Marshall University Information Technology Council

ITG-9

MOBILE COMPUTING AND STORAGE DEVICES GUIDELINE

1 General

1.1 Scope: This standard applies to all mobile computing and storage devices used by Marshall University users in the performance of their duties, and to all Marshall University Restricted data when accessed through, or stored on, mobile computing and storage devices, regardless of the device's ownership. Marshall University Restricted data may not be released for storage on, or access through, devices that do not meet these requirements.

1.2 Authority: Marshall University Information Technology Council

1.3 Passage Date: November 21, 2014

1.4 Effective Date: November 21, 2014

1.5 Controlling over: Marshall University

1.6 Purpose: To establish standards for the use of mobile computing and storage devices, and to specify minimum configuration requirements for them at Marshall University (MU).

1.7 Applicability: This procedure applies to students, faculty, staff, vendors and anyone with an account capable of connecting to the university network or access to university resources.

2 Definitions

2.1 Portable Computing Devices: Portable devices intended primarily for the access to or processing of data, which can be easily carried by a single person and provide persistent storage. New products with these characteristics continue to be released by manufacturers. Current examples include, but are not limited to, the following types of products:

- Laptop, notebook, netbook and similar portable personal computers
- Smartphones (Android, Blackberry, iPhone…etc.), Tablets (iPad, Kindle…etc.)

2.2 Portable Storage Devices: Media that can be easily carried by a single person and provide persistent storage. New products with these characteristics continue to be released by manufacturers. Current examples include, but are not limited to, the following types of products:

- Magnetic storage devices (USB hard drives)
- Optical storage devices (CDs, DVDs)

- Memory storage devices (SD cards, thumb drives, etc.)
- Portable devices that make nonvolatile storage available for user files (cameras, MP4 and music players, audio recorders, smart watches, cell phones)

2.3 Restricted Data: Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of Marshall University activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, driver licenses, non-directory student records, research protocols and export controlled technical data. Refer to ITG-4 Data Classification Guidelines.

3 Standard

All mobile computing and storage devices that access the Marshall University Intranet and/or store Marshall University Restricted data must be compliant with Marshall University Information Security Policy MUBOG IT-2 Information Security Policy.

3.1 Encryption of data. As stated in MUBOG IT-3 Electronic Communications Policy, Messages containing Personally Identifiable Information (PII) or Protected Health Information (PHI) are not permitted to be sent or received unless they are encrypted end to end and explicitly authorized by the President or a Vice President on a case by case basis.

3.1.1 All laptops and portable personal computers storing restricted data must utilize whole disk encryption. In addition, any laptops and portable personal computers purchased after the effective date of this standard must utilize whole disk encryption. All other laptops and portable personal computers shall have whole disk encryption installed by December 31 2015.

i) The encryption passphrase must meet or exceed Marshall University MUNet password strength rules, must not be shared, and not stored in a visible or plaintext form on or with the device.
ii) The encryption system must include a management component that provides key recovery and proof that the device is encrypted.

3.1.2 All portable computing devices that access Marshall University data must be configured to encrypt any restricted data in persistent storage. In addition, any smartphones and PDAs purchased after the effective date of this standard must utilize encryption. All other smartphones and PDAs shall have encryption installed by December 31, 2015. If the device does not support encryption, no restricted data is allowed to be stored on that device.

3.1.3 All portable computing devices must include the ability to remotely wipe stored data in the event the device is lost or stolen.

3.1.4 All portable storage devices must include built-in encryption. The following exceptions apply:

i) Specific uses where no Restricted Data will be stored and encryption would interfere with the device's intended use. Devices used in this way must be clearly marked as not for use with Restricted Data

ii) Specific uses in which devices are used for marketing and public relations, no Restricted Data will be stored, and the intended recipient is not a member of the MU Community. Devices used in this way must be clearly marked as not for use with Restricted Data.

iii) The encryption and key management methods used must have the approval of the Chief Information Security Officer or designee.

iv) Restricted Data must be protected by encryption during transmission over any wireless network and any non-MU wired network.

3.2 Authentication

3.2.1 The portable computing device must be configured to require a strong password of its user and administrator, consistent with or exceeding MUNet password requirements. Small portable computing devices where keyboard entry is cumbersome (ex. Smartphones) may use reduced password complexity if the device is configured to allow no more than 10 failed password entry attempts before preventing use by locking for a significant amount of time or erasing all storage.

3.2.2 The portable computing device must be configured with an inactivity timeout of not more than 30 minutes, which requires re-authentication before use.

3.3 Disposal. Disposal of mobile computing and storage devices must be in compliance with the Marshall University Information Technology Council disposal procedures (ITP-33 for School of Medicine)

3.4 Backup. Users must maintain a copy of data needed for MU activities, including research, teaching and business processes, on a secure server when the MU data are stored on a mobile computing or storage device.

3.5 Physical Security. The mobile computing device must have a durable physical or electronic label with contact information sufficient to facilitate an expedient return in the event that a lost device is found.

3.5.1 Mobile computing and storage devices must be used and stored in a manner that deters theft.

3.5.2 Devices should use tracking and recovery software to facilitate return if lost or stolen (when applicable).

4 Responsibilities

4.1 The Marshall University Information Security Office will establish standards to govern the secure use of all mobile computing and storage devices at the Marshall University.

4.2 The Marshall University Office of the Senior Vice President for Information Technology and Chief Information Officer will provide guidance to assist units in complying with these requirements.

4.3 All Marshall University deans, directors and department chairs, in conjunction with their IT support teams, are responsible for migrating all existing uses of mobile computing and storage devices within their areas of responsibility to devices and services that are compliant with university policies and standards.

4.4 All members of the Marshall University constituency who are currently using personally owned mobile computing and storage devices that access the Marshall University Intranet and/or store Marshall University Restricted Data are required to bring their personal device into compliance with the Marshall University Information Security Standard for Mobile Computing and Storage Devices.

4.5 All members of the Marshall University constituency will report the loss or theft of a mobile computing or storage device to their department IT Service Provider (ITSP) personnel, immediately upon detection of the loss. The university Chief Information Security Office (CISO) be immediately notified of theft or loss of any portable computing device or media that contains Restricted Data.

4.6 Personally-Owned Devices Use: This standard applies to personally-owned devices when used to access or store Marshall University data. Additionally, Use of personally-owned devices is covered by the institution's policies and procedures including MUBOG IT-1 Information Technology Acceptable Use Policy, MUBOG IT-2 Information Security Policy, and MUBOG IT-3 Electronic Communications Policy.

5 Enforcement

5.1 It is the user responsibility to take privacy and security into consideration when making decisions about when it is, and is not, acceptable to use cloud computing services. All University and campus policies, procedures, and guidelines apply to any University data, whether the data is stored on University or non-University systems. Failure to comply may result in disciplinary sanctions consistent with current collective bargaining agreements, University policies, and applicable law.

5.2 For assistance assessing these risks, please contact the Office of Information Technology or the Office of the General Counsel.