EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Standard

Effective Date	Date of Last Revision
June 15, 2013	June 15, 2013

Chapter Name	
Security	
Chapter Number	**Title**
8.14.S.1	**Desktop and Laptop Security Standard**

1.0 Purpose

This standard establishes baseline security configuration for all desktop and laptop devices owned by, leased to, or deployed by DoIT. This standard does not cover devices owned by or leased to private individuals, contractors, students, etc.

2.0 Governing Policy

Number/Document Name	Effective Date
8.14 Desktop and Laptop Security	
8.10 Data Encryption Policy	November 14, 2012

3.0 Standard

Systems deployed by DoIT must conform to the standards listed below:

- Systems must be running an operating system from the list of supported operating systems that can be found on the IT Help Desk Minimum Support Standards web site.
- Systems must be promptly updated with the latest patches and updates. Any appropriate method may be used to test and deploy these patches, including but not limited to Windows Update, SCCM, or WSUS.
- Appropriate Anti-Virus/Anti-Malware must be installed and kept current.
- It is recommended that all systems be configured to use Active Directory or similar appropriate systems for user authentication and management. Users are required to use DoIT provided authentication to access any networked resource. Users may be given Administrator/Root or similar access to systems expressly issued to them for daily use. The use of local or guest accounts is not recommended.
- Systems containing sensitive material will have the appropriate encryption software installed and configured as per the Data Encryption Policy.
- DoIT will create and maintain standardized images for use on appropriate university desktops and laptops.

Exceptions:

- Exceptions will only be granted on a case-by-case basis and only upon approval by CIO or designate. An appropriate business case must be made for deviating from this standard, with mitigation plans provided.
- Systems deviating from this standard may not be supported by DoIT, and may be isolated from EMU networking resources at any time without notice.

4.0 Responsibility for Implementation

The Chief Information Officer is responsible for the implementation of this policy.

5.0 Definitions

Term	Definition

6.0 Revision History Description	Approval Date
Approved by CIO	June 15, 2013