Sam Houston State University
A Member of The Texas State University System
Information Technology (IT)

Intrusion Detection/Prevention and Security Monitoring Policy: IT-23

PURPOSE:

The Sam Houston State University (SHSU) Information Security Office is charged with securing all SHSU owned information technology resources, both centralized and decentralized, and has the responsibility and university-wide authority to monitor the use of information technology resources to confirm that security practices and controls are in place, are effective, and are not being bypassed.

The purpose of the Intrusion Detection/Prevention and Security Monitoring Policy is to outline university policy regarding the monitoring, logging and retention of network packets that traverse SHSU networks, as well as observe events to identify problems with security policies, document existing threats and evaluate/prevent attacks.

Intrusion Detection and Prevention systems focus on identifying possible incidents, logging information about them, and reporting attempts to security administrators. It plays an important role in implementing and enforcing security policies.

SHSU takes reasonable measures to assure the integrity of private and confidential electronic information transported over its networks and to detect attempts to bypass the security mechanisms of information resources. This will allow for early detection of wrongdoing, new security vulnerabilities, or new unforeseen threats to information technology resources, thus minimizing the potential harmful impact.

SCOPE:

The Intrusion Detection/Prevention and Security Monitoring Policy applies to all information system custodians of SHSU information resources.

POLICY STATEMENT:

1. It is the policy of SHSU that Intrusion/Detection/Prevention and Security Monitoring systems will be in use across all university networks and any data traversing those networks may be subject to be scanned, monitored, logged, and retained.

2. Information system custodians who are authorized to scan, monitor, log, and retain electronic information transported over the University network must treat the contents of electronic packets to have the potential to be private and confidential.

3. Audit logging, alarms, and alert functions of operating systems, user accounting, application software, firewalls, and other network perimeter access control systems will be enabled and reviewed annually by information system custodians.

4. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually by information system custodians.

5. Information system custodians must check the following types of files/event logs for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

    a. Automated intrusion detection system logs
    b. Firewall logs
    c. User account logs
    d. Network scanning logs
    e. System error logs
    f. Application logs
    g. Data backup and recovery logs
    h. Service desk trouble tickets and telephone call logs
    i. Network printer logs

6. The following checks will be performed at least annually by information system custodians:

    a. Password strength
    b. Unauthorized network devices
    c. Unauthorized personal web servers
    d. Unsecured sharing of devices
    e. Operating system and software licenses

7. All suspected and/or confirmed instances of security issues or intrusions must be immediately reported to the Information Security Officer.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, June, 2023
Next Review: June, 2024