Information Technology Network and Security Monitoring Procedure

Office: Information Technology

Procedure Contact: Chief Information Officer

Revision History

Revision Number:	**Change:**	**Date:**
1.0	Initial version	**02/06/2012**
1.2	PCI DCE	**04/05/2013**
1.3	Format Changes	**0324/2014**

A. Purpose

This procedure defines the network and security monitoring practices for the Information Technology Department of Southern Oregon University. The purpose of monitoring activities includes maintaining the integrity and security of the university's network infrastructure and collecting information to be used in network design, engineering and troubleshooting.

B. Definitions

Chief Information Security Officer (CISO)

The CISO is responsible for the University's information security program and for ensuring that policies, procedures, and standards are developed, implemented and maintained

Information Resources

Any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information.

Baselines

Baselines are mandatory descriptions of how to implement security packages to ensure a consistent level of security throughout the organization. Different systems have different methods of handling security issues. Baselines are created to inform user groups about how to set up the security for each platform so that the desired level of security is achieved consistently.

C. Procedure

1. Applicability

This procedure applies to all individuals that are responsible for the installation of new information resources, the operations of existing Information Technology resources, and individuals charged with Information Technology resource security.

2. Monitoring Activities

A. **Automated tools are deployed to monitor system status. These systems include all physical and virtual servers, all network switches, the telephone system, networked storage devices, and all networked server appliances.**

B. **Automated tools are deployed to monitor the following services for real time detection of intrusion and vulnerability exploitation:**
Internet traffic
Electronic mail traffic
LAN/WAN traffic, protocols, and device inventory
Operating system security parameters

C. **The following files will be checked for signs of intrusion and vulnerability exploitation at a frequency**

determined by risk:
Automated intrusion detection system logs
Firewall logs
User account logs
Network scanning logs
System error logs
Application logs
Data backup and recovery logs
Help desk trouble tickets
Telephone activity – call detail reports
Network printer and fax logs

D. **The following checks will be performed at least annually by assigned Information Technology staff:**
Unauthorized network devices
Unauthorized personal web servers
Unsecured sharing of devices

E. **Any security issues discovered will be reported to the CISO or their designated representatives for follow-up investigation.**

3. Authorized Personnel

The Chief Information Security Officer and their designated representatives are the only individuals authorized to routinely monitor network traffic, system security logs, or other computer and network security related information.

4. Exceptions

The Computer Science test network and any users on that network are excluded from this policy.

5. Retention

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed. Electronic logs will be retained when required as part of a campus investigation or when required by as part of law enforcement or legal proceedings.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately.

D. Associated Procedures or Other Information

1. **PCI Compliance Procedures and Monitoring**

A. **Cardholder Data Environment.**

1. CDE must be monitored and on isolated subnets using firewall rules that restrict traffic to only approved payment processors and business needs approved by Business Services.

2. Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.

3. Encrypt all non-console administrative access using strong cryptography such as SSL/TLS. Clear text protocols such as telnet must be disabled.

4. All traffic must use strong encryption. Certificates for SSL/TLS must be from trusted CA’s. HTTPS must appear when accessing Web based implementations.

5. Any remote access by vendors must use two factor authentication. Accounts used by vendors must only be enabled during the time period needed. Monitoring must be in place during remote access.

6. Scans for unauthorized wireless devices must occur quarterly. USB interfaces must be disabled on any workstation/device in the CDE isolated subnets. No wireless network or device such as PDA’s, laptops, tablets, or any other mobile device may be used for any credit card environment or transaction. Automated monitoring and alerting for rogue AP’s should be in place. Any rogue AP’s discovered must be immediately taken down and the incident reported to the proper channels.

7. CDE subnets/devices shall be scanned for vulnerabilities at least every quarter. If vulnerabilities are found, a rescan must be done until a passing result for all “High” failures are resolved. Scan shall be done by qualified security personnel not directly involved with PCI compliance assessment or job duties that include processing credit card transactions.

8. All sessions shall be configured to time out after 30 minutes of inactivity.

2. SOU Related Policies

SOU Information Security Policy FAD.040