Texas A&M University System Standard – Incident Management

Standard Statement

This standard 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 standards, intrusion detection standards, internet/intranet standards, and acceptable use standards.

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.

Archer – Security Incident Reporting: an electronic system for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations. Also see reporting an incident or breach here.

SO ISO – System Office Information Security Officer

Official Rule/ Responsibilities/ Process

1. APPLICABILITY

This Standard (standard) applies to all System Office (SO) information resources.

The purpose of the implementation of this 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 standard 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 standard. All exclusions must be in accordance with the standard *Exclusions from Required Risk Mitigation Measures*.

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

2. STANDARDS

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. Any incident or potential incident should be

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 SO ISO see TAC 202.76 (c) for reporting requirements (as of 05/06/05). Also, see the System web page for reporting an incident or breach at this link.

2.5 If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow System Policy 10.02.01, 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 TAMUS help desk, (979) 458-6430, if action is urgently needed or via email to iso@tamus.edu as soon as an incident is identified and also refer to the TAMUS cybersecurity website here.

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

Contact Office

For clarification contact: The Texas A&M University System Chief Information Officer
OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer