Title:	Network and Security Monitoring Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	4/7/2023		
Related Policies or Procedures:	EWU 901-02: Appropriate Use of University Resources EWU 203-01: Information Security Policy Patching and Vulnerability Management Procedure		

History

Revision Number:	Change:	Date:
1.0	Initial version	8/6/2018
1.1	Added scope and expanded policy to be compliant with WA OCIO Policy	3/28/2023

A. Purpose

This procedure defines the network and security monitoring practices for Eastern Washington University Information Technology. 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. Scope

This procedure applies to all IT assets, endpoints, infrastructure, systems, and networks under control of the university, including cloud assets. All assets will be configured to allow access for vulnerability scans.

3. 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, network storage devices, and all server appliances.
b. Regular periodic scans will be scheduled commensurate with the risk or severity of a compromise.
c. Ad-hoc scans will be conducted when the environment has undergone changes that introduce new vulnerabilities or when significant vulnerabilities are announced that may impact the university's technical environment.
d. 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
e. 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
f. 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
g. Any security issues discovered will be reported to the CISO or their designated representatives for follow-up investigation. Any false positives will be documented.

3. Authorized Personnel

The Chief Information Officer, 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. Ongoing Threat Assessment

The Chief Information Officer, the Chief Information Security Officer, and their designated representatives will actively participate in ongoing external threat intelligence gathering and sharing, including subscriptions to threat intelligence feeds.

5. Exceptions

Test networks and any users on that network may be excluded from the restrictions in this policy. Test systems may be monitored in any way deemed necessary by Information Technology staff.

6. Retention of Logs

Electronic logs that are created as a result of network and security monitoring are 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 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 upon approval.