General
The Texas A&M International University (TAMIU) network infrastructure is provided as a
central utility for all users of TAMIU Information Resources. Intrusion detection plays an
important role in implementing and enforcing an organizational security policy. As Information
Resources 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 that the systems and network are secure is needed. Intrusion detection systems can
provide part of this assurance.

Applicability
The purpose of this SAP is to establish the rules for the access and use of the network
infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality
of TAMIU’s Information Resources. This SAP applies to all individuals with access to TAMIU
Information Resources.

Definitions

Information Resources (IR): Any computer printouts, online display devices, magnetic storage
media, and all computer-related activities involving any device capable of receiving email,
browsing websites, 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, tablets, distributed processing systems, network attached and
computer controlled medical and laboratory equipment (i.e. embedded technology),
smartphones, telecommunication resources, network environments, telephones, fax machines,
printers and service bureaus. Additionally, it includes 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.

Information Resources Manager (IRM): Person 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 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. At TAMIU, the IRM is the Associate Vice President for IT/CIO.

**Information Security Officer (ISO):** Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMIU’s internal and external point of contact for all information security matters.

**Office of Information Technology (OIT):** The name of the TAMIU department responsible for computers, networking and data management.

### Procedures and Responsibilities

At TAMIU, several systems are used to monitor, detect and log intrusion attempts via the IP network. These systems include a network behavior and anomaly detection system, intrusion prevention systems, firewalls, email antivirus protection for Exchange servers and antivirus software for computers. In accordance with these security measures, the Information Security Officer monitors and audits intrusion detection logs. Anomalies will be investigated and appropriate measures will be taken in the event of an actual threat in accordance with the incident management procedures.

1. **Network Access**
   1.1 All suspected and/or confirmed instances of host, server, or network intrusions will be reported immediately as outlined in TAMIU’s 29.01.99.L1.08 Incident Management SAP to the Information Security Officer at itsecurity@tamiu.edu or 956-326-2026.
   1.2 Operating system, user accounting and application software audit processes will be enabled on all host and server systems where resources permit.
   1.3 Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems will be enabled.
   1.4 Logs from the firewalls and network perimeter access control systems will be monitored and reviewed as risk management decisions warrant.
   1.5 Logs for servers and devices will be reviewed as warranted based on risk management decisions.
   1.6 Anomalous activity detected in audit logs and reports will be reported according to the procedures outlined in TAMIU’s 29.01.99.L1.08 Incident Management SAP.

### Related Statutes, Policies, Regulations, Rules or Requirements

TAC 202.75 Security Standards for Institutions of Higher Education

### References

Appendix

- Copyright Act of 1976
- Foreign Corrupt Practices Act of 1977
- Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

<table>
<thead>
<tr>
<th>Contact Office</th>
<th>Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information Technology</td>
<td></td>
</tr>
<tr>
<td>Hotline: (956) 326-2310</td>
<td></td>
</tr>
<tr>
<td>Killam Library 257</td>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
<tr>
<td>Office Hours</td>
<td>ITSecurity Group</td>
</tr>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
<td></td>
</tr>
</tbody>
</table>