CHAPTER 20

Security and Use of Mobile Information Technology Resources

PURPOSE:

This manual chapter defines the accepted practices and responsibilities for the use of mobile information technology resources and defines the overall requirements for securing, and maintaining mobile information technology resources. Additionally, this manual chapter defines the process for requesting, justifying, securing, maintaining, and allowing for the use of personally owned mobile information technology resources.

AUTHORITY:

Sections 20.23(4)(a) and 334.048(3)
Chapter 815, Florida Statues (F.S.)
Rule Chapter 71A-1, Florida Administrative Code (F.A.C.)
Security and Use of Information Technology Resources, Topic No. 001-325-060

REFERENCES:

Chapter 1 of this Manual, Topic No. 325-000-002
Chapter 11 of this Manual, Topic No. 325-000-002
Security and Use of Information Technology Resources, Topic No. 001-325-060
Chapter 119, F.S.

20.1 Mobile Device Management

To ensure the ongoing security, proper configuration, management, and maintenance of the Department's data, information, and information technology resources, the Department's Office of Information Systems (OIS) shall implement and manage a mobile device management (MDM) solution. The implementation of an MDM platform adds an additional layer of security and ensures the ongoing availability, integrity, and confidentiality of the Department's information technology resources.

At a minimum, the MDM platform shall:

1. Remain up to date and properly patched in accordance with OIS' patch and version standards
2. Allow for the restriction of applications available for download to a Department owned mobile computing device
3. Include a remote-wipe feature
4. Support real time monitoring and configuration management
5. Generate event log notifications and alerts

20.1.1 Mobile Computing Devices

As defined in Rule 71A-1.002(51), FAC, all mobile computing devices used to access the Department's network, data, and information which are capable of being managed by the MDM platform shall be configured into the solution by OIS.

20.1.2 Configuration management of Department owned mobile computing devices shall be performed centrally to provide for consistency, efficient management, ease of auditing, and greater assurance of security compliance at least monthly.

20.1.3 The Department shall review security logs for the MDM platform frequently to ensure items of sufficient criticality can be investigated, addressed, and communicated to management in a proactive manner. The frequency of review shall be no less than once per week, and the logs shall be maintained for the period specified in item #391 of the ***General Records Schedule GS1-SL for State and Local Government Agencies***.

20.1.4 A complete inventory of mobile computing devices shall be maintained and include, but not be limited to information such as:

1. Assigned member of the Department's workforce
2. Applications installed
3. Software and/or operating system versions
4. Firmware versions (where possible)

20.1.5 Mobile computing devices shall require members of the Department's workforce to authenticate using a device password that is at least 4 characters in length and must be changed at least every 65 days.

20.1.6 Mobile computing devices shall "lock" and require entry of the members of the Department's workforce's password after a period of inactivity no greater than 5 minutes.

20.1.7 Where technology permits, mobile computing devices shall have their local storage encrypted.

20.1.8 Any Jail-broken or "rooted" devices shall be quarantined, disconnected, or isolated such that Department data cannot download to the device and/or the device shall be prevented from establishing a connection to the Department's network and information technology resources.

20.1.9 Where technology permits, mobile computing devices shall have anti-malware software installed, running, and kept up-to-date.

20.1.10 Members of the Department's workforce must report lost or stolen mobile computing devices immediately as specified within ***Chapter 1*** of this ***Manual***.

20.1.11 Members of the Department's workforce shall report suspicious activity or unauthorized access to Department owned data via a mobile computing device immediately as specified within ***Chapter 1*** of this ***Manual***.

20.1.12 Members of the Department's workforce shall not load, download, or install illegal content onto any mobile device.

20.1.13 Members of the Department's workforce shall only send Department related emails through the Department's email system. If a member of the Department's workforce suspects Department owned data or information has been sent via a personal email account, either within the body of the email or as an attachment, they must notify the Service Desk immediately.

20.2 Agency-managed Mobile Computing Devices

20.2.1 New mobile computing devices will be approved and tested by the OIS prior to being used in production.

20.2.2 Testing shall include but is not limited to: connectivity, protection, authentication, application functionality, solution management (such as centralized management), logging, performance, acceptability of battery life, and possible safety and security concerns.

20.2.3 Mobile Computing Devices will be configured and secured prior to being delivered to and used by the members of the Department's workforce.

20.2.4 Only approved software and/or hardware as listed in the ***Department's Software and Hardware Standards Lists*** may be installed on or connected to FDOT Mobile Computing Devices.

20.2.5 Non-standard application sources for mobile devices must be requested through ***Information Resource Request (IRR) System*** and receive appropriate approval prior to use.

20.2.6 Only applications necessary to perform Department business duties are to be placed on assigned mobile computing devices.

20.2.7 Devices will have security patches installed after a short period of testing to ensure compatibility with applications as well a general stability of the patch. The Office of Information Systems shall provide notification of available patch releases.

20.2.8 Agency-managed devices as defined in Rule 71A-1.002(7), FAC, shall comply with all device sanitization requirements, as specified within ***Chapter 11*** *of this* ***Manual***.

20.2.9 Members of the Department's workforce requesting to use Department owned mobile computing devices must receive documented approval within the Automated Access Request Form (AARF) System.

20.2.10 The use of the Department's mobile computing devices is governed by this ***Chapter, Security and Use of Information Technology Resources, Topic No. 001-325-060****,* and the ***Information Technology Resource User's Manual, Topic No. 325-000-002.***

20.3 Personally Owned Mobile Computing Devices

Topic No. 001-325-060 establishes, "Individuals choosing to use personally owned devices to conduct Department business must receive approval and agree to sign and comply with the ***Request to Use Personally Owned Computer Mobile Computing Device, Form No, 325-060-020***".

20.3.1 Use of personally owned devices is governed by this policy, ***Security and Use of Information Technology Resources Policy, Topic No. 001-325-060,*** *and* ***Request to Use Personally Owned Computer or Mobile Computing Devices, Form No. 325-060-45****.*

20.3.2 The Department is not responsible for maintaining, supporting, protecting, replacing or repairing personally owned devices.

20.3.3 The Department is not responsible for damage to a personally owned device or for any loss of data, or liability. This includes any personal data that may be lost as a result of a device wipe.

20.3.4 The owner of a personally owned device is responsible for ensuring that the device is protected, has anti-virus software installed, enabled, and that the anti-virus software remains updated. The Department is not responsible for providing antivirus software for personally owned devices.

20.3.5 The owner of a personally owned device is responsible for ensuring that data exchanged with the Department is free from viruses and other forms of malware.

20.3.6 The owner of a personally owned device is responsible for ensuring that the latest operating system updates are applied, including all applicable security patches.

20.3.7 The owner of a personally owned device shall ensure that all Department documents or other Department business information stored or maintained on the device are copied to a Department system or service to ensure compliance with ***Chapter 119, Florida Statutes.***

20.3.8 The owner of a personally owned device shall not send, transmit, or store confidential, exempt, or confidential and exempt information on a personally owned device.

20.3.9 All data transmitted from a personally owned device while connected to the Department's network and systems must only be for business purposes and such use is subject to audit and inspection in the event of a department investigation or public records request.

20.3.10 If a personally owned device that has been used to conduct Department business is lost or stolen, the owner of the personally owned device shall immediately report the incident in accordance with the provisions specified within ***Chapter 1*** *of this* ***Manual.***

20.3.11 OIS is responsible for using available resources to remote-wipe or physically wipe the personally owned device used for conducting Department business in the event the employee/employer relationship

with the device owner is severed, and in the event the device is lost, stolen, or ownership of the device is transferred.