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 provided they meet the requirements of the Personnel Security Policy and the following:
    a. They are physically located inside US territory. Remote access from locations outside of the territory of the United States of America may only be granted to employees of US based service providers who are assigned to overseas office locations.

    b. Consultant remote access is approved in writing by their sponsor.

    c. The consultant has provided written acknowledgement of receipt of the Citywide User Responsibilities Policy.

    d. Any application for exception to [a-c] must be submitted by the requesting agency head to the Citywide CISO.

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 with 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 services.
7) Modems, or modem type devices on desktops, laptops, and servers are not authorized entry points.
8) The fax modem function must be appropriately configured on all network resources to not answer any incoming call requests.
9) Users must disconnect from the remote access connection when not actively in use and they must 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.

b. Users must not use any method acting in their absence to avoid the inactivity disconnect.

User Responsibilities

10) 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.

11) Any disclosure of a password must be immediately communicated to the DoITT Help Desk or the appropriate agency contact and the password immediately changed.

12) 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.

13) 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

14) All City of New York owned software and hardware must be returned upon conclusion of a user’s employment or contract.

Document Revision History

Date	Description
July 28, 2008	**Version 1.1** Issued.
June 16, 2011	**Version 1.2** Updated header with new NYC logo and added this revision history table to the document.
June 28, 2012	**Version 1.3** Expanded bullet # 3: non-City employees requesting remote access must be located in US territory; service providers may not export City data classified as PRIVATE or CONFIDENTIAL outside the United States; and requests for exceptions must be must be submitted by the requesting agency head to the Citywide CISO.
February 13, 2013	**Version 1.4.** Removed the following statement because this topic is already covered in the Citywide Service Provider Policy: 3c) “Service providers may not export City data classified as PRIVATE or CONFIDENTIAL outside the United States.”
Sept. 9, 2014	**Version 1.5** Policy review and minor formatting updates.