EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

# Policy

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

| Chapter Name | |
|---|---|
| **Security** | |
| **Chapter Number** | **Title** |
| **8.14** | **Desktop and Laptop Security** |

## 1.0 Purpose

The purpose of this document is to detail the minimum-security required for a desktop or laptop to be deployed by DoIT, as well as the requirements for users to maintain security on an ongoing basis.

## 2.0 Scope

This policy applies to all desktop and laptop devices owned by, leased to, or deployed by EMU. This policy does not apply to systems owned by or leased to individuals, contractors, students, etc.

## 3.0 Policy

- All systems issued under this policy must conform to the Desktop and Laptop Security Standard.
- Users must ensure reasonable physical security for devices issued to them. At a minimum, systems should be in locked rooms when not in regular use or at the end of the working shift. Laptops should be secured through the use of locking cables and similar devices or containment in a locked drawer such that they cannot be easily removed. Lab machines, kiosk machines, and other devices that are in publically accessible areas shall use physical locks or equivalent systems to prevent theft.
- Users shall not bypass any control that automatically locks their device after a period of inactivity.
- Users must be able to present a valid license to DoIT upon request for any personally installed software; links to relevant Open-Source licenses are acceptable. Users may not replace University issued software with personally owned versions of the same software.
- Users may not disable, uninstall, or interfere with software and systems that provide update, backup, encryption, management, or anti-malware services without prior approval or upon instruction by DoIT Help Desk for troubleshooting.

## 4.0 Responsibility for Implementation

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

## 5.0 Enforcement

Any employee found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any student found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of state or federal laws will be reported to the appropriate legal authority for investigation.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

| 6.0 Definitions<br>Term | Definition |
|---|---|
| | |
| | |
| | |

| 7.0 Revision History<br>Description | Approval Date |
|---|---|
| Approved by CIO | June 15, 2013 |
| | |
| | |
| | |