

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.08 Incident Response

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

This procedure describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to; malware 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.

2. APPLICABILITY

This university procedure applies to all university information resources.

The purpose of the implementation of this university procedure 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

The intended audience is system administrators, directors, and department heads.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

4.1. University system administrators have information security roles and responsibilities, which can take priority over normal duties.

4.2. University employees must report any security incidents that may involve criminal activity under Texas Penal Code Chapters 33 – Computer Crimes or 33A – Telecommunications Crimes to the Information Resources Manager who shall report each incident as defined in TAC 202.76.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 4.3. 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 and Fraudulent Actions.
- 4.4. The Information Resources Manager shall coordinate the design, development, publication, testing, implementation, control, and maintenance of an incident response plan for the university. The incident response plan includes processes and strategies for identifying and responding to security incidents of varying severity related to university information resources. All university departments and colleges shall adhere to and provide resources for responding to specific security incidents according to strategies documented within the incident response plan.
- 4.5. Resource custodians and department managers that identify security incidents that could propagate to other systems beyond departmental control shall immediately report such incidents to the Media and Computer Services Helpdesk.
- 4.6. Security incidents involving any system that contains sensitive information, is directly connected to storage containing sensitive information, or accesses sensitive information through a network connection shall be immediately reported to the Information Resources Manager.
- 4.7. The University Marketing and Communications office shall handle all interactions with public or private media related to any security incident involving university information resources and sensitive information. All university employees must refer any questions about these issues to this office.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- Texas A&M System Policy
 - 01.03 Appointing Power and Terms and Conditions of Employment
 - 07.01 Ethics Policy, TAMUS Employees
 - 32.02 Discipline and Dismissal of Employees
 - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
 - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
 - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
 - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration