****

|  |  |
| --- | --- |
| Section: | IT |
| Title: | System Logging and Monitoring |
| Effective Date: | 10/1/2013 |
| Approved By: | Information Technology |
| Responsible Unit: | Information Technology |
| History: |  |
| Related Documents: |

1. **INTRODUCTION**

This document describes the requirements for computer device logging and monitoring. This includes servers and network devices such as firewalls.

1. **DEFINITIONS**

None.

1. **STANDARD**

All critical servers and network devices need to be configured to send their security and other system events to a central log aggregation system. This log aggregation system will store the events in files or a database for proactive notifications and forensic use. The log aggregation device will use analytics and event correlation to determine when to proactively alert IT security personnel of possible threats or systems in distress. Reports and log output will be reviewed on a regular schedule (e.g. daily or weekly as appropriate for a particular device).

1. **RELATED DOCUMENTS**
2. **HISTORY**