Information Security Standard 6.2a

Mobile Computing Devices Standard

Initially Approved: February 16, 2015
Revised: March 30, 2020 (as the Mobile Computing Devices Standard)
Standard Topic: Information Security
Administering Office: Office of the CIO

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 un-registered 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:

1. University 97 Data Security and Stewardship Policy and Data Handling Procedures

2. University 93 Electronic Mail Policy for Non-Student Users

3. University 52 Responsible Use of Information Technology Resources Policy

ii. MCD Data Push Terms of Service (for those using it)

b. Registration of mobile devices

Because of the enhanced security controls which are enforced, MCDs which are registered (as defined above) and managed by the University are considered to be in the Medium Security Zone in the Data Handling Procedures, while unregistered MCDs are considered to be in the Low Security Zone. This differentiation determines which types of sensitive data can be stored on or accessed by the device.

WCU-owned MCDs are automatically registered. Personally-owned MCDs that are set up to synchronize Email with the University MCD Data Push service are also considered registered.

c. Encryption

The Data Handling Procedures require the use of encryption for certain sensitive data. MCDs which are registered and managed by the University are considered to be in the Medium Security Zone and MCDs which are not registered or managed by the University are considered in the Low Security Zone. Refer to the Data Handling Procedures for guidance on what the encryption requirements are.

MCDs which are utilizing the University MCD Data Push service are required to have the device's built-in encryption enabled.

d. Physical Protection

Mobile devices must be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Devices carrying important, sensitive or critical business information must not be left unattended and, where possible, must be physically locked away, or utilize special locks to secure the devices.

e. Access controls

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 must require a passcode or the use of your organization's username and 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 for 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 suspension of access privileges to university data/Email.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002, 6.2, Mobile devices and teleworking)