SO Southern OREGON UNIVERSITY

Mobile Device Security

Office: Information Technology
Procedure Contact: IT Infrastructure Manager
Related Policy or Policies: Information Security Policy

Revision History

Revision Number:	**Change:**	**Date:**
1.0	Initial Version	**February 2018**

A. Purpose

The purpose of this document is to establish procedures that mitigate the security risks and manage administrative burdens associated with the use of mobile devices to facilitate University business. The criteria below should enable consistent decision making regarding procurement and maintenance of institutionally owned and operated mobile devices for SOU faculty and staff.

B. Definitions

"Secure Wireless Networks" are WiFi networks that require authentication to join, and protect all traffic to and from the device with encryption utilizing strong cryptography.

"Device Encryption" refers to a method by which all data stored on a device is encrypted at rest with strong cryptography.

"Remote Wipe" is the ability for the contents of a device to be deleted remotely, such that the device is either unusable, or is returned to factory state.

C. Device Security Standards

1. Require a pin/password/passcode/passphrase to unlock the device.
2. Devices must be vendor-supported, such that they receive patches for critical security vulnerabilities in timely manner.
3. Devices must be configured not to automatically join unknown wireless networks.
4. Devices should only connect to Secure Wireless Networks authorized by the Information Technology department.
5. Enable Device Encryption.
6. Enable Remote Wipe capability.

D. Lost or Stolen Devices

1. In the event that a University-owned mobile device is damaged, lost, or stolen, the end-user must immediately report the situation to the IT Helpdesk, or their Computing Coordinator.
2. Information Technology will take actions necessary to locate and/or remotely wipe the device.

E. Transferring a Device

1. Before transferring the possession of a University-owned mobile device from one eligible employee to another, the sponsoring department must contact their Computing Coordinator.

2. For devices issued to an individual employee: all data must be removed from the device before assigning the device to another employee.

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