Mobile Computing Devices Standard

I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security. The use of mobile computing devices to access University information technology resources introduces different and increased risks than traditional stationary computers do. One big difference is the use of personally owned devices. This standard addresses these risks and the steps necessary to reduce them.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all university workforce members that use mobile computing devices as defined in this standard and have access to University information technology resources including wireless network access. This standard applies to any mobile computing device whether it is owned by the university or otherwise.

III. DEFINITIONS

Mobile Computing Device (MCD): A portable computing device with Internet browsing capability. This definition includes, but is not limited to, laptops and notebook computers, tablet computers, smartphones, and wearable computers.

Registered MCD: Registered MCDs are managed by the University in a way that makes them more secure than unregistered devices.

IV. Mobile Computing Devices Standard

a. Compliance with other policies

MCD users must comply with:

i. All University and IT security policies, but specifically:

Care must be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection must be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices.

Access to all MCDs which access University information technology resources Y dzăű NŜIjdzNŜ a LJaăăc2ŘŜ 2NJ ůKŜ dzăŜ 2Ŧ è2dzN 2NJEayϒÎaúλ2yQă dzŜNyaY Ŝ ayŘ password.

Screens must be locked any time the device is not in use. Inactivity timeouts must be used to put the device in a locked mode.

f. Remote disabling, erasure, or lockout

Whenever possible, MCDs that access or store University data must allow the ability to be remotely disabled, erased or locked by the University. The nature of MCDs makes them more prone to theft or loss which puts any data on them at a higher risk of unauthorized disclosure.

g. Backups

Institutional data must never be stored on MCDs without a backup copy stored on another approved data storage location. The nature of MCDs and the inherent risk of them being lost or rendered useless is too high to trust as the only storage location of valuable data. You may refer to the Data Handling Procedures for approved storage locations.

V. Enforcement

Failure to comply with this standard may result in

University Policy 52 Responsible Use of Information Technology Resources

University Policy 117 Information Security

MCD Data Push Terms of Service