**Texas A&M University-San Antonio**

29.01.03.O0.06  Backup Recovery  
Approved: June, 2013  
Next Scheduled Review: June 2015

---

**Procedure Statement**

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 information resources.

---

**Reason for Procedure**

This Standard Administrative Procedure (SAP) applies to all University resources that contain mission critical information.

The purpose of this Standard Administrative Procedure is to provide a set of measures that will mitigate information security risks associated with Backup/Recovery of information resources. There may also be other or additional measures that owners of information resources, department or division heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators in collaboration with the University ISO. 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 SAP based on documented and approved information security risk management decisions and business functions.

The Texas A&M University-San Antonio account management security policy applies equally to all individuals with authorized access to any Texas A&M University-San Antonio Information Resources.
1. PROCEDURES

1.1. The extent of backups shall be determined by the importance of the information, potential impact of data loss/corruption, and risk management decisions by the data owner. Backups shall be stored on backup media, redundant disk drives, and/or virtual tape libraries. Activities from the annual risk assessment will assist in identifying this importance.

1.2. Mission critical information backup and recovery processes for each system, including those for offsite storage, must be documented and reviewed periodically.

1.3. Physical access controls implemented for on or offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additional backup media must be protected in accordance with the highest sensitivity level of the information stored.

1.4. Backups shall be periodically tested to ensure that they are recoverable.

1.5. Physical and logical authentication mechanisms used for permitting access to university backup applications and media must be reviewed annually or when an authorized individual leaves the university.

1.6. Any vendor(s) providing offsite backup or backup storage for university information resources must be cleared to handle the highest level of information stored. Procedures between the university and the offsite backup or backup storage vendor(s) must be reviewed at least annually.

1.7. Backups of system that contain, or may contain, sensitive information must be encrypted and stored in a secure, environmentally safe, locked facility accessible only to authorized University approved representatives (TAC 202.74(b) and the keys associated with the encryption mechanism must be escrowed in a secure location.

1.8. All backup media shall be preserved for the appropriate retention period prior to being overwritten for reuse.

2. DISCIPLINARY ACTIONS.

2.1. Violation of this procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Students are bound to the code of student conduct. Additionally, individuals are subject to loss of access and privileges to The University information resources, civil, and criminal prosecution.
Related Statutes, Policies, or Requirements

TAMU-SA Procedure 29.01.03.00.01 Electronic Information Services Access and Security

Definitions

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) – The IRM ensures that all information resources are acquired appropriately, implemented effectively, and complies with regulations and agency policies. Per requirements of the State of Texas, each agency or institution of higher education must designate an IRM.

Information Resource Owner – an entity responsible for:
  • A business function; and,
  • Determining controls and access to information resources supporting that business function.

Mission Critical Information - Information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Information Security Officer (ISO) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the university’s internal and external point of contact for all information security matters.

Contact Office

Information Technology Services – (210) 784-4357 (HELP)