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 Citywide 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. In a situation of accidental loss or theft of a portable device the appropriate parties should be notified. Where the device permits, the data should be remotely wiped.
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 also bound to the **Portable Data Security Policy**.
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.

Document Revision History

Date	Description
September 7, 2007	**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.
April 19, 2012	**Version 1.3** Changed classification of this policy from sensitive to public.