

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.10 Intrusion Detection

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

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.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Intrusion Detection Policy applies to all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.

1.5 Definitions

- **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Security Incident:** In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.
- **Information Attack:** An attempt to bypass the physical or information security measures and controls protecting an IR. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Information Operations:** Actions taken to affect adversary information and information systems while defending one's own information and information systems.
- **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the information resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.
- **Information Security Officer (ISO):** Responsible to the IRM for administering the information security functions within the institution. The ISO is the

institution's internal and external point of contact for all information security matters.

- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Host:** A computer system that provides computer service for a number of users.
- **Server:** A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.
- **Firewall:** An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

2. INTRUSION DETECTION POLICY

- 2.1 Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- 2.2 Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- 2.3 Audit logging of any firewalls and other network perimeter access control system must be enabled.
- 2.4 Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
- 2.5 System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
- 2.6 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 ISO.
- 2.7 Host based intrusion tools will be checked on a routine schedule.
- 2.8 All trouble reports should be reviewed for symptoms that might indicate intrusive activity.

2.9 All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the HSC Incident Management Policy.

2.10 Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the OIT Help Desk.

3. 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 Information Technology and Chief Information Officer