UTSA® Institutional Compliance
Office of Information Security

OIS 32 – Standard for Security Monitoring

I. STANDARD STATEMENT

This standard serves as a companion to the Standard for Intrusion Detection and provides for the continuous monitoring that takes place at the system level.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Security Monitoring provides a means by which to confirm that information resource security controls are in place, are effective and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability and capacity planning.

B. The UTSA Standard for Security Monitoring applies to all individuals who are responsible for the installation of new information resources, the operations of existing information resources and individuals charged with information resource security.

   1. UTSA will use automated tools to provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions. These tools will be

deployed by University Technology Solutions (UTS) to monitor UTSA computers and devices for:

a. Internet traffic:
   - SPLUNK
   - ExtraHop

b. Electronic mail traffic:
   - Spam and Phishing email filters are deployed and monitored/reporting on a weekly basis.

c. LAN traffic, protocols and device inventory:
   - SPLUNK
   - ExtraHop

d. Operating system security parameters:
   - M365 monitoring tools

e. Rogue access points/devices:
   - SPLUNK
   - ClearPass

f. Installed software on servers and desktops:
   - ServiceNow
   - M365 monitoring tools

2. The following systems will be used to check for signs of illicit activity and vulnerability to exploitation at a frequency determined by risk:

a. Automated intrusion detection system logs:
   - SPLUNK

b. Firewall logs:
   - SPLUNK
   - Fortinet
   - Juniper

c. User account logs:
   - M365
   - Elucian system logs

d. Network scanning logs:
   - Tennable output

e. System error logs:
   - SPLUNK

f. Configuration files:
   - System Specific files

g. Application logs:
   - SPLUNK

h. Data backup and recovery logs:
   - SPLUNK

i. TechCafe service tickets:
   - Service-Now

j. Telephone activity – Call Detail Reports:
   - System specific logs

k. Network printer and fax logs:
   - System Specific logs

3. Assigned individuals will monitor the following (at least annually):
   a. Password strength
   b. Unauthorized network devices
   c. Unauthorized personal Web servers
   d. Unsecured sharing of devices:
   e. Unauthorized modem use:
   f. Operating System and software licenses:

4. For audit purposes, logs will be archived for a minimum of 90 days.
5. Any security issues discovered will be reported to the Information Security Officer (ISO) for follow-up investigation.

Effective Date: January 1, 2013
Last Revised: April 10, 2013
Reviewed: June 29, 2017