

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.11 Intrusion Detection

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Intrusion detection plays an important role in implementing and enforcing an organizational security policy that is capable of preserving the integrity, availability, and confidentiality of data and information resources within the Texas A&M University-Corpus Christ network. 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 and decentralized systems and network topology, some type of assurance is required so that the systems and network are secure. Intrusion detection capabilities can provide part of that assurance through detection of and altering to anomalous system and network activity so that incident management procedures can be initiated in an efficient and effective manner.

2. APPLICABILITY

This university procedure applies to university information resources that store, process, or transmit Sensitive Information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with intrusion detection.

There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

The intended audience for this university procedure includes, but is not limited to, all information resources management personnel, owners, and system administrators.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions

4. PROCEDURES

4.1. All suspected and/or confirmed instances of host, server, or network intrusions shall be immediately reported according to procedures outlined in University

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

Procedure 21.01.06.C2.08 Incident Response. Unusual behavior or activity should be reported to the Media and Computer Services Helpdesk to help identify trends and indicators of intrusive activity.

- 4.2. Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems shall be enabled.
 - 4.3. Audit logs from the firewalls and network perimeter access control systems shall be monitored/reviewed as risk management decisions warrant.
 - 4.4. Operating system, user accounting, and application software audit logging processes shall be enabled on all host and server systems where resources permit and risk management decisions warrant.
 - 4.5. Hosts, servers, and devices that contain Sensitive Information, directly connect to storage containing Sensitive Information, or access Sensitive Information through a network connection must enable operating system, user accounting, and application software audit logging processes. If a system or device with these accesses is not capable of implementing these controls, notification of the Information Resource Manager is required for risk mitigation.
 - 4.6. Audit logs for hosts, servers, and devices will be reviewed as warranted based on risk management decisions.
 - 4.7. Host based intrusion tools shall be utilized on hosts, servers, and devices as risk management decisions warrant.
 - 4.8. Anomalous activity detected in audit logs and reports shall be reported according to the procedures outlined in University Procedure 21.01.06.C2.08 Incident Response. Audit logs, reports, and any additional related information shall be furnished to representatives of the Information Resources Manager immediately upon request.
5. **CONSEQUENCES FOR VIOLATIONS**

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
 - 01.03 Appointing Power and Terms and Conditions of Employment
 - 07.01 Ethics Policy, TAMUS Employees
 - 32.02 Discipline and Dismissal of Employees
 - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
 - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
 - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
 - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration