I. POLICY STATEMENT

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, assurance is needed that the systems and network are secure. Intrusion detection systems can help provide that assurance.

II. PURPOSE AND SCOPE

Intrusion detection provides two important functions in protecting information resources and technology:

1. Feedback and information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working, and

2. A trigger mechanism that determines when to activate planned responses to an intrusion incident.

The Intrusion Detection Policy applies to all individuals who are responsible for the installation, operation and security of information resources technology. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

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

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

3. Audit logging of any firewalls and other network perimeter access control system must be enabled.

4. Audit logs from the perimeter access control systems must be monitored and reviewed daily by the system administrator.

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

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

7. Host-based intrusion tools will be checked on a routine basis.

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

9. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy – M APP 04.06.11.

10. Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the Office of Information Technology ("OIT") Help Desk.

11. Disciplinary Action

    Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

12. Applicable TSU Security Policy Standards

    All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

    - Security Standard 1
    - Security Standard 3
    - Security Standard 14
    - Security Standard 16
    - Security Standard 17