Information
Technology &
Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Mobile Computing Device Security Policy

The Policy

All mobile computing devices and related virtual devices (hereafter referred to collectively as mobile computing devices) which access and/or store City of New York data must be configured, managed, used and discarded in accordance with this and all applicable Citywide security policies, standards and processes.

Mobile computing devices may not store City of New York data classified as CONFIDENTIAL. Please see the Citywide Data Classification Policy for details on this policy.

Scope

For the purposes of Citywide Information Security Policy, a mobile computing device is any portable device which has a central processing unit (CPU), networking and storage capability and is not running a workstation-grade operating system. A mobile computing device includes devices such as:

- Commercial, off-the-shelf, general-purpose mobile phones, smart phones, PDAs, tablets.
- Special purpose smart phones and other portable devices designed and/or customized to work with an internal City/Agency application to provide functionality not available on a general-purpose mobile device (e.g., parking ticket scanners).

The following table details the applicability of this policy:

Scenario	This Policy Applies?
City Data classified as SENSITIVE, PRIVATE or CONFIDENTIAL is accessed by the device	Yes
Device is used for authenticated logins to City applications	Yes
PUBLIC data is accessed through a public-facing application.	No
City email systems are accessed from mobile computing devices through a web browser and DoITT-approved, web-based applications such as Outlook Web Access (OWA).	No

Exception: Where SENSITIVE or PRIVATE data is accessed through a public-facing application and that data pertains strictly to the individual accessing the data, this policy does not apply. For example, a user accesses his/her account information through a public-facing application with a mobile computing device. The application gives the user access to his/her own birthday, social security number and driver's license number. This policy does not apply as long as the user can only access data which pertains to him or herself and to nobody else.

Device Authorization, Management and Authentication

1) Mobile computing devices must be authorized by DoITT to access and/or store City of New York data. Minimum requirements include the following device capabilities:

   a. Encryption which complies with the Citywide Encryption Policy and Standard.

   b. Remote wipe support (permits removal of all data from the device and resets the settings to the factory defaults in the event the device is reported lost or stolen).

   c. Where email will be accessed from the device, support for Microsoft ActiveSync or Blackberry Enterprise Server is required.

2) Authorized mobile computing devices falling within the scope of this policy may access and/or store City data only where managed by a DoITT approved and accredited centralized mobile device management (MDM) solution.

3) Life-cycle provisioning and de-provisioning procedures for mobile computing devices must be documented and implemented by each agency.

4) As per the Citywide Identity Management Security Policy, "all access to City of New York systems must be authorized and based upon individual identification and authentication." This includes all mobile computing devices, (whether City/Agency provided or personally owned).

BYOD[1] − Use of Personal Mobile Devices to Access and/or Store City Data

5) At the discretion of an agency head, or his/her designee, a personally owned mobile computing device (non-City property) may be used to access and/or store City data provided that the following conditions are met:

   a) The device complies with this policy and all applicable Citywide security policies, standards and procedures.

   b) The owner of the mobile device and his/her manager have provided their written consent to follow applicable Citywide security policies and standards.

   c) As part of this written consent, the owner/user of the mobile computing device understands and agrees that, in the event of an investigation concerning a suspected security incident, the device and any relevant activity on it may be monitored and/or remotely fully wiped (if necessary) and the user will have no expectation of privacy pertaining to any activities or data on the device.

6) Responsibility for the storage, backup and retrieval of personal information is the

[1] The use of personal mobile computing devices within an organization is commonly referred to as BYOD or "bring your own device."

responsibility of the user.

7) Devices which have been jail-broken, rooted or otherwise modified in an unauthorized manner may not be used.

8) Violations of this policy may result in the revocation of access privileges through the device and/or disciplinary action up to and including termination of employment.

Document Revision History

Date	Description
June 28, 2012	**Version 1.0** Initial draft
Sept. 9, 2014	**Version 1.1** Policy review and minor formatting updates.
April 1, 2015	**Version 1.2** Updated paragraph 5c for clarification.
April 13, 2016	**Version 1.3** Updated paragraph 5c for clarification.