

April 23, 2009

September 4, 2009

Chapter Name

8.0 Security

Chapter Number Title

8.7 Log Management

1.0 Purpose

The purpose of this policy is to direct and authorize the establishment of requirements and parameters for creating, maintaining, storing, and accessing computer and communication device logs.

The logs shall be used to assist in troubleshooting, monitoring significant negative changes to system performance, record the actions of users when necessary to properly maintain security but without violating reasonable privacy expectations of legitimate users, give the ability to trend and track security instances, and provide data useful for investigating malicious activity.

2.0 Scope

This policy applies to all Eastern Michigan University (EMU) hardware and software used to establish and support a production environment.

3.0 Policy

EMU shall implement a log management program that includes generating, transmitting, storing, analyzing, and disposing of computer log data. This program will:

1. Create and maintain a secure log management infrastructure by balancing system performance, storage resources, and legal requirements.
2. Commit resources to perform timely log review,
3. Identify roles and responsibilities of staff associated with this process,
4. Develop standards, procedures, and guidelines as needed to support this program.

4.0 Responsibility for Implementation

The DoIT Director of IT Security Administration and the Director IT, Network and Systems 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 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>
Log	Record of the events occurring within an organization’s system, network and/or applications
Log Management	The process for generating, transmitting, storing, analyzing, and disposing of computer log data.
Hardware	The electronic, electrical and mechanical components of information systems.
Software	Computer programs designed for a specific purpose (such as accounts receivable, billing, or inventory control).
Production Environment	<p>Any machine used to store or transfer data between two machines where both machines meet the requirements below:</p> <ol style="list-style-type: none"> 1) are part of the Eastern Michigan University (EMU) Enterprise Resource and Planning System (ERP), or 2) system(s) approved for purchase by the Enterprise Resource and Planning System Tactical Committee (ERP-TAC), or 3) system(s) whose contract is signed by the CIO of DoIT, or 4) any hardware/software where memorandums of understanding (MOU) agreements are present between DoIT and a department/division, making a machine part of the EMU production environment. <p>Exceptions to the above definition are: applications used for academic classroom projects; systems purchased for DoIT internal use; and duplicate production environments used for testing and training purposes only.</p>

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Dorendorf	NIST Special Publication 800-92 basis – Initial Draft	December 1, 2006	
A. Barr	Substantial re-write and change of structure	January 5, 2007	
Dorendorf	Minor Modifications	January 9, 2007	
Sherenco	Revamp for all log storage	January 12, 2008	
A. Barr	Number assigned; ICT changed to DoIT	February 23, 2009	
A. Barr	Set up for publication to Policy Web site – Corrected footer and filename (f/k/a “Log Review); add logo; expand enforcement (5.0) paragraph; run spell check.	March 3, 2009	
A. Barr	IT All-Staff Town Hall – Policy Committee agreed to hold all-campus town hall and to send special notice on policy; committee also agreed procedures would be created before new log management software implemented.	April 7, 2009	
A. Barr	All-campus town hall withdrawn by CIO; policy 8.7 deemed in effective this date.	April 23, 2009	
A. Barr	Update of this Revision History Table. – Policy Posted to IT Website.	September 4, 2009	