EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

# Policy

| Effective Date | Last Revision | Last Review | Next Review |
|---|---|---|---|
| 7/6/2016 | 08/30/2016 | 5/28/15 | FY19 |

| Chapter Name | |
|---|---|
| Security | |
| **Chapter Number** | **Title** |
| 8.7 | Log Management |

## 1.0 Purpose

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

There are multiple reasons why log data may be needed. Logs may be used to monitor operational stability and performance. They may be used in order to assist in troubleshooting. They may be needed to monitor the security of I.T. infrastructure and systems/users. They may allow for the identification and analysis of security issues on the EMU network and connected systems.

## 2.0 Scope

This policy applies to all Eastern Michigan University (EMU) community members that configure the hardware and software used to establish and support the University's production technology environment.

## 3.0 Policy

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

1. Requires that all servers connected to the network send their log files consistently to a central repository. Delivery shall use either SYSLOG to one of the I.T. managed SYSLOG servers connected to Splunk or use a Splunk Forwarder directly, insofar as system storage and resources allow.
2. Requires that critical network infrastructure capable of SYSLOG send logs to a SYSLOG repository which is connected to Splunk insofar as storage allows, unless there is a specific reason for an exception.
3. Does not require that all data sent to SYSLOG by forwarded to Splunk. Due to licensing constraints Splunk cannot process all of the data that would be generated. The Security Team shall work with the device and server owners to prioritize data relevant to security alerting.
4. Requires the review of any alert generated data sent to Splunk by the IT Security Operations Center.
5. Requires that exceptions to this policy must be approved in writing (or via email) by the Director of Network and Systems.

## 4.0 Responsibility for Implementation

The Director 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 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** |
| **Production technology environment** | This term applies primarily to hardware and software managed by Information Technology staff as part of the institution's core technology infrastructure including hardware (servers, network devices, appliances, computing devices) and software (systems, applications and services). Cloud based services not owned by EMU or academic servers not managed by Information Technology staff may be exempt from this policy at the discretion of the Director of Network and Systems. |
| **Splunk** | A log aggregation, correlation and analysis tool |
| **SYSLOG** | A log aggregation tool |

| **7.0 Revision History** | |
|---|---|
| **Description** | **Approval Date** |
| Rewrite by R. Jenkins | 07/11/2016 |
| Approved by CIO | 08/30/2016 |
| | |
| | |