General
The number of computer security incidents and the resulting cost of business disruption and service restoration continues to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Applicability
This SAP provides a set of measures that will mitigate information security risks associated with incident management and describes the requirements for dealing with computer security incidents. It applies to all individuals who use Texas A&M International University (TAMIU) Information Resources.

Definitions
CIA triad: Confidentiality, Integrity and Availability.

Incident Response Team (IRT): Personnel responsible for coordinating the response to computer security incidents in an organization. The IRT holds regular meetings to review any incidents that have occurred, and discusses projects relating to IT Security. Emergency meetings may also be called at the discretion of the CIO or ISO if an incident needs immediate attention. The team members and their roles include:

Information Security Officer - Advises team of incidents that have occurred and updates members on security projects.

FERPA Officer - Advises team of all aspects regarding FERPA, as well as enrollment management processes.

PCI Compliance Representative - Advises team regarding PCI Compliance, as well as Business and Finance processes.

Financial Services – Advises team of all financial operations for students.

Academic Affairs - Advises team regarding the processes within Academic Affairs.

Risk Management & Compliance - Advises team of risk and compliance matters.
Judicial Affairs – Advises team of student judicial affairs.

UPD Representative - Advises team of any criminal computer incidents.

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 function within the University. The ISO is TAMIU’s internal and external point of contact for all information security matters.

Security Incident: 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.

---

**Procedures and Responsibilities**

1. **How to report an Information Security Incident**

TAMIU’s ISO is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operations quickly and if required, maintain evidence for further disciplinary, legal, or law enforcement actions.

1.1 Incidents involving computer security will be managed by TAMIU’s ISO and will be reported as required by federal or state law or regulation.

1.2 All faculty members, staff and/or students must promptly report any unauthorized or inappropriate disclosure of confidential information.

1.3 Additional information on Information Classification is described in TAMIU’s 29.01.99.L1.31 Information Classification SAP.
1.4 There are three ways to report an incident:

- E-mail: itsecurity@tamiu.edu
- Call: 956-326-2026
- Fill out form at http://incidents.tamiu.edu

2. Incident Categories:

2.1 Level 1 – These are the least severe and most common types of incidents. They have no widespread effect on any TAMIU function. Level 1 incidents will be handled by the appropriate IT department via work orders. Incident types and quantities will be tracked and they will be discussed at the IRT monthly meeting. Incident reports will be sent to the Department of Information Resources (DIR) via their Security Incident Reporting (SIRS) system.

2.2 Level 2 - Incidents that have a small impact on operational functionality but have no impact on the overall business function of the University. Level 2 incidents will be handled by the appropriate IT department via work orders and will be reported to the CIO or ISO. IT personnel will continue to monitor the incident after remediation and will report findings to the CIO and ISO for as long as they deem necessary. Incident types and quantities will be tracked. Reports will be discussed at the IRT bi-monthly meeting and will be sent to the Department of Information Resources (DIR) via their Security Incident Reporting (SIRS) system.

2.3 Level 3 - These are the most severe incidents. They have a major impact on either business or operational functions at TAMIU and may prevent the University from fulfilling its mission. This category also includes incidents that may cause reputable or financial damage to TAMIU. Level 3 incidents may require an emergency IRT meeting. The incident will be handled by the appropriate IT department manager via work orders, and all steps taken must be approved by either the CIO or ISO. IT personnel will continue to monitor the incident after the threat has been mitigated, and must report findings to the CIO and ISO for as long as they deem necessary. An incident report will be prepared by the ISO for review by the CIO, IRT and upper administration. Incident types and quantities will be tracked and reported to the IRT and the Department of Information Resources (DIR) via their Security Incident Reporting (SIRS) system. The following are examples of the categories of IT security related incidents:

<table>
<thead>
<tr>
<th>Incident Categories</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Level 1             | No widespread effect on TAMIU functions | • Minor rule violations by an employee  
• Detection and removal of viruses or malware |
| Level 2             | No impact on overall business functions, but do have an impact on operational functions | • Repeated reconnaissance activity from the same source  
• Attack blocked by TAMIU’s security infrastructure  
• Regular occurrences of Level 1 incidents  
• Successive attempts to gain unauthorized access to a system |
| Level 3 | Affect TAMIU’s ability to meet its mission objectives; major impact on University’s business or operational functions | • Unavailability of systems
• Unauthorized access to sensitive systems
• Improper use of high level accounts such as root or administrator
• Defacement of TAMIU Web site
• “Denial of service” attacks
• Unauthorized changes to key infrastructure
• Theft/Loss of computer systems, or media, containing sensitive information or confidential information
• IT related Payment Card Industry (PCI) or Family Educational Rights and Privacy Act (FERPA) violations |

3. Procedures

3.1 The ISO is responsible for initiating, completing and documenting the incident investigation.

3.2 TAMIU’s ISO is responsible for reporting the incident to the:
- IRT
- IRM
- Department of Information Resources of the State of Texas using SIRS reporting tool
- University, local, state or federal law officials as required by applicable statute and/or regulations

3.3 In cases where law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the IRM.

3.4 Any incident that involves criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) must also be reported to the University Police Department.

3.5 For incidents directly involving TAMIU employees, the Human Resources department and the appropriate Vice President or Dean will be contacted.

3.6 For incidents directly involving TAMIU students, the Judicial Student Affairs department will be contacted.

3.7 The ISO is responsible for determining and gathering the physical and electronic evidence necessary for the incident investigation.

3.8 The ISO and IRM will determine if a widespread TAMIU communication is required, the content of the communication and how best to distribute the communication.

3.9 The IT security team is responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
# Related Statutes, Policies, Regulations, Rules or Requirements

TAC 202.75 Security Standards for Institutions of Higher Education

## Appendix

**References**
- 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

## Contact Office

<table>
<thead>
<tr>
<th>Office of Information Technology</th>
<th>Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline: (956) 326-2310</td>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td>Killam Library 257</td>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Office Hours</th>
<th>ITSecurity Group</th>
</tr>
</thead>
<tbody>
<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>