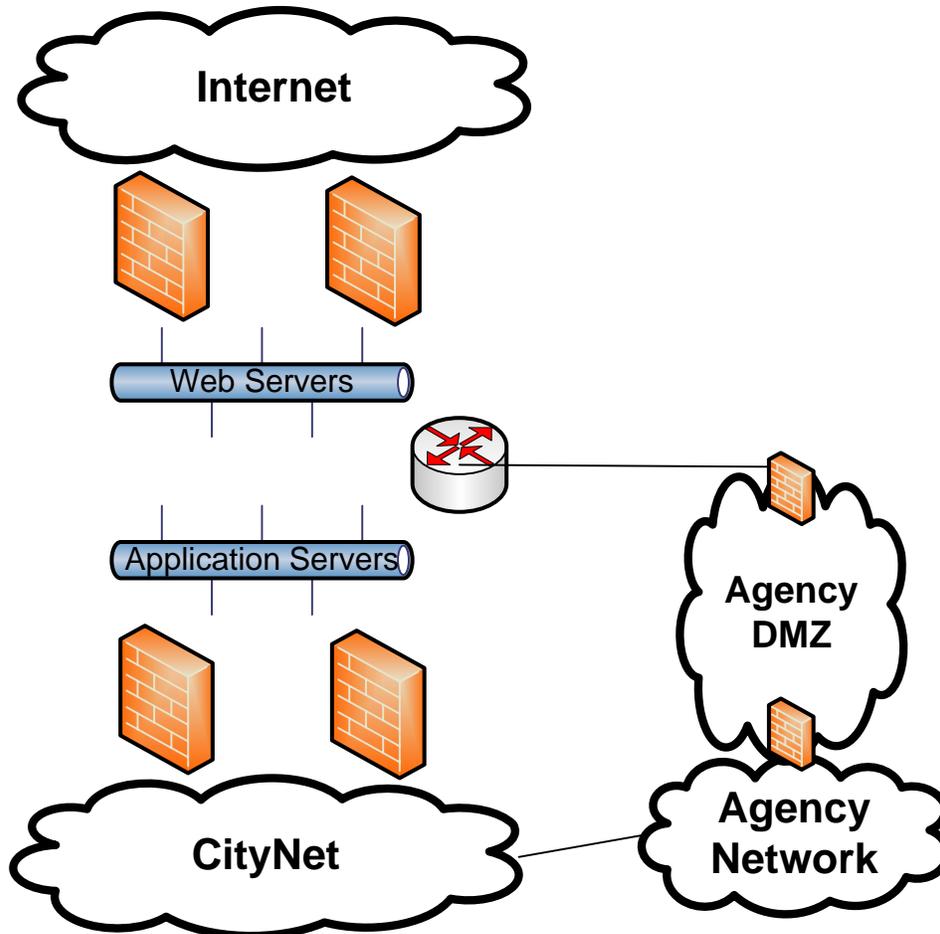


3. All new applications will be built to the 3-Tier model, wherever appropriate, and existing applications are being migrated to the new environment.



4. There are some agencies that maintain dedicated T1 lines to a router in the 2-Tier DMZ for the purposes of supporting a local DMZ and Internet access. Existing connections are grandfathered and connections are discouraged. New connections will not be approved.

Agency DMZ



Note: Applications that have been developed primarily for internal users, but have a limited external user base will not be exposed to the Internet and will use VPN for access.



Security Monitoring

DoITT maintains a number of monitoring tools that collect and analyze information that moves across Citynet.

1. *Network* – intrusion detection (IDS) and behavior analysis tools collect information from the network through direct observation and Netflow statistical analysis.
2. *Event Based* – security information management (SEIM) tool collects log events from firewalls.
3. *Host Based Intrusion Prevention* - Agents collect information on unauthorized changes made to systems.

Email Protection

DoITT maintains two redundant email gateway infrastructures that provide anti-spam and anti-virus protection for email that flows through Citynet. One set of gateways process email transiting the Internet perimeter. The other gateways process inter-agency email (including outbound agency email) for agencies that cannot route email via DNS and cannot provide anti-virus gateway services. DoITT anti-spam controls are configured less granularly, and agencies may use local controls for more granular control.

