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

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

PURPOSE:

The 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 individuals that are responsible for the installation of new information technology resources, the operation of existing information technology resources and individuals charged with information technology resource security.

POLICY STATEMENT:

SHSU considers all electronic information transported over the university network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of SHSU to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the university's internet links. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by SHSU policies.

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. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will 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 to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic; protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing 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
- Service desk trouble tickets and telephone call logs
- Network printer logs

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Any security issues discovered will be reported immediately to the Information Security Officer (ISO).

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015