

Section x	<b>IS Security Policies</b>	mm/dd/yy	-Effective
Policy x.xx	<b>Backup/DRP</b>	mm/dd/yy	-Revised
		Information Services	-Author

---

## 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.

---

## Purpose

The purpose of the [AGENCY] Backup/DRP Policy is to establish the rules for the backup and storage of electronic [AGENCY] information.

---

## Audience

The [AGENCY] Backup/DRP Policy applies to all individuals within the [AGENCY] enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security and data owners.

---

## 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 [AGENCY] 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 [AGENCY] Campus may be appropriate.

**Vendor:** someone who exchanges goods or services for money.

---

## Services

Information Services may have existing contracts for offsite backup data storage. These services can be extended to all [AGENCY] entities upon request.

Section x	<b>IS Security Policies</b>	mm/dd/yy	-Effective
Policy x.xx	<b>Backup/DRP</b>	mm/dd/yy	-Revised
		Information Services	-Author

---

## Backup Policy

- 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.
- The [AGENCY] Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for [AGENCY] must be cleared to handle the highest level of information stored.
- 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 [AGENCY] sensitivity level of information stored.
- A process must be implemented to verify the success of the [AGENCY] electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s) for access to [AGENCY] backup media must be reviewed annually or when an authorized individual leaves [AGENCY].
- Procedures between [AGENCY] and the offsite backup storage vendor(s) must be reviewed at least annually.
- 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.]
  - ❖ [AGENCY] Contact Information

---

## Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; 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 [AGENCY] Information Resources access privileges, civil, and criminal prosecution.

Section x	<b>IS Security Policies</b>	mm/dd/yy	-Effective
Policy x.xx	<b>Backup/DRP</b>	mm/dd/yy	-Revised
		Information Services	-Author

**Supporting Information**

**This Security Policy is supported by the following Security Policy Standards.**

**Reference # Policy Standard detail**

- 7 Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
- 9 On termination of the relationship with [AGENCY], users must surrender all property and IR managed by [AGENCY]. All security policies for [AGENCY] IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.
- 11 The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.
- 14 The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
- 16 Custodian departments must provide adequate access controls and system monitoring to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

Section x	<b>IS Security Policies</b>	mm/dd/yy	-Effective
Policy x.xx	<b>Backup/DRP</b>	mm/dd/yy	-Revised
		Information Services	-Author

**Supporting Information, continued**

**This Security Policy is supported by the following Security Policy Standards.**

**Reference # Policy Standard detail**

- 17** All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that [AGENCY] is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.
- 18** All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized [AGENCY] officer and must contain terms approved as to form by the Legal Department, advising vendors of [AGENCY]'s IR retained proprietary rights and acquired rights with respect to its information systems, programs, and data requirements for computer systems security, including data maintenance and return.
- 19** [AGENCY] IR computer systems and/or associated equipment used for [AGENCY] business that is conducted and managed outside of [AGENCY] control must meet contractual requirements and be subject to monitoring.

**References**

Copyright Act of 1976  
Foreign Corrupt Practices Act of 1977  
Computer Fraud and Abuse Act of 1986  
Computer Security Act of 1987  
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)  
The State of Texas Information Act  
Texas Government Code, Section 441  
Texas Administrative Code, Chapter 202  
IRM Act, 2054.075(b)  
The State of Texas Penal Code, Chapters 33 and 33A  
DIR Practices for Protecting Information Resources Assets  
DIR Standards Review and Recommendations Publications