Procedure Statement

This Procedure describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to: malicious code detection; unauthorized use of computer accounts and computer systems; theft of computer equipment or theft of information; accidental or malicious disruption or denial of service as outlined in security monitoring procedures, intrusion detection procedures, internet/intranet procedures, and acceptable use procedures. Incidents, deemed to be severe or repetitive, should be reported to either the Chief Information Officer (CIO) or the Information Security Officer (ISO) as soon as possible. Once an incident is reported the CIO and ISO will determine the severity of the incident, and categorize it appropriately.

Reason for Procedure

This Procedure 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 University -San Antonio (A&M-San Antonio) information resources.

Official Responsibilities and Procedure

1. INCIDENT MANAGEMENT PROCEDURES:

   1.1 The ISO is responsible for initiating, completing and documenting any and all incident investigations.

   1.2 Upon discovery of an incident the ISO is responsible for notification to, but not limited to, the IRM, DIR, University administration, or other law enforcement, as applicable. At a minimum, the ISO will provide the IRM with regular reporting of all incidents discovered and/or reported to ITS. In addition, all incidents are required to be submitted monthly to the DIR through SIRS.
1.3 Faculty/Staff/Students that identify a security incident should immediately contact the ITS Help Desk and/or ISO.

1.4 In cases where law enforcement is not involved, the ISO will recommend corrective or disciplinary actions, if appropriate, to the IRM. The IRM will review and submit through the appropriate vice president or executive team member.

1.5 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 (UPD).

1.6 For incidents directly involving A&M-San Antonio employees, the Human Resources department and the appropriate vice president or dean will be contacted.

1.7 For incidents directly involving A&M-San Antonio students, the Division of Student Affairs will be contacted.

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

1.9 The ISO and IRM will determine if a campus wide notification is required, the content of the communication and how best to distribute the communication.

1.10 The ITS security team is responsible for ensuring that any damage from a security incident is repaired.

2. CATEGORIES OF INCIDNTS:

<table>
<thead>
<tr>
<th>Incident Categories</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Level 1             | Least severe and most common type of incident. These have no wide spread effect on University functions. | • Minor policy violations by an employee  
• Detection and removal of viruses or malware |
| Level 2             | No impact on overall business functions and small impact on operational functions. | • Repeated reconnaissance activity from the same source.  
• Attack blocked by the University’s security Infrastructure.  
• Regular occurrences of Level 1 incidents.  
• Successive attempts to gain unauthorized access to a system |
| Level 3             | Impact on the University’s ability to meet its mission objectives, major impact on business or operational functions. Risk of damage to | • Unauthorized access to sensitive systems  
• Improper use of high level accounts such as root or administrator  
• Defacement of A&M-San Antonio web site.  
• Denial of service attacks |
| University reputation or financial loss. | • Unauthorized changes to key infrastructure  
• Theft/Loss of computer systems, or media, containing sensitive information or confidential information  
• IT related PCI, HIPAA or FERPA violations |

Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.

Related Rules

**DIR Practices for Protecting Information Resources Assets**

**Family Educational Rights and Privacy Act (FERPA)**

**Gramm Leach Bliley Act (GLB Act)**

**Health Insurance Portability and Accountability Act (HIPAA)**

**TAMU System Policy 29.01 Information Resources**

**Texas Administrative Code (TAC) 202** as amended or supplemented

**Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education**

Definitions

**Accounts** - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).
**Incident Report** – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

**Information Resources (IR)** - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

**Information Resources Manager (IRM)** - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central information technology department for the University.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.

**Network Scanning** - The process of transmitting data through a network to elicit responses in order to determine configuration state or the presence of security vulnerabilities within an information system.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**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.

**Security Incident Reporting System (SIRS)** - The electronic system used for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.
System Custodian – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

Unscheduled Change – A system modification that fails to present notification to the formal process in advance of the change being made.

User - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s procedures and rules.

Contact Office

Finance and Administration, Information Technology Services (210)784-4357 (HELP)