TEXAS A&M INTERNATIONAL UNIVERSITY

# Standard Administrative Procedure (SAP)

## 29.01.99.L1.08 Incident Management

**First Approved:** March 28, 2013
**Revised:** January 9, 2019
**Next Scheduled Review:** January 9, 2024

## Procedure Statement and Reason for Procedure

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.

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. This SAP applies to all individuals who use Texas A&M International University (TAMIU) information resources.

## Procedures and Responsibilities

**1. REPORTING AN INFORMATION SECURITY INCIDENT**

The TAMIU Information Security Officer (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 the ISO and will be reported as required by federal or state law or regulation.

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

1.3 Additional information about information classification is available in TAMIU SAP 29.01.99.L1.31, *Information Classification*.

1.4 Security incidents are reported via email to itsecurity@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 TAMIU's functionality. Level 1 incidents will be handled by the appropriate IT (information technology) department via work orders. Incident types and quantities will be tracked. Incident reports will be submitted to the Department of Information Resources (DIR) of the State of Texas via their Security Incident Reporting System.

2.2 Level 2 – Incidents that have a small impact on operational functionality but have no impact on the overall business function of TAMIU. Level 2 incidents will be handled by the IT department and will be reported to the Chief Information Officer (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 Incident Response Team (IRT) quarterly meeting and will be sent to the DIR of the State of Texas via their Security Incident Reporting 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 TAMIU 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 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 DIR of the State of Texas via their Security Incident Reporting System.

2.4 The following are examples of the categories of IT security-related incidents:

| Incident Category | Description | Examples |
|---|---|---|
| Level 1 | No widespread effect on TAMIU functions | • Minor rule violations by an employee<br>• 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<br>• Attack blocked by TAMIU's security infrastructure<br>• Regular occurrences of Level 1 incidents<br>• Successive attempts to gain unauthorized access to a system<br>• Unavailability of systems |
| Level 3 | Affect TAMIU's ability to meet its mission objectives; major impact on TAMIU's business or operational functions | • Unauthorized access to sensitive systems<br>• Improper use of high level accounts such as root or administrator<br>• Defacement of TAMIU website<br>• "Denial of service" attacks<br>• Unauthorized changes to key infrastructure<br>• Theft/Loss of computer systems or media, containing sensitive information or confidential information<br>• 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 The ISO is responsible for reporting the incident to the following:

- IRT
- IRM (information resources manager)
- DIR of the State of Texas using their Security Incident Reporting System
- TAMIU, 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 Office of Human Resources and the appropriate vice president or dean will be contacted.

3.6 For incidents directly involving TAMIU students, the Office of Student Conduct & Community Engagement 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 TAMIU-wide 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, or Rules

TAC 202 Subchapter C - Security Standards for Institutions of Higher Education
TAMIU Rule 29.01.99.L1, *Information Resources*

## 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

Office of Information Technology, 956-326-2310, itsecurity@tamiu.edu