



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: July 28, 2008 Final Version 1.1

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.