IR- 6 Incident Reporting

Description

Information resources incident and crisis situations are ongoing and pervasive resulting in costly business disruptions and service restoration. Crises can be events that adversely affect electronic systems, result in loss of confidential information or catastrophic events that impact facilities. This Control describes the requirements for appropriate handling of information resources security incidents and crises that are likely to expand beyond the control of one unit’s ability to manage effectively.

The principal priority for mitigating the effects of an information resources crisis is the containment and protection of university information resources.

Texas Administrative Code, Chapter 202 requires institutions of higher education to have specific procedures to contain and mitigate the effects of events and incidents, i.e., crisis. Due to the IT Service Management implementation which uses Information Technology Infrastructure Library (ITIL) terminology, this Control utilizes the term “crisis” in place of the traditional use of “incident” to describe IT security situations that require intervention to resolve.

This procedure is intended to ensure that university units interact efficiently with common terminology and common processes to effectively manage information resources situations that have escalated to a crisis level.

Situations that do not rise to the level of a crisis are expected to be handled in coordination with the Texas A&M IT help desk. When a situation cannot be effectively handled by the Texas A&M IT help desk and/or rises to the level of a crises, the procedures in this Control will be applied. The Texas A&M IT help desk will not manage crisis level situations independently.

Applicability

This procedure applies to all unit heads, system administrators, and third parties who are responsible for Texas A&M University (Texas A&M) information resources assets. This Control is intended to address those crisis situations that escalate beyond the capability of one unit or department to handle effectively. Ubiquitous events such as malware, single denial of service attacks, or other events that are detected, mitigated, and resources restored within a reasonable amount of time with locally available unit resources are not included in these procedures.

Implementation

1. Ongoing or real-time crisis situations require immediate response and should be reported by phone call to the Texas A&M IT help desk at 979-345-8300 or the Chief Information Security Officer (CISO) at 979-845-0372.

2. It is the responsibility of all university employees to report suspected or confirmed IT security related events, incidents, or crises.
2.1 Anyone can report illegal, disruptive, or unusual activity at any time to one of these offices:

2.1.1 Texas A&M IT help desk

2.1.2 security@tamu.edu

2.1.3 CISO@tamu.edu

2.1.4 After normal business hours contact: helpdesk@tamu.edu or call 979-845-8300 to request the CISO.

ROLES

1. Chief Information Officer (CIO) – within the context of this procedure this position is responsible to the university CEO for management of the university’s information resources. The CIO will designate the IR-CIRT Crisis Manager (CM) in consultation with the CISO. The CIO will also determine the need, when appropriate, for a unified inter-departmental or intra-unit IR Crisis Management team.

2. Chief Information Security Officer (CISO) – The CISO is the university’s internal and external point of contact for all information resources security matters. The CISO, in consultation with the CIO, may function as the Crisis Manager on the IRCIRT.

3. Crisis-Incident Manager, IR-CIRT (CM) - the individual assigned by the CIO or the CISO to provide primary leadership to a university level IR-CIRT. When activated, all of the information resource crisis activities are coordinated by this individual including, but not limited to: assessment, mitigation, repair, restoration of services, investigations, reports, etc.

4. Crisis Response Team, Information Resources (IR-CIRT) - personnel responsible for coordinating or facilitating the response for information resources/computer security crises at the university level. IR-CIRT members report directly to the Information Resources Crisis-Incident Manager (CM). Positions that could normally be included in an IR-CIRT (but are not limited to):

   4.1 Information Resources Crisis-Incident Manager

   4.1.1 Department or Unit Advisor

   4.1.2 University Executive Leadership Liaison

   4.1.3 Communications Team Leader

   4.1.4 Operations Team Leader

   4.1.5 Supporting Crises Personnel (dependent upon the needs of the crisis)

5. Liaison, Executive Leadership (Liaison) – this individual is the conduit for information flow between the Crisis Manager and university executive managers.
6. Office of General Counsel (OGC) – may be called upon to help assess the need for legal action.

7. Owner of an Information Resource (Information Resource Owner) – this individual will retain ownership of resources and may advise the CM about current state and desired state of impacted information resources.

8. Advisor, Information Resources (IR-Advisor) - an individual assigned by the department/unit head and who will be the department/unit’s contact with the IRCIRT CM for questions regarding ongoing objectives and actions being taken to mitigate the effects of the information resources crisis. This individual serves as liaison between the IR-CIRT and the department/unit head. This individual reports directly to both the CM and to their respective department/unit head.

9. Internal System Audit – Audit may be called upon to help assess the security controls applied to information resources. During an on-going information resources crisis, auditors will coordinate with the CM so as not to disrupt activities needed to mitigate the crisis.

10. Supporting Crisis Resources – individuals that are not specifically identified in this section but provide support to IR-CIRT functions. Such resources may be individuals with a particular skill or third parties with access to needed resources (e.g., Crisis Coordinator, Communications Leader, Technical Support, vendor or third party contacts) and who may be called upon to provide said services or other duties.

11. University Police Department (UPD) – UPD is normally the liaison between the university and law enforcement agencies external to the university. While an information resources crisis is ongoing, the UPD will coordinate directly with the assigned CM or designee.

Last Revised: September 1, 2016

(This control replaces the previous SAP 29.01.03.M1.09 Information Resources – Crisis Management)