

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.05 Backup Recovery

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Electronic backups are a requirement to enable the recovery of data and applications in case of events such as natural disasters, system disk drive failures, corruption, data entry errors, or system operations errors. The purpose of the university backup/recovery procedure is to establish the process for the backup and storage of electronic information.

2. APPLICABILITY

This university procedure applies to university resources that contain sensitive information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with backup/recovery of information. 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 all university staff responsible for the support and operation of university information resources which contain Sensitive Information.

3. DEFINITIONS

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

4. PROCEDURES

4.1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner(s).

4.2. The backup and recovery process for each university information resource must be documented and periodically reviewed.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 4.3. The vendor(s) providing offsite backup storage for university information resources must be cleared to handle the highest level of information stored.
- 4.4. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest sensitivity level of information stored.
- 4.5. A process must be implemented to verify the success of the information backup.
- 4.6. Backups must be periodically tested to ensure that they are recoverable.
- 4.7. Physical and logical authentication mechanisms used by the offsite backup storage vendor(s) for permitting access to university backup media must be reviewed annually or when an authorized individual leaves the university.
- 4.8. Procedures between the university and the offsite backup storage vendor(s) must be reviewed at least annually.
- 4.9. Backups of systems that contain, or may contain, sensitive information must be encrypted and stored in a secure location, and the keys associated with the encryption mechanism must be escrowed in a secure location.
- 4.10. Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
 - (1) system name,
 - (2) creation date,
 - (3) security risk rating as outlined by Texas Administrative Code 202.72 Managing Security Risks,
 - (4) university contact information, and
 - (5) type of encryption.

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.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

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.

- 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