Any email (excluding ISP Agencies) that enters or exits Citynet must first pass through the DoITT mail gateways for anti-virus and anti-spam scanning.

Citywide Directory Services

DoITT maintains an Enterprise LDAP directory service that provides centralized authentication services and Agency directory interoperability. This service should be used for all authentication and authorizations needs. Application specific and proprietary credential stores are strongly discouraged.

Telephony

Citywide Telephony Services (currently 311 and 1 Center St) are physically located behind firewalls in order to protect from Security attacks from Citynet and to prevent unauthorized network level access.

Policies related to the environment

1. There are 3 Security Zones
 - a. Nortel Telephony Server LAN" **Most Trusted**
 - b. "3rd Party Server DMZ" **DMZ**
 - c. "External" **Trusted.**



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

2. PBX is located in the “Most Trusted” Zone.
3. Servers and components that need to talk to the PBX should be located in the Most Trusted Zone.
4. Components from DMZ or Trusted zone are not authorized to talk across network to the PBX. This is to prevent PBX IP stack from being overloaded by external communications except from Nortel authorized products that are certified to communicate with a PBX in a proper manner.(due to a security Nortel recommendation).
5. Third Party Servers and components that are related to Telephony will be located in DMZ Zone.
6. Servers and components in DMZ Zone are authorized to talk to **non PBX** Servers and Components in the Trusted Zone by firewall rules.
7. Firewall Policy requirements

Traffic Flow	Firewall Access Rules
CityNET > Inside	Access Rule controlled on per IP host basis
CityNET > DMZ	Access Rule controlled on per IP host basis
Inside > CityNET	No restrictions
DMZ > Citynet	No restrictions
Inside > DMZ	No restrictions
DMZ > Inside	Access Rule controlled on per IP host basis

Digital Certificates

Digital certificates play a key role in effective deployment of SSL based technologies and PKI. DoITT maintains an internal certificate authority for the provisioning and revocation of internally used certificates. DoITT facilitates the procurement of 3rd party certificates from vendors such as Verisign, for publicly facing applications.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

USER RESPONSIBILITIES POLICY

THE POLICY

ALL USERS OF THE CITY OF NEW YORK SYSTEMS MUST COMPLY WITH CITYWIDE INFORMATION SECURITY POLICIES.

INFORMATION PROTECTION RESPONSIBILITIES

- 1) All users, consultants, and contractors are responsible and accountable for safeguarding information assets from unauthorized modification, disclosure, and destruction.
- 2) Critical data and removable data devices (USB drives, CDs, external drives, etc) must be protected by appropriate physical means from modification, theft, or unauthorized access. All removable media must meet the requirements set forth in the ***Citywide Portable Data Security Policy***.
- 3) Users may not install unauthorized access points (wired or wireless) to Citynet.
- 4) Confidential agency or citizen data must be controlled in accordance with pertinent regulatory requirements and City of New York policies.
 - a. Access to electronic data should be appropriately limited to appropriate users.
 - b. Paper documents must be filed and stored in a locked device when not in use.
- 5) When faxing sensitive information, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
- 6) When finished faxing, copying or printing all documents should be removed from the common area.
- 7) Users must screen lock their active workstations when left unattended.
- 8) Users must utilize passwords to protect city-issued PDA devices and voice mail systems.
- 9) All City of New York assets must be returned upon a user's end of employment or conclusion of contract.

PASSWORD CONFIDENTIALITY

- 10) Individual users must properly protect credentials¹ for their accounts. Individual credentials must never be shared.
- 11) The use of group IDs is prohibited.
- 12) Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.

