New 6-20
Information Technology Services
509-335-4357

Mobile Device Management—Personally-Owned Devices

OVERVIEW

Personally-owned 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 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* 87.11) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Use of Personally-Owned Mobile Devices

Information owners may allow the use of personally owned mobile devices to access institutional information system resources in accordance with this policy. Use of a personally-owned mobile

Mobile Device Management—Personally-Owned Devices

Use of Personally-Owned Mobile Devices (cont.)

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.

Without Mobile Device Management Solution

Business units may allow employees to use their personally owned mobile devices, that are not managed by a mobile device management solution, for business purposes such as:

- Accessing self-service and public web pages; and
- Responding to communication requests by voice, text, and approved e-mail solutions.

Operating Systems and Software

Personally-owned mobile devices allowed to connect to institutional information systems and data, are to do so in accordance with all applicable University policies and procedures. When accessing institutional information systems and data, all workforce members must have an up-to-date operating systems, applications, and appropriate security software installed and running on their mobile devices. Compromised devices are removed from the WSU network.

Device Configuration

Mobile devices used to collect, access, share, store, process, or transmit institutional 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 personally-owned mobile device, only if:

- The mobile device is used as part of a University or regulatory compliant solution;

Mobile Device Management—Personally-Owned Devices

Data (cont.)

- The mobile device and institutional data are appropriately managed by a mobile device management solution; and
- Institutional data are maintained and backed up to WSU managed systems.

Where operationally feasible, centrally managed, University-wide solutions should be leveraged.

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.

Lost, Stolen, or Compromised Device

WSU is responsible for supporting only the connectivity to, and any WSU-controlled applications and data installed on personally-owned mobile devices. The University is not liable for the loss, theft, or compromise of personally-owned mobile devices. It is the responsibility of the owner of the device to rebuild their personally owned mobile device if necessary.

If an employee's mobile device contains institutional data and has been lost or stolen, the employee must immediately notify:

- Their supervisor; and
- The ITS Security Operations Center (telephone 509-335-0404); or
- The WSU Chief Information Security Officer (CSIO).

Visiting Vendor

A visiting vendor requiring access to institutional networks with a mobile device must obtain authorization to do so from the appropriate business unit. Prior to connecting a visiting vendor to WSU managed networks, the business unit must submit an Exceptions Request form to Information Security Services to request a security authorization. The form is available at:

its.wsu.edu/documents/2020/02/its-exemption-form.docx

Mobile Device Management—Personally-Owned Devices

Visiting Vendor (cont.)

Further information regarding the Exceptions Request process is available at:

its.wsu.edu/documents/2020/02/its-exceptions-process.pdf/

If there is an urgent request for immediate access, the business unit submits an Exceptions Request for security authorization as a follow-up. This requirement is intended for access to WSU managed networks and not for access to the guest wireless network which provides visitors' general access to the internet.

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 must 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 must not use their personally-owned mobile devices to access institutional information systems and data. If employees require access to institutional information systems and data, business units should issue temporary devices to them, which are to be used only for the duration of their international travel.

Users are not to 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 Management

At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device. It is the responsibility of the equipment owner to backup all personal software and data to

Data Management (cont.)

other appropriate backup storage systems. Institutional data should be backed up to WSU managed storage systems and services.

When the use of a personally owned device is no longer required or the user leaves WSU, all institutional data on the device must be backed up to WSU managed storage systems, and then securely wiped from the device. Institutional data is retained and disposed of in accordance with University records retention and disposition (*BPPM* 90.01) requirements and the University Data Policies (EP8).

Data and Communications Ownership

All data and communications created, sent, received, and stored on personally-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).

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.

Mobile Device Management—Personally-Owned Devices

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.