



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

USER RESPONSIBILITIES POLICY

THE POLICY

ALL USERS OF 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

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

individual user. Passwords that are written should not reference the account or data store they protect.

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 found 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.

ACKNOWLEDGEMENT

- 20) Every user of City of New York computing resources will receive a copy of the Citywide User Responsibilities Policy and sign an acknowledgement of receipt and understanding.