1.0 Policy Statement

Intrusion prevention systems are a preemptive approach to detect and respond to attempts to compromise the network. Network security should use a defense-in-depth strategy by layering security mechanisms to increase overall security.

2.0 Reason for Policy

The purpose of this policy is to establish a set of guidelines to detect and respond to information security risks associated with network intrusions.

3.0 Applicability

This policy applies to all individuals that are responsible for installing, operating and securing information resources.

4.0 Terms and Definitions

Intrusion detection - is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

Intrusion prevention - is the process of performing intrusion detection and attempting to stop detected possible incidents.

5.0 Policy
5.1 Network-based Intrusion Prevention Guidelines

An intrusion prevention system should be implemented at the network perimeter to detect, analyze and respond to external vulnerabilities and threats.

Intrusion prevention capabilities should include features for monitoring and analyzing system logs, notifications, warnings, alerts and audit logs.

System logs should be review periodically to track intrusions or other type of security incidents.
Thresholds for alarms and alerts should be configured to identify possible intrusion detection and prevention events or violations of security policies.

Security incidents will be responded to in compliance with the Security Incident Response Policy.

5.2 Host-based Intrusion Prevention Guidelines

A host-based endpoint management system should be implemented to detect, analyze and respond to internal vulnerabilities and threats.

All systems accessible from the Internet must operate SSU-supported intrusion detection software.

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