The Division of Information Technology
University Information Security Standards

Information Security Standard – Backup Recovery (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

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 information resources.

2. Applicability

This standard applies to all University resources that contain mission critical information.

The purpose of this standard 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 division, department heads, or deans 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 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 is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all University staff responsible for the support and operation of University information resources which contain mission critical information.

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 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.3 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, and failure to comply with regulations or legal obligations, or closure of the University or department.

3.4 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. Procedure

4.1 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 (Department Heads and Information Security Administrators). Backups shall be stored on backup media, backup system disk drives, and/or virtual disk backup systems. Activities from the annual risk assessment will assist in identifying this importance.

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

4.3 Physical access controls implemented at offsite backup storage locations.

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

4.7 All backup media shall be maintained for six months prior to being overwritten for reuse.

4.8 The centralized backup program shall be conducted on a daily basis with additional backups to occur at month end. Offsite data vaulting shall be conducted electronically and synchronized from the primary campus data center to the information resources facility at the Amarillo Center.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer