EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Policy

Effective Date	Date of Last Revision
November 14, 2012	November 14, 2012

Chapter Name	
8.0 Security	
Chapter Number	**Title**
8.10	Data Encryption Policy

1.0 Purpose

In order to better comply with the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Health Information Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley act (SOX), as well as all addenda to these acts, Eastern Michigan University has implemented a Data Encryption Policy to determine under what circumstances data requires encryption.

2.0 Scope

This policy applies to all computers, servers, mobile devices or other systems that store EMU protected electronic data.

3.0 Policy

All data defined as protected as per the above referenced Acts must be made inaccessible by unauthorized parties. Division of Information Technology Staff (DoIT) will consult with EMU Legal Affairs to determine which EMU departments handle data protected by the above Acts and as a result, subject to the requirements of this policy.

Communications between the data center and a system outside the data center that contains protected data must utilize encrypted protocols, such as SSL, SCP, or SFTP.

Systems outside of the data center that contain protected data, or that may contain protected data due to their use by appropriate personnel, must have OS and Data drives encrypted to the standard deemed acceptable by the most restrictive of the applicable Acts.

Protected data must not be stored on removable storage media of any sort unless that storage media is similarly encrypted.

Systems that are not used primarily by personnel that handle protected data as a part of their daily duties must not store protected data at any time. If the business need requires that a given system store protected data, it must be encrypted as above.

4.0 Responsibility for Implementation

The Director of Network and System Services shall have the responsibility and authority to cause this policy to be implemented and maintained.

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**
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health act
SOX	Sarbanes-Oxley act
Protected Data	Data that contains ePHI or other information as defined under the Acts listed
ePHI	Electronic Personally Identifiable Information

7.0 Revision History	
Description	**Approval Date**
RKeefer-Submittal Draft	