STANDARD ADMINISTRATIVE PROCEDURE

29.01.99.S1.09  Information Resources – Incident Management

Approved

Next Scheduled Review:

Standard Administrative 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.

Definitions

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.

SIRS – Security Incident Reporting: an electronic system for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.

SO ISO – System Office Information Security Officer

Official Rule/ Responsibilities/ Process

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all System Office (SO) information resources.

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with incident management. 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.
The information resource owner or designee (e.g., custodian, user), is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.99.S1.27 Exclusions from Required Risk Mitigation Measures.

The intended audience is system administrators, Directors, and Department Heads.

2. **PROCEDURES**

2.1 SO system administrators have information security roles and responsibilities which can take priority over normal duties.

2.2 System administrators are responsible for notifying their Directors and initiating the appropriate action including restoration.

2.3 System administrators are responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation such as initiating, completing, and documenting the incident investigation.

2.4 System administrators shall report the security incidents that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) to the Director SO ISO see TAC 202.76 (c) for reporting requirements (as of 05/06/05).

2.5 If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow System Policy 21.04, Control of Fraud, Waste and Abuse.

2.6 If there is a substantial likelihood that security incidents could be propagated to other systems beyond departmental control, system administrators shall report such incidents to SO ISO and TAMU CIS help desk, (979) 845-8300, if action is urgently needed or via email to security@tamu.edu as soon as an incident is identified.

2.7 System administrators shall prepare an after-action report and submit it to SO ISO.

---

**Related Statutes, Policies, or Requirements**

**Supplements SO Rule 29.01.99.S1**