

INFORMATION TECHNOLOGY STANDARD ADMINISTRATIVE PROCEDURES

SAP No. 24.99.99.W1.10

Information Resources – Incident Management

Approved: April 15, 2005

Last Revised: August 30, 2011

Next Scheduled Review: August 2012

Supplements [University Rule 24.99.99.W1](#)

1. General

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 any University Community member is aware of them either by phone or email to security@wtamu.edu. Once an incident is reported the CIO and ISO will determine the severity of the incident, and categorize it appropriately.

If an incident involves the loss of “Personal Identifying Information” as defined in Texas Business & Commerce Code § 521 section (a), notification of the incident will be made in accordance with § 521.053 sections (e) & (f). Notification should include a general description of the incident, steps individuals can take to mitigate harm, including credit report monitoring and fraud alerts, as well as sources of information designed to assist the public in protecting against identity theft, a reminder to remain vigilant over the next 12 to 24 months, and a customer service number individuals can call for additional information.

<http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm>

2. Applicability

This Standard Administrative Procedure (SAP) applies to all TAMU 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 intended audience is system administrators, Directors, and Department Heads.

3. Definitions

- 3.1 **Information Resources:** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- 3.2 **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.
- 3.3 **Information Security Officer (ISO):** Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

4. Incident Categories:

Level 1 - Least severe and most common type of incident, these have no wide spread effect on any University function. Level 1 incidents shall be handled by the appropriate IT department, via work orders. Incident types and quantities shall be tracked and reported at the IRT monthly meeting, and to the Department of Information Resources (DIR), via their Security Incident Reporting (SIRS) system.

Level 2 - Incidents that have a small impact on operational functionality but have no impact on the overall business function of the University. Level 2 incidents shall be handled by the appropriate IT department, via work orders, and reported to the CIO, or ISO. IT personnel shall continue to monitor the incident, after remediation, and report findings to the CIO and ISO for as long as they deem necessary. Incident types and quantities shall be tracked and reported at the IRT monthly meeting, and the Department of Information Resources (DIR), via their Security Incident Reporting (SIRS) system.

Level 3 - Most severe incidents, these have a major impact on either business or operational functions of the University, and may prevent the University from fulfilling its mission. This category also includes incidents that may cause damage to the University's reputation, or financial damage. Level 3 incidents shall require an emergency meeting of the IRT. The Incident will be handled by the appropriate IT department manager, via work orders, and all steps taken must be approved by either the CIO, or ISO. IT personnel shall continue to monitor the incident, after the threat has been mitigated, and report findings to the CIO and ISO for as

long as they deem necessary. An incident report will be prepared by the ISO, for review by the CIO, IRT and upper administration. Incident types and quantities shall be tracked and reported to the IRT and the Department of Information Resources (DIR), via their Security Incident Reporting (SIRS) system.

The following are examples of the categories of IT security related Incidents:

Incident Categories	Description	Examples
Level 1	These have no wide spread effect on University functions.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - Unauthorized access to sensitive systems - Improper use of high level accounts such as root or administrator - Defacement of WTAMU web site. - Denial of service attacks - Unauthorized changes to key infrastructure - Theft/Loss of computer systems, or media, containing sensitive information or confidential information -IT related PCI or FERPA violations

4. Procedures

- 4.1 Information Security Administrators have information security roles and responsibilities which can take priority over normal duties.
- 4.2 Information Security Administrators are responsible for notifying their Deans and/or Department Heads of any incidents. Notification shall also be made to the Information Security Officer.
- 4.3 Information Security 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 with assistance from the Information Security Officer.
- 4.4 The Information Security Administrators shall report the security incident(s) to Deans and/or Department Heads, and the University Information Security Officer. Any incident that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) should also be reported to the University Police Department.
- 4.5 If fraud or theft is suspected as part of the security incident detection, the person detecting the incident should follow System

Policy 21.04 Control of Fraud and Fraudulent Actions.

- 4.6 If there is a substantial likelihood that security incident(s) could be propagated to other systems beyond departmental control, Information Security Administrators should report such incidents to the Helpdesk, (806) 651-4357, or via email to <mailto:security@mail.wtamu.edu>, as soon as an incident is identified.
- 4.7 The information security officer (ISO) shall file an incident report to the Department of Information Resources.
- 4.8 Any incident that may involve criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) shall also be reported to the University Police Department.
- 4.9 For incidents directly involving University employees, the Personnel department will be contacted, as well as the appropriate Vice President or Dean.
- 4.10 For incidents directly involving a University student the Vice President for Student Affairs will be contacted.

IRT Team:

In an effort to help mitigate IT Security Related Incidents WTAMU has formed the IT Incident Response Team (IRT). The IRT will hold regular meetings to review any incidents that occurred, and discuss projects relating to IT Security. Emergency meetings may also be called at the discretion of the CIO or ISO, if an incident needs immediate attention. The following are members of this team and their roles within the team:

[James Webb](#), CIO, team leader will run meetings, categorize incidents, and report to upper administration.

[Lane Greene](#), Security Analyst (Information Security Officer), backup Team leader, categorize incidents, documents Incident reports for level 3 Incidents, reports all Incidents to DIR via SIRS, primary point of contact for security matters.

[Raymond Duncan](#), Supervisor of Programming Services, Team member in charge of all aspects with regard to Datatel Colleague system.

[Mike Howsmon](#), Network Systems Engineer, Team member in charge of all aspects with regard to University network.

[Michael Reagan](#), ITSC Supervisor, team member in charge of all aspects with regard to University desktop systems, and in charge of updating University Community.

[Dan Garcia](#), Telecommunications Supervisor, team member in charge of all aspects with regard to University telecommunications.

[Carl Welch](#), Web Programmer, team member will advise team on aspects of Web security and Linux\Unix systems on campus.

[Tana Miller](#), Registrar (FERPA Officer), team member will advise team on all aspects with regard to FERPA, as well as enrollment management processes.

[Shelly Davis](#), Director of Accounting (PCI Compliance Coordinator), team member will advise team with regard to PCI Compliance, as well as Business and Finance processes.

[Barbara Petty](#), Assistant Vice President for Academic Affairs (Member from Academic Affairs) team member will advise team with regard to processes within Academic Affairs.

[Zach Workman](#), Assistant Vice President for Risk Management & Compliance, team member will advise team on risk and compliance matters.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer