COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Mobile Device Standard**	Number: **STD-ENSS030**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of: Shirley A. Monroe Shirley A. Monroe, Dir of Div of Technical Engineering
Date Revised: **10/24/2013**	

Abstract

The purpose of this standard is to describe the department's minimum expectations for secure mobile device deployment, management and threat mitigation.

This standard addresses the general security control requirements that are applicable to the protection of department mobile devices, as well as covers the various risks associated with the use of those mobile devices. This standard applies to all department-owned mobile devices and the information systems and supporting facilities used to manage those devices.

The following areas are to be addressed to improve mobile device security:

Mobile Device Management

A centralized mobile device management solution shall be deployed.

The objective is to simplify device enrollment, monitoring and management across the department.

Asset Management

A process shall be in place for requesting, registering and revoking a department mobile device.

The objective is to ensure a clear business need is established before a department mobile device is assigned, all devices are accounted for and devices are returned once the business need is no longer served.

Physical Security

A policy shall be in place to address the use of department mobile devices in public, as well as the reporting of lost and stolen devices.

The objective is to ensure the department has a process to secure the data on department mobile devices when they are no longer in the authorized user's possession.

Vulnerability Management

A periodic vulnerability assessment shall be performed on the infrastructure supporting department mobile devices in accordance with the department infrastructure vulnerability assessment policy.

The objective is to identify potential security flaws in the mobile device infrastructure and to provide management with the necessary information to take the necessary mitigation measures.

Access Control

A process shall be in place for device identification, authorized user device access and logging and monitoring on department mobile devices.

The objective is to control and monitor access to department mobile devices in order to protect sensitive data that may be accessed on or via these devices.

Email Controls

A process shall be in place for securely accessing Agency email on department mobile devices.

The objective is to minimize the loss of sensitive data via email on these highly mobile devices.

Data Loss Prevention

A process shall be in place for decommissioning, backing up and remotely erasing all data on department mobile devices.

The objective is to minimize the loss of sensitive data when the device is no longer in the authorized user's possession, while still ensuring the authorized user can recover data efficiently.

Mobile Software Security

A process shall be in place for malicious code protection, third-party applications and Personal Area Network (PAN) connectivity on department mobile devices.

The objective is to minimize risk exposure on department mobile devices via applications and communication channels that are not controlled by the department.

The scope of the Mobile Device Security Standards is limited to the deployment and management of department mobile devices. The department will undertake the holistic vulnerability and penetration testing aspects that include the infrastructure, network, and other components that make up the mobile device infrastructure. This standard complements other system deployment standards already in place by the department.

General

Mobile Device Security Standard covers various risks associated with the use of mobile devices at the department of Public Welfare ("Department"). The requirements outlined in this document are the minimum considered adequate to identify potential vulnerabilities due to improper device deployment and management.

Standard

DPW Mobile devices include any portable storage media and portable computing and communications devices with information storage capability. Below, are the devices that are considered as mobile devices:

- USB memory sticks
- External hard disk drives
- Notebook
- Laptop computers
- Personal digital assistants
- Cellular telephones
- Digital cameras; and
- Audio recording devices.

Mobile Device Management

The department’s Networking Team shall deploy centralized mobile device management solution. The management solution must be capable of enforcing the following functions:

- Remote over-the-air (OTA) enrollment of Mobile Devices.
- Management of security configurations such as password policies, antivirus launch (Android), email configurations, feature restrictions, encryption, screen lock timeout, Wi-Fi settings, LDAP settings etc.
- Remote device monitoring such as monitoring IMEI, SIM, Network Information.
- Detect & quarantine compromised devices such as Jailbreak (Apple iOS), Rooted (Android), Unlocked (Windows Phone).
- Profile management such as role based profiles & mobile policies.
- Remote full wipe and partial wipe commands to set factory defaults or non-operational status.
- Remote lock and clear password to reset lost password.
- GPS location tracking such as track time and location coordinates of mobile devices[1].
- Mobile device software and application management. Examples include find and report installed applications and software, setup recommended applications as defined on the server, restrict installation of application and software on mobile devices.
- Provide real time notifications to network administrators for exceptions.
- Detect faults in the mobile device and configuration (hardware) changes, and report to the server for further action.
- Standard reporting for role based summary & detailed reports on authorized user activity

Asset Management

A formal request for a department mobile device shall include documentation of a justified business need from DPW management. Device allocation shall be based upon the authorized user’s role, designation and job description.

A list of approved device makes and models shall be developed and maintained by the department. The approval of a particular make and model shall be based on an evaluation, which at a minimum covers:

- Suitability for business needs.
- Compatibility with the current department environment and relevant security controls which includes the security controls set forth in this standard

A list of approved devices and associated owner details shall be maintained centrally in an asset register. Mobile devices shall be registered based on Media Access Control (MAC) ID

[1] Note that this feature can be disabled locally by the user on iOS and Android based devices.

or Unique Device ID (IMEI, ESN, or MEID for devices with a cellular radio e.g. smartphones, tablets).

Physical Security

Department mobile devices shall not be left unattended or unsecured. They must be carried by the device owner or secured to / stored inside an immovable object in order to prevent unauthorized access. The device owner will be held responsible for the physical safety of their mobile device.

