

Executive Summary of Proposed Policies on Mobile Computing Security

Scope: The proposed policies apply to:

1. University-owned mobile computing devices that is used to store University confidential/restricted data.
2. Personally-owned mobile computing devices if they are used to store University confidential/restricted data.

Notes: Separate policies on protected health information are managed by the HIPPA compliance officer. Devices that have payment card information have more restrictive policies than those described in this proposal.

Definitions:

Confidential/Restricted Data: Files that contain individually identifiable information about students, faculty, staff, retirees, alumni, donors, vendors or others whose information is required to be kept confidential.

Mobile Computing Device: Any electronic device capable of storing data and which is easily portable. It includes laptop computers, USB drives, smartphones, personal digital assistants, and other devices.

Proposed Policies:

1. **Secure Servers:** Where possible, University confidential data should only be stored on secure servers, not on desktop or mobile computing devices.
2. **Laptop Tracing:** University-owned laptop computers must have Computrace, or other University-approved tracking software, installed prior to delivery to the department making the purchase. This installation will be managed by TotalTech. Departments may also choose to have this software installed on computers already in service, in addition to computers ordered in the future. Such purchases will be made through TotalTech. Funding will be managed by each vice-presidential area.
3. **Data Encryption:** Encryption must be used to protect any University confidential/restricted data stored on a mobile device, including devices that are personally owned. Encryption software for laptops will be provided by OIT if it is not built into the operating system. Instructions and support will be provided by OIT.
4. **Network Registration:** All University-owned computers (laptop and desktop) must be accurately registered to the network in the name of the person who is the principal user. Personally owned computers must be registered if they are used on the WMU network or if they contain University confidential/restricted information. Re-registration will be required at least annually.
5. **Physical Security:** Mobile computing devices that are University-owned and personally owned devices which contain University confidential/restricted information must be physically secured when not under the immediate control of the person to whom they are assigned. They may be secured by being kept in a locked room, a locked cabinet or drawer,

by means of a security cable or by some other device that has the effect of reducing the likelihood of theft or loss.

6. **Security Responsibility:** Implementation of these policies will be led by the Office of Information Technology, TotalTech, and the LAN managers across the University. Formal policies regarding all of these issues will be posted on the OIT Web site.

Computrace

The primary purposes of Computrace are to protect the data stored on the computer, to identify a thief for possible criminal prosecution, and to recover the stolen item. New laptops will be licensed for four years and faculty and staff will be informed that their laptops have Computrace installed. Computrace software cannot be removed by the user. If a computer is reported lost or stolen, the following should happen:

1. A police report has to be faxed to Computrace.
2. The Chief Information Office or the General Counsel can authorize Computrace to track the computer. This means that Computrace can tell us the IP address used if the computer is connected to the Internet. Computrace will assist in notifying the appropriate police departments about the location of the computer. WMU staff can follow up with police departments as appropriate. This is handled through the WMU public safety department.
3. The CIO and the General Counsel can authorize Computrace to download software to the computer to track the activity on the machine. This can help to identify who is using the machine.
4. OIT, after consultation with the General Counsel and the appropriate University department, can issue a command that will destroy all data on the hard drive when the computer is next connected to the Internet. This step is necessary when the device contains confidential information.

Encryption

Modern encryption software is so powerful that it is not possible to read the data in a file without the password. If an employee forgets the encryption password, it is not possible for technical staff to recover the file. Newer Windows and Macintosh computers have encryption software in the operating systems. For older machines, OIT will provide links for downloading free encryption software. OIT will provide instructions for installation and use of encryption software. There are commercial products that allow for more centralized management of encryption, including the availability of a master password for a group of machines. OIT will advise any offices that are interested in purchasing such systems. TotalTech will stock USB drives that include encryption capability. Encryption capability is built into smartphones. Vendors can provide directions for use on individual devices.

Network Registration

Network registration is the mechanism for knowing who has registered what computer, so that if a loss is reported, OIT can identify the machine by model, type, and serial number. Every computer connected to the WMU network has been registered using a Bronco NetID and password. Often, technical staff register computers for others. With this policy, all computers must be registered in

the name of the individual to whom the computer is assigned. OIT will implement forced re-registration at least once per year. Registration is easy to do and requires only a few minutes of time.

Physical Security of Devices

Most laptops are stolen through “thefts of convenience.” To limit such thefts, devices should be secured when not under the direct control of the person to whom they are assigned. They can be secured by security cables, by being placed in a locked office, locked cabinet or drawer, or the trunk of a car.