¹ Detail entered to gain access to a system. Normally credentials consist of a user ID and password combination.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

PASSWORD REQUIREMENTS

- 13) Passwords must be constructed in accordance with the Citywide Password Policy. It must have a minimum of eight (8) characters and consist of at least one (1) alphanumeric character and at least one (1) numeric character.
- 14) Passwords should not be composed of easily guessed words, such as words founds in dictionaries, a user's own user IDs, proper names, or other criteria that can be associated to the user.
 - a. Users should not select passwords that contain personally identifiable numbers such as their phone extension, Social Security number or home zip code.
- 15) PINs for Blackberry, PDA, and voicemail must be a minimum of four (4) digits.
- 16) Passwords must be changed every ninety (90) days.
 - a. Passwords cannot be changed more than once a day.
 - b. Users cannot reuse any of the past four (4) passwords

PRIVACY & CONFIDENTIALITY CONSIDERATIONS

- 17) Computer systems and all related computing equipment are the property of the City of New York. Users have no right to privacy when using City computing resources. All content and traffic on Citynet may be monitored and reviewed by management.
- 18) Unauthorized use of computing resources may result in disciplinary actions.
- 19) Impersonating another user is explicitly prohibited.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

WIRELESS SECURITY POLICY

THE POLICY

WIRELESS DEVICES OR NETWORKS USED TO ACCESS, STORE, PROCESS, OR TRANSMIT CITY OF NEW YORK INFORMATION OR ACCESS CITYNET MUST BE IMPLEMENTED IN A SECURE MANNER.

BACKGROUND

Wireless devices and networks enable un-tethered communications to mobile users. Improperly installed, configured or managed wireless technology presents a significant risk to the confidentiality of information. Wireless network security refers to the protection of wireless network hardware, software, and the information contained in them from threats caused by the inherent vulnerabilities in the technology and its implementation.

SCOPE

This policy applies to all wireless devices, networks, services, and technologies used to access, store, process or transmit city information or connect to Citynet. The term “wireless” refers to any technology that does not use cables.

Wireless includes radio frequency (i.e. satellite, microwave, radio) and optical (i.e. infrared) technologies.

Wireless networks include both wireless local area networks (WLANs) and wireless wide area networks.

Wireless devices are any end-user device that uses wireless technology to communicate. These include but are not limited to: Personal Digital Assistants (PDAs), cellular phones, laptop computers, printers, wireless keyboards, wireless mice or trackballs, and bar code scanners

Wireless Network Nodes are network elements that terminate one end of the wireless communication. That communication may be between a wireless device and a wireless network element or between two wireless network elements.

Wireless Bridges are wireless transceivers used to connect two or more remote networks. They are typically used to provide campus building-to-building wireless connectivity

APPROPRIATE USE

- 1) Wireless technology may be used to access, store, process or transmit City of New York business and connect to Citynet’s infrastructure provided that it conforms to all applicable DoITT Information Security Policies including but not limited to this policy.
- 2) Wireless devices may not be used to gain or attempt to gain unauthorized access to any network. This includes accessing Citynet, external non-city networks and the internet where the user has not been granted access.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 3) Only approved services and applications may be used with wireless devices.
- 4) Any planned wireless connection(s) must be reviewed and approved in advance of installation by the local agency including the agency CISO. If the wireless connection(s) provide access to Citynet, or a network connected to Citynet, then approval must include DoITT.
- 5) The Wireless network must have a disaster recovery plan if required based on business function of the applications running on the network.

ACCESS CONTROL

- 6) Access to the city's networking and computing infrastructure via a wireless connection is considered remote access and must utilize strong authentication and encryption.
- 7) The Agency must use the current City of New York wireless standard at the time of the implementation of their wireless system.
- 8) Appropriate encryption utilizing approved ciphers must be used.

RISK ASSESSMENT

The agency CISO should employ security measures commensurate with the risk associated with the wireless network. If the network is used for transmission of business sensitive material, classified communications or supports City critical services the risk of loss in the event of an attack on the wireless network, or loss of service can be extensive.

- 9) Due to the ever changing threats and vulnerabilities, risk assessments should be conducted on a periodic basis no less than annually to provide an accurate picture of the total risk to the organization.
- 10) A risk assessment should be performed to ensure the capabilities of protection for the technologies utilized. A risk assessment should include but not be limited to; identifying data sensitivity, network vulnerabilities, and critical services. The focus should be to identify potential threats and vulnerabilities.

AUTHENTICATION

- 11) All users of WLANs are required to authenticate before being allowed to access the network.