While using department mobile devices in public places, the device owner shall ensure that sensitive data is not viewed by other individuals.

The device owner shall immediately report the loss, theft, tampering, unauthorized access and damage of a department mobile device to the CWOPA Help Desk Services. CWOPA Help Desk will initiate response procedures and attempt a remote wipe of the device.

Vulnerability Management

The departments' Chief Information Security Officer (CISO) shall supervise a periodic vulnerability assessment of the department mobile device infrastructure. The assessment shall be performed in accordance with the department Infrastructure Vulnerability Assessment policy.

Mitigating controls shall be applied based on the results of the vulnerability assessments performed. The results of the scans and subsequent actions taken shall be recorded and documented.

Access Control

Department mobile devices shall be uniquely identified when connecting to the DPW internal network. The unique device ID will be captured for all connecting devices. The device details will be compared with the asset register to validate identity of the user.

DPW shall employ approved method of cryptography as outlined in the *POL-SEC002 - Cryptography Policy* to protect information residing on portable and mobile information devices. A whole-disk encryption solution shall be used for laptops.

Certificate-based authentication must validate the identity of the connecting device along with other parameters such as device ID and user credentials which are provided at the time of authentication. Digital certificates will be installed on all department mobile devices before a device is authorized for use. Digital certificate information will be stored along with device registration details.

The following guidelines will be adhered to with respect to user access on department mobile devices:

- Minimum PIN/Password length shall be set to 4 characters.
- The device shall be configured to require the PIN/Password to unlock.
- The device shall auto-lock itself after 5 minutes of inactivity and the authorized user shall re-enter the PIN/Password to gain access[2].
- The data on the device shall be erased after 10 failed authentication attempts.
- By default, information system functionality that provides the capability for automatic execution of code on mobile devices shall be disabled.

Access to department networks and information systems from department mobile devices shall be revoked under the following circumstances, but not limited to:

- Expiry of the period for which access was granted.

[2] This feature can only be enforced remotely on iOS based mobile devices.

- Detection of malware on the device – access shall be revoked until the malware is completely removed.
- Violation of company policies by the device owner.
- Severance of device owner's relationship with the department

Access to department information systems from department mobile devices shall be logged and monitored on an on-going basis to identify potential security threats. Log data shall include MAC/device ID, date, time, IP address and application accessed. Application-specific logs shall be reviewed to analyze mobile device user activity.

Email Controls

Email controls shall be implemented on department mobile devices to ensure message privacy, message integrity, and user authentication. Email clients on the mobile devices shall be configured to use an encrypted communication channel as per the department's encryption policy.

Email clients shall be configured to:

- Disable downloading and processing of active content.
- Enable anti-spam and anti-phishing features[3].
- Encrypt locally stored data, including messages and downloaded file attachments.

Data Loss Prevention

The centralized MDM solution shall be capable of remotely erasing (remote wipe) all data stored on the department mobile device. Data erasure will remove all information on the device and bring it to the factory-default state. A remote wipe will be performed by sending preset commands from the central server under the following scenarios:

- Device is lost or stolen.
- Upon termination of service with the department.
- Transfer of the device to another authorized user.

Additionally, the device will be configured to automatically execute a local wipe when a certain number of failed authentication attempts occur.

The centralized MDM solution or an equivalent capable of backing up data from the department mobile device will be implemented. Data backups will be performed daily and stored on a centralized server. Data backups will be encrypted as per the department encryption policy.

Mobile Software Security

Requests for any application required for business needs will follow the appropriate approval process. The department will maintain a list of internally developed mobile applications which can be installed on department devices on request.

End-point protection mechanisms shall be enabled and updated regularly to safeguard the department mobile device against threats from viruses, spam, phishing attacks and tampering. Department mobile devices will have antivirus software installed, if the operating system is capable of running antivirus software.

Only services necessary for proper functioning of the device will be enabled. The following guidelines will be adhered to for PAN connectivity:

- Infrared Data Association (IrDA) service shall be disabled when not required.
- Bluetooth service shall be disabled when not required.
- Bluetooth protocols prior to version 2.1+Enhanced Data Rate (EDR) shall be disabled.

[3] This feature is enforced on the department mail Exchange server.

- Bluetooth Device Discovery mode shall be disabled when not required.
- Transmitting power of Bluetooth devices shall be restricted to minimal to protect devices from longer-range based attacks.
- All Bluetooth communication shall be encrypted, wherever encrypted Bluetooth communication is supported.

Web browser clients on department mobile devices will be configured to:

- Restrict web browser cookies.
- Block popup windows.
- Disable unneeded browser plug-ins.
- Disable web form auto-fill and saving of user passwords.
- Run with least privileges.

Exemptions from this Standard

Any exemptions to comply with this standard shall be discussed with the Departments' Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Standard Supplements

Mobile Application Security Standard

References

1. ITB-PRV001 Commonwealth of Pennsylvania Electronic Information Privacy Policy
2. NIST SP800-124: Guidelines on Cell Phone and PDA Security

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Mobile Device Security	Clifton Van Scyoc
10/24/13	1.1	Reviewed Content and formatted	Mathieu Saury