UTSA Institutional Compliance
Office of Information Security

OIS 19 – Standard for Intrusion Detection

I. STANDARD STATEMENT

The UTSA Intrusion Detection Standard applies to all individuals who are responsible for the installation of new information resources, the operations of existing information resources and individuals charged with information resources security.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Intrusion detection is the use of tools and policies to monitor system performance in order to prevent unauthorized use of UTSA information resources. Intrusion detection provides two important functions in protecting information resources:
   1. Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.
   2. Feedback: information about 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.

B. Users shall be trained to report any anomalies in system performance and/or signs of suspected wrongdoing to the Information Security Officer (ISO) or the Computer Incident Response Team at 210-458-5555, UTS Tech Cafe at 210-458-5555 or to the UTSA Compliance Hotline, 210-458-5365.

C. All suspected and/or confirmed instances of successful and/or attempted intrusions must be reported immediately in accordance with the Information Security Incident Response(http://www.utsa.edu/hop/chapter8/8-17.html).

D. Operating system, user accounting and application software audit logging processes must be enabled on all host and server systems.
E. Alarm and alert functions of firewalls and other network perimeter access control systems must be enabled.
F. Audit logging of firewalls and other network perimeter access control systems must be enabled.
G. Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
H. System integrity checks of the firewalls and other network perimeter access control systems must be performed on a daily basis.
I. Audit logs for servers and hosts on the internal, protected network must be reviewed on a weekly basis. The system administrator must furnish any audit logs as requested by the ISO.
J. Network/host-based intrusion tools will be checked on a daily basis.
K. All trouble reports received by system administration personnel should be reviewed for signs that might indicate intrusive activity.

Title: OIS 19 – Standard for Intrusion Detection
Effective Date: October 15, 2011
Last Revised: July 30, 2020