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 Christi 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.

This University Procedure applies to all University information resources.

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.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience for this University Procedure is all users, especially custodians and owners of servers and network perimeter equipment.

Please refer to University Procedure 29.01.03.C2.01 Definitions
4.1. The IRM or his or her designees shall issue guidelines (“the intrusion detection guidelines”) pursuant to this Procedure which shall define one or more classes of information resources and for each defined class specify the following:

4.1.1. Which intrusion detection measures shall be enabled on those resources, e.g., host intrusion detection software (HIDS), network intrusion detection systems (NIDS), intrusion prevention systems (IPS), audit logging, alarms, and alerts;

4.1.2. For each measure defined in 4.1.1.:

4.1.2.1. What events must be logged, e.g., logins, logouts, password reset events;

4.1.2.2. What information must be recorded about each event, e.g., date, time, source IP and port, destination IP and port;

4.1.2.3. Whether, how often, and by whom the log file will be reviewed, and;

4.1.2.4. For each log file created, how much history will be retained, e.g., 30 days.

4.2. The IRM shall ensure that the intrusion detection guidelines comply with the following policy:

4.2.1. All intrusion detection measures shall be logged.

4.2.2. Custodians of firewalls and other network perimeter access-control systems shall enable audit logging, alarm, and alert functions on those systems.

4.2.3. Custodians of information resources (e.g., operating systems, user accounting, application software) on servers shall enable audit logging on those information resources.

4.3. Custodians shall report anomalous activity detected by intrusion detection measures according to University Procedure 29.01.03.C2.08 Incident Response.

4.4. Custodians shall furnish audit logs, reports, and any additional related information to the IRM or his or her designees immediately upon request.

4.5. All users shall immediately report any suspected and/or confirmed instances of host, server, or network intrusions according to University Procedure 29.01.03.C2.08 Incident Response.

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 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:** Office of Information Security

**Office of Responsibility:** Office of the Associate VP for Information Technology and CIO