EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Policy

Effective Date	Date of Last Revision
6/1/2016	6/1/2016

Chapter Name	
Security	
Chapter Number	**Title**
8.19	**Physical Security Requirements for non-IT Managed Systems**

1.0 Purpose

To safeguard the integrity of Eastern Michigan University's (EMU) information resources, it is mandatory that physical access to departmental computer systems be maintained at the same restricted access level as the university's data center. This policy outlines the required access restrictions and monitoring that must be adhered to for all computer systems not managed by the Division of Information Technology.

2.0 Scope

This policy applies to any computer system in use at EMU that is not housed in the university's secured data center. This policy covers all persons (employees, vendors, visitors and others) requiring access to these decentralized computer locations.

3.0 Policy

Physical access shall be limited to the minimal access necessary to complete job duties. Only staff that require physical access in order to complete his/her specific job duties shall be permitted entry. Access shall be granted to authorized employees via ID card reader or assigned key.

All access by visitors or non-authorized individuals must be approved by an authorized individual. The name, date, time, and purpose must be recorded in a permanent log. All visitors allowed physical access to security controlled spaces must be accompanied and monitored.

Intrusion alarm systems should be used to detect and alert University police of unauthorized access into security controlled spaces.

Video cameras and video recording devices should be used for surveillance and monitoring access to security controlled spaces.

4.0 Responsibility for Implementation

The University's Chief Information Officer, or their designee, 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 Term	Definition

7.0 Revision History Description	Approval Date
Created	06/01/2016
Approved by CIO	06/01/2016