This procedure is meant to enhance the Western Michigan University (WMU) policies and procedures related to security of information technology. It is not exhaustive. It does not contain all policies and procedures of WMU. WMU policies and procedures can be found on individual central office websites or by contacting the responsible department. Refer to the Data Security Policies and Information Security on the Office of Information Technology’s website for additional information.

**SCOPE**

- The confidentiality, privacy, and security of University electronic data and communication is a shared responsibility and requires the highest level of attention and protection. Employees who remove electronic data from its originating computing system/database are responsible for the confidentiality and integrity.

- This procedure is meant to protect confidentiality and University data.

- This procedure applies to all ODI employees (including contract employees, temporary employees, student employees, interns, volunteers, etc.) who use WMU-owned electronic equipment including computers, laptops, cellular phones, tablets, etc.

- If an employee chooses to use personal electronic device(s) for University work that may access confidential data, the employee must first obtain approval from the LAN & Systems Specialist using the “Personal Electronic Equipment form.” These electronic devices would also be subject to this policy.

**SECURITY MEASURES**

- Effective Nov. 8, desktop redirection was implemented. All user data previously stored to desktops were stored on the ODI-FS1 file share.

- Effective Nov. 27, all University-owned computers will be added to the Office of Diversity and Inclusion’s Spiceworks inventory.
• Effective Dec. 3, the Meraki Mobile Device Management system was implemented in ODI to allow for remote wipe (reformat) of all ODI laptops, cell phones, tablets, and offsite computers.

• Effective Dec. 9, all ODI electronic devices will have a paper copy of shipping documentation kept in a secure location within ODI-IT.

• Effective Dec. 20, bitlocker enabled on all university laptops and offsite PCs, to enhance security.


**PROCESSES**

• During Dec. staff meetings (main office, DMA, and DSS), staff members are trained on the importance and proper use of True Crypt and the Western Michigan University VPN. They are also reminded not to include confidential information in Webmail Plus calendars and that student data should not be sent via email without first password protecting the document.
  o If a staff member does not receive this training, it the responsibility of the staff member to contact the LAN & Systems Specialist to receive individual training.

• New hires must also receive training by the LAN & Systems Specialist within the first two weeks of employment. To obtain training, contact the LAN & Systems Specialist.

• The bi-weekly ODI-IT informational emails reinforce data security measures.

• Effective Jan. 2014, semiannual security audits of all ODI file shares are conducted by ODI-IT.

• Effective Jan. 2014, the ODI Computer Users group (meets monthly) submit a quarterly security update to the Vice President for Diversity and Inclusion.

• Effective Feb. 2014, a data security tutorial is available through the ODI website. It is mandatory for all employees to view it annually.

• Each fiscal year, employees are queried regarding on the below.
  o If they use remote access (connecting to the University network using a home Internet provider or using a mobile device on or off campus)
    ▪ Employees must be approved for remote access work. This approval must be granted by the employee’s immediate supervisor with review of the device by the LAN & Systems Specialist. If using remote access, they must certify that they have read and agree to the Office of Information Technology’s Remote Access Policy.
• Employees are sent the “Personal Electronic Equipment form” to indicate whether or not they use personal electronic equipment for work purposes so that remote access can be monitored.

• Employees must certify that they have read and understand the OIT Data Security Policies and the Information Security, as well as the ODI-IT Electronic Security Measures Policy.

**Enforcement**

• Units and employees who execute their position responsibilities in good faith following the Electronic Security Measures policy and applying a reasonable standard of care will not be subject to disciplinary action if there is a security breach.

• If an employee fails to comply with the Electronic Security Measures Policy, disciplinary action will be taken in accordance with University policy. Depending upon the severity of the infraction, the employee’s appointment with the University may be terminated.