Policy: 10.15. Intrusion Detection Policy

1.0 Purpose

The purpose of this policy is to identify and respond to malicious activity targeted at computing and networking resources. It is intended to increase the level of security by actively searching for signs of unauthorized intrusion, prevent or detect the confidentiality of organizational data on the network, preserve the integrity of organizational data on the network, prevent unauthorized use of organizational systems, keep hosts and network resources available to authorized users, and increase security by detecting weaknesses in systems and network design early.

2.0 Scope

This policy applies to every host on the University network including every path that University data may travel that is not on the Internet. Paths covered by this policy include University wireless networks.

2.0 Policy

All systems accessible from the Internet must operate IT approved active intrusion detection software.

All systems in the demilitarized zone (DMZ) must operate IT approved active intrusion detection software.

All host-based and network-based intrusion detection systems must be checked on a regular basis and their logs reviewed.

All intrusion detection logs must be kept for a minimum of 30 days.

Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

Audit logging of any firewalls and other network perimeter access control systems must be enabled.
Audit logs from the perimeter access control systems must be monitored/reviewed regularly by the system administrator.

System integrity checks of the firewalls and other network perimeter access control systems must be performed on a regular basis by CSIT.

Audit logs for servers and hosts on the internal, protected, network must be reviewed on a regular basis. The system administrator will furnish any audit logs as requested by the CIO.

Host-based intrusion tools will also be checked on a regular basis.

All trouble reports should be reviewed for symptoms that might indicate intrusive activity.

All suspected and/or confirmed instances of successful and/or attempted intrusions, suspicious activity, or unexplained erratic system behavior must be immediately reported according to the Security Incident Response Policy.

Users should report any anomalies in system performance and signs of wrongdoing to the Computer Services and Information Technology Help Desk.