Reason for the Guidelines

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, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

1. Official Guideline

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

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

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

1.4 Audit logs from the perimeter access control systems must be monitored/reviewed by the system administrator.

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

1.6 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 Information Security Officer (ISO).

1.7 Host based intrusion tools will be checked on a routine schedule.

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

1.9 All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the HSC Incident Management SAP.
1.10 Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the OIT Help Desk.

2. Disciplinary Actions

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration