Title:	Mobile Device Management Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	7/23/2019		
Related Policies or Procedures:	EWU 203-03: Cellular Telephones and Services Policy EWU 901-02: Appropriate Use of University Resources Washington State Office of the CIO Policy 191		

History

Revision Number:	Change:	Date:
1.0	Initial version	7/23/2019

A. Purpose

To establish and explain standards for mobile device management practices at Eastern Washington University in compliance with Washington State Office of the CIO Policy 191 and relevant university policies.

B. Definitions

Mobile Device - Any portable computing device. This includes:

- Cell phones
- Smartphones
- Tablet computers (includes iPads)
- Mobile or laptop computers
- Mobile Hotspots

Mobile Device Management (MDM) - Software for administering mobile devices in an enterprise to ensure adherence to policies and standards.

C. Procedure

Applicability and Requirement

University-owned mobile devices and personally-owned devices used for university business are subject to mobile device management requirements and procedures, including those required by the State of Washington by policy or law. This may include the installation of software on a mobile device or use of an enterprise management policy through an MDM system.

Privacy and Security

As explained in EWU 203-03, "Mobile devices are not secure. Discretion should be used in relaying confidential information on cell phones. In particular, cell phones with email, text messaging, Internet, and/or voicemail, require special attention regarding security and privacy. Such records may remain part of a University system long after they have been supposedly deleted. The university Information Security policy, EWU Policy 203-01, provides additional information related to privacy and disclosure of such information."

"Electronic records relative to mobile devices used for university-purposes, including personally-owned devices, are not private. As such, those electronic records are public records subject to Washington State's Public Disclosure Records Act (RCW 42.56). Further, electronic records may be disclosed for audit or legitimate state operational or management purposes."

- All call records, communications, texts, documents, data, photos, etc. used to conduct university business are subject to records retention requirements and public records laws, rules, and policies.
- All call records, communications, texts, documents, data, photos, etc. used to conduct university business may be subject to review in the event of a litigation hold, public records request, or audit.
- It is a best practice to limit the use of texting as an official form of business communication from a records management standpoint because text messages are not currently captured as an original record.

As explained by Washington State Office of the CIO Policy 191, "State agencies [including Eastern Washington University] have an affirmative duty under state law to retain, preserve exempt and non-exempt public records, and produce non-exempt public records in response to a request, including those created, accessed, used or stored on mobile devices. Public records, both exempt and non-exempt, include those records – including, but not limited to, texts, voicemail, email, instant messaging, calendars, photos, and video – an employee prepares, owns, uses, receives or retains within the scope of employment."

Using a Mobile Device for University Business Purposes

EWU employees who use a mobile device, whether university or personal owned, for business purposes should:

- Use web-based access and interfaces, for example Office 365 OneDrive or Google Drive, to access university files and systems.
- Not save any files or data locally, only in university-provided services or systems.
- Consider using a secure means, such as employee remote access (VPN) or web-based services, to access university resources. VPN use is not mandatory and applies only in certain circumstances.

Physical Security for University-owned Mobile Devices

As explained in EWU 203-03, "Precautions must be taken to restrict access to University-owned cell phones to authorized personnel. If a cell phone becomes lost or stolen, the user and/or department shall immediately notify the Information Technology department. IT will take appropriate action to protect university data. If theft is suspected, employees shall file a police report with the appropriate police department within 24 hours of discovering the loss."

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.