

Chapter Name

7.0 Privacy

Chapter Number

Title

7.3

Electronic Data Storage and Transmission Policy

1.0 Purpose

The Electronic Data Storage & Transmission Policy is intended to help Eastern Michigan University (EMU) employees and Third Party Affiliates determine how information can be accessed, transmitted, stored and destroyed depending upon its sensitivity.

2.0 Scope

EMU employees should focus on two critical areas as they consider protection of institutional data: privacy and security. In the context of this policy privacy deals with the classification and release of protected data, while security deals with the protection of confidentiality, integrity, and availability of data.

The protection of EMU data is governed by a growing collection of federal and state laws relating to privacy and security. Through a number of legal statutes and regulations, institutions now have a legal responsibility for protection of student, employee, and faculty information.

EMU is responsible for complying with all state and federal laws and regulations concerning data privacy and security.

3.0 Policy

The following policy provides minimum requirements on how to protect the privacy and security of information at varying sensitivity levels while at rest, in transmission, and through the disposal process. The sensitivity levels are defined in policy 7.2 [Data Classification](#).

EMU data associated with each Data Classification may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the process being assessed. Refer to Data Classification Matrix.

3.1 Public Data

Access: General public including EMU employees

Labeling: No specific identifying information is required

Transmission within EMU: No restrictions on electronic mail and electronic file transmission methods.

Electronic transmission outside of EMU e-mail: No restrictions on electronic mail and electronic file transmission methods.

Non e-mail Electronic transmission outside EMU: No restrictions except that it is sent to only approved recipients.

Electronic Storage: No restrictions except that information should be stored on Division of Information Technology (DoIT) approved storage devices.

Disposal/Destruction: The data should be removed when no longer needed to perform job functions.

3.2 Sensitive Data

Access: Only individuals with signed confidentiality agreements who have a business need to know should receive, distribute store or have in their possession this type of data.

Labeling: Paper format and electronic media should be identified as containing “Sensitive Data”.

Transmission within EMU: No restriction on Electronic mail and electronic file transmission methods.

Electronic transmission outside of EMU e-mail: No restrictions on electronic mail and electronic file transmission methods.

Non e-mail Electronic transmission outside EMU: Should be encrypted and sent to recipients approved by the Functional Security Representatives (FSR) outside of EMU premises.

Electronic Storage: All confidential information shall be stored on DoIT approved storage devices in a directory with no additional access and/or exposure beyond those with authorized business need. Sensitive data that are stored on local hard drives, removable media, and/or mobile computing devices must be encrypted with at least 128-bit encryption.

Disposal/Destruction: The data should be removed when no longer needed to perform the functions of their job responsibilities.

3.3 Confidential Data

Access: Only individuals designated with approved access and signed confidentiality agreements that have a business need to know should receive, distribute, store or have in their possession this type of data. Information should be accessed only from a controlled access area.

Labeling: Paper format and electronic media shall be identified as containing “Confidential Data”.

Transmission within EMU: All information digitally transmitted in any form shall be encrypted – exceptions must be approved by the Functional Security Representatives (FSR) and Director of IT Security.

Transmission outside of EMU e-mail: Not permitted without approval of the Functional Security representatives (FSR) and Director of IT Security.

Non e-mail Electronic transmission outside EMU: All information digitally transmitted in any form to appropriate recipients outside of EMU must be approved by the Functional Security representatives (FSR) and Director of IT Security.

Electronic Storage: All confidential information shall be stored on IT’s network storage devices in a directory with no additional access and/or exposure beyond those with authorized business need. Confidential data shall not be stored on local hard drives, removable media, and/or mobile computing devices/media without approval from the Functional Security representatives (FSR) and Director of IT Security.

Disposal/Destruction: The storage device or file MUST be wiped clean using the Department of Defense data destruction method, or the device must be physically destroyed.

Exclusions:

DoIT managed systems that are located in secure DoIT datacenters can be exempt from media labeling, transmission and storage requirements for both sensitive and confidential data. Transmissions and storage in DoIT datacenters are physically secure and reside on restricted networks. If a data transmission must transit beyond the restricted network, then transmission methods in this policy apply.

Media labeling with the secure DoIT datacenter is not needed because all media is handled as if it contains confidential data.

4.0 Responsibility for Implementation

Any person in possession of confidential data is responsible for reporting the loss or possible inappropriate use of this information to the Director of IT Security and/or Incident Response Team (it-irt-incident@list2.emich.edu).

Functional Security representatives and the Director of IT Security are responsible for this policy’s implementation.

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 suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution.

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.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including suspension or expulsion from school.
- Criminal prosecution.

If you break the law, you can be prosecuted. Even if you are not charged criminally, you can be held personally liable, and you can be suspended or dismissed from the University, or fired if you are an employee.

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	
<u>Term</u>	<u>Definition</u>
Functional Security Representatives (FSR)	FSR administer and approve access to data contained within a specific module within the Enterprise Resource Planning (ERP) system.
Enterprise Resource Planning (ERP) system	The management information systems (MISs) that integrate and automate many of the business practices associated with the operations or production of the University.
Third Party Affiliates	<p>Affiliated third parties are persons or entities that maintain a relationship with the University for (without limiting possible relationships), research, education, military training, service, fund raising, athletic support, or other activities or interests that the University specially recognizes and supports as desirable in carrying out its educational mission, but are not students, employees, or faculty members.</p> <p>Examples of affiliated third parties include, but are not limited to:</p> <ul style="list-style-type: none"> • The Eastern Michigan University Foundation • Military Science and Reserve Officers Training Corps • Emeritus Faculty and Spouses • Emeritus Staff • Grant employees • Temporary employees from an outside agency participating in a University class or project but otherwise not affiliated. • Persons who an authorized WebCaucus organizer desires to be given temporary access to the WebCaucus conferencing system only, for purposes consistent with the University mission.
Department of Defense(DoD) data destruction method	Specific data destruction method that overwrites data seven passes and can be done by numerous shareware and commercially purchased software packages.

Transmitted in any form	File Transfer Protocol (FTP), World Wide Web, etc
Protected data	Data with a classification level of sensitive or confidential, Refer to Policy: 7.2 Data Classification

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Dorendorf	Initial draft based on SAN's policy template and Medical College of Georgia policies		
Dorendorf	Functional Security Team Comments	March 13, 2007	
Sherenco	Changes tracked in yellow	October 14, 2008	
Dorendorf	Additional changes for media exception	October 23, 2008	
Dorendorf	Send to Policy Committee	November 17, 2008	
Dorendorf	Sent to Legal for Comments	November 25, 2008	
A. Barr	Modified Section 5.0 Enforcement to conform with enforcement provisions in Acceptable Use Policy of December, 2008.	January 23, 2009	
A. Barr	Prepare for Web and Town Hall	February 25, 2009	