

THE TEXAS A&M UNIVERSITY SYSTEM HEALTH SCIENCE CENTER INTERNAL POLICIES

29.01.99.Z1.03 Backup/Recovery

Approved September 1, 2010

Supplements System Policy 29.01

1. GENERAL

1.1 Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Backup/Recovery Policy applies to all individuals within the HSC that are responsible for the installation and support of information resources, individuals charged with information resources security and data owners.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.

1.5 Definitions

- **Information Resources (IR):** 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.

- **Backup:** Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.
- **Offsite Storage:** Based on data criticality, offsite storage should be in a geographically different location from the HSC campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the HSC Campus may be appropriate.
- **Vendor:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

2. BACKUP/RECOVERY POLICY

- 2.1 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.
- 2.2 The HSC information resources backup and recovery process for each system must be documented and periodically reviewed.
- 2.3 The vendor(s) providing offsite backup storage for HSC must be cleared to handle the highest level of information stored.
- 2.4 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 HSC sensitivity level of information stored.
- 2.5 A process must be implemented to verify the success of the HSC electronic information backup.
- 2.6 Backups must be periodically tested to ensure that they are recoverable.

2.7 Signature cards held by the offsite backup storage vendor(s) for access to HSC backup media must be reviewed annually or when an authorized individual leaves HSC.

2.8 Procedures between HSC and the offsite backup storage vendor(s) must be reviewed at least annually.

2.9 Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:

- System name
- Creation Date
- Sensitivity Classification [Based on applicable electronic record retention regulations.]
- HSC Contact Information

3. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; 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. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY

Vice President for Information Technology and Chief Information Officer