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) Agency 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 users.
    b. Documents classified PRIVATE or CONFIDENTIAL must be filed and stored appropriately 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) Passwords and PINs:
    - Must never be shared or displayed on screen.
    - Must be changed when there is any indication of system or password compromise.
11) Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored in a secure location to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.

Password Requirements

12) Passwords and PINs must have a minimum length of eight (8) characters with the exception of voice mail systems, and Blackberry and PDA devices issued by the City which must use a password or PIN of at least 4 alphanumeric characters.

13) Passwords must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character.

14) Passwords must not be derived from easily guessed, common words or phrases such as those found in dictionaries (English and non-English), nor should they be constructed from user IDs, proper names or other names, words, numbers or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or zip code).

15) Passwords must be changed every ninety (90) days.

16) Users cannot re-use any of the past four (4) passwords.

17) Passwords used by a person on City of New York systems should be different from any passwords used by the same person on non-City of New York systems (for example, on accounts used on social networking, ecommerce and other personal online sites). In the event that a personal (non-City) account password is compromised, this reduces the risk to City systems

Privacy and Confidentiality Considerations

18) 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.
19) Unauthorized use of computing resources may result in disciplinary actions.
20) Impersonating another user is explicitly prohibited.

Acknowledgement

21) 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.

Document Revision History

Date	Description
May 5, 2010	**Version 1.3** Page 1, paragraph 4: "Confidential Agency or citizen data" changed to "Agency Data." Page 1, paragraph 4b: "Paper documents must be filed and stored in a locked device when not in use" was changed to "Documents classified as PRIVATE or CONFIDENTIAL must be filed and stored appropriately when not in use.
June 16, 2011	**Version 1.4** Updated header with new NYC logo and added this revision history table to the document.
November 29, 2012	**Version 1.5** Added the following text: *Passwords used by a person on City of New York systems should be different from any passwords used by the same person on non-City of New York systems (for example, on accounts used on social networking, ecommerce and other personal online sites). In the event that a personal (non-City) account password is compromised, this reduces the risk to City systems.*