Information Resources – Incident Management

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
This procedure describes the requirements for dealing with computer security incidents.

Reason for Standard Administrative Procedure
The purpose of this incident management procedure is to provide a set of measures that will mitigate information security risks associated with incident management.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES
   
   1.1 Division system administrators have information security roles and responsibilities which can take priority over normal duties.

   1.2 The division system administrators are responsible for notifying their division heads and initiating the appropriate action including restoration.

   1.3 Division 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.

   1.4 The division system administrator shall report the security incidents that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) to the TEES information security officer. See Texas Administrative Code §202.76 (c) for reporting requirements.

   1.5 If fraud or theft is suspected as part of security incident detection, the person detecting the incident shall follow System Policy 10.02, Control of Fraud, Waste, and Abuse.

   1.6 If there is a substantial likelihood that such incidents could be propagated to other systems beyond division control, the division system administrator shall report security incidents to TEES information security officer (979).
847-8585 and TAMU Computing and Information Services (CIS) help desk, (979) 845-8300.

1.7 TEES information security officer is responsible for reporting the incidents to Department of Information Resources as outlined in Texas Administrative Code §202.76.

**Related Statutes, Policies, or Requirements**

*System Policy 10.02, Control of Fraud, Waste, and Abuse*

*TAMU SAP 29.01.99.M1.09, Information Resources – Incident Management*

*TEES Rule 29.01.99.E1, Security of Electronic Information Resources*

*Texas Administrative Code §202.76, Security Incidents*

*Texas Penal Code Chapters 33 (Computer Crimes)*

*Texas Penal Code Chapter 33A (Telecommunications Crimes)*

**Contact Office**

Information Technology Services
(979) 847-8585