Mobile Device Management—WSU-Owned Mobile Devices

OVERVIEW

Mobile devices used to conduct University business are required to operate in a way that complies with University policies and appropriately protects institutional data. This policy defines appropriate use and procedures for the use of WSU-owned mobile devices (e.g., cellular telephones, "smart" telephones, and tablets) by University workforce members who access institutional information systems and data.

Scope

This policy applies to all University business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

Related Policies

See *BPPM* 87.01 for definitions related to this section. See also *BPPM* 85.45.

POLICY

WSU is responsible for ensuring the confidentiality, privacy, integrity, and availability of institutional data under its care, including information created, collected, stored, processed, accessed, shared, or transmitted on mobile devices.

Workforce members who use mobile devices to access institutional data or conduct University business are responsible for complying with all applicable University, state, and federal policies and laws, to include data security and privacy policies and regulations that govern the use and handling of institutional data.

Public Records Responsibility

WSU and its workforce members are obligated to preserve and provide information an employee creates, collects, uses, and/or receives in the conduct of University business in response to legal and public records requests (e.g., documents, texts, phone calls, voicemail, email, instant messaging, calendars, photos, and video).

See the Washington Public Records Act, *RCW* 42.56, the Preservation of Public Records law, *RCW* 40.14, and related University policies and procedures, *BPPM* 90.01, 90.05, 90.06, 90.07, and 90.12.

Development of Procedures

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

Information owners must develop procedures to implement this policy (*BPPM* 87.10) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

WSU-Issued Mobile Devices

Information owners may choose to issue mobile devices to certain workforce members for conducting University business, in accordance with *BPPM* 85.45. WSU-issued mobile devices must

Mobile Device Management—WSU-Owned Mobile Devices

WSU-Issued Mobile Devices (cont.)

be used in accordance with this policy and *BPPM* 85.45. Use of a mobile device on WSU networks is a privilege and may be revoked by the appropriate business unit in the event of misuse or for any reason.

Mobile Device Management Solution

All mobile devices that are used to access institutional information systems and data must be deployed, secured, and appropriately managed by a mobile device management solution. Where operationally feasible, a centrally managed, University-wide solution is to be leveraged.

Operating Systems and Software

Only operating systems and software applications approved by University business units are to be installed and supported on mobile devices. Each mobile device must have an approved and updated operating system, applications, and appropriate security software installed and running on the system. Compromised devices are removed from the WSU network.

Device Configuration

All mobile devices used to access institutional information systems and data must be configured to:

- Lock when not in use;
- Unlock with the use of a secure authentication method, e.g.:
  - Password;
  - PIN (personal identification number);
  - NFC (near-field communication) token;
  - Biometric authentication, such as fingerprint, facial recognition, etc.; and
- Remotely wipe institutional data stored on the device.

All mobile devices must be configured with whole-disk or system encryption. Encryption methods must be in accordance with University Data Policies (EP8).

Data

Institutional internal, confidential, and regulated data are allowed to be collected, stored, processed, accessed, shared, or transmitted on a mobile device, only if:

- The mobile device is used as part of a University or regulatory compliant solution;
- Institutional data are appropriately managed; and
- Institutional data are maintained and backed up to WSU managed systems.

Mobile Device Management—WSU-Owned Mobile Devices

Network Connection

If connecting to a non-WSU managed network (not to include the WSU Guest wireless network), the use of WSU-approved VPN or encrypted communications protocols (e.g., SSL, HTTPS) is required.

Security or Policy Bypass Prohibited

"Jailbreaking" or actions taken to bypass WSU policies and/or manufacturer's security mechanisms, are prohibited.

Software

WSU licenses computer software from a variety of outside companies or other third parties. WSU does not own this software or its related documentation, and this software is usually protected by license agreements. Users are to adhere to all software licenses and agreements when using or copying software to or from their mobile devices for business purposes. For additional information, see *BPPM* 35.30.

Decommissioning a Device

Once a mobile device is no longer necessary to meet a University business need, any institutional data on the device must be retained and disposed of in accordance with University records retention and disposition (*BPPM* 90.01) requirements. The device must then be decommissioned in accordance with surplus property (*BPPM* 20.76) requirements.

Lost or Stolen Device

Workforce members are responsible for notifying their supervisor and business unit equipment coordinator and complying with the University property inventory policy (*BPPM* 20.50) if their mobile device has been lost or stolen. If their WSU-issued mobile device has been lost or stolen and contains institutional data, the Chief Information Security Officer (CSIO) and/or the ITS Security Operations Center (509-335-0404) must be notified immediately.

Noncompliant Device

In circumstances where institutional confidential or regulated data are discovered on a noncompliant mobile device, users must immediately notify the CSIO and/or the Office of the Chief Information Officer (CIO).

Physical Security

Mobile device users must be especially careful to keep physical possession of their devices and not leave their mobile devices unattended in public places. Mobile devices are to be carried as hand luggage when traveling, subject to federal and other applicable guidelines.

International Travel

Many countries do not respect the personal privacy of individuals and monitor personal communications. When traveling internationally and potentially traveling to one of these countries, employees should not take their WSU-issued mobile devices with them. Business units should issue temporary, travel devices to

Mobile Device Management—WSU-Owned Mobile Devices

International Travel (cont.)

employees, which are to be used only for the duration of their international travel.

Users should not store and/or maintain institutional data on a mobile device when traveling internationally. When the employee returns from their trip, they must return the temporary device, which must be reimaged prior to being issued to another user.

See the following security tips for international travel:

- orso.wsu.edu/export-control-regulations/
- ora.wsu.edu/export-controls/
- its.wsu.edu/documents/2019/01/electronic-device-security-tips-for-international-travel.pdf/

Data and Communications Ownership

All data and communications created, sent, received, and stored on WSU owned mobile devices are the property of WSU.

Training and Acceptable Use

University Information Technology Services (ITS) personnel and information system users are to:

- Receive the appropriate training that is applicable to their role(s) regarding the provisioning, implementation, maintenance, and use of mobile devices according to this policy; and
- Follow WSU acceptable use and social media policies, in accordance with EP4.

ENFORCEMENT

The Office of the CIO is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, *WAC* 504-26).

Exceptions

Exceptions to this policy must be approved by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CSIO).

Mobile Device Management—WSU-Owned Mobile Devices

Exceptions (cont.)

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, legal, or regulatory requirements.