Backup Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

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

# II. Purpose

The purpose of this policy is to establish the rules for the backing up and storage of backups containing ABC Company’s electronic information.

# III. Scope

This policy applies to all Staff that are responsible for the installation and support of IT, individuals charged with IT Security, and data owners.

# IV. Policy

Backups are used to provide corrective action against various types of threats including:

* Human error - accidental deletion of files
* Malicious software – viruses delete or corrupt systems and data
* Intentional actions – a hacker deletes files
* Hardware failure – a hard drive fails and files must be deleted
* Application processing errors – database must be restored
* Facility issues – a fire, water damage, or electrical surge damages equipment

Backups are an important part of providing Information System availability and are critical to ABC Company’s business continuity. The Chief Security Officer (CSO) will determine the risks related to Information Systems and will evaluate the following tiers to determine the appropriate Tier for ABC Company given our Business Impact Analysis, recovery time objectives (how much downtime is acceptable), recovery point objectives (how much data loss is acceptable), and costs:

* Tier 1: Data backup with no hot site - systems are backed up and the media is sent to an off-site storage facility. Without a hot site, recovery may require weeks or months. Manual or additional processes are needed to continue business operations.
* Tier 2: Data backup with a hot site – contains the elements of Tier 1 plus a hot site provides the required hardware and operating systems to allow recovery from the backup media. Recovery can typically be achieved in one to two days depending upon the extent of damage, activation of hot site, and restore time.
* Tier 3: Electronic vaulting - contains the elements of Tier 2 plus mission critical data is electronically vaulted where data is transmitted to another secure location (typically off-site) via a network or communication link rather than via portable media. Recovery can typically be achieved in less than one day.
* Tier 4: Point-in-time copies (images) - key systems are copied to disk according to a pre-determined schedule. In this Tier either an off-site facility receives encrypted disks or the point in time copies (images) are used to supplement traditional encrypted backup media sent off-site. Imaging enables the quick recovery of an entire system. Depending upon the type of disruption, recovery may require several hours up to one day.
* Tier 5: Transaction integrity - software applications are coded to ensure transactions are fully complete with integrity. This ensures consistency of data between production and recovery systems. Recovery may be able to be achieved in less than one hour.
* Tier 6: Near zero data loss - robust business continuity solutions maintain the highest levels of data currency and allow quick access to data. Solutions have no dependence on the applications and may require some form of disk mirroring or synchronizing solutions. Recovery may be achieved in less than an hour with almost no loss of data.
* Tier 7: Highly automated, business integrated solution - contains the elements of Tier 6 plus automation. Restoring of systems, applications, and data is automated. This Tier may involve data replication to a redundant data center. Recovery may be achieved in a few minutes with almost no loss of data.

Once the appropriate Tier has been identified, the Chief Security Officer shall ensure:

* ABC Company’s Backup Plan identifies procedures to implement the requirements of this policy and the appropriate Tier.
* All system data is automatically backed up on regular basis.
* Documentation identifies the location of sensitive information to ensure that it can be backed up.
* Documentation includes all important sources of data such as accounting systems, electronic records, diagnostic images, and other documents created or used.
* Procedures create and maintain retrievable exact copies of information.
* The frequency and implementation of backups is appropriate according to the requirements of the selected Tier.
* Backups are stored and transmitted in a safe and secure manner and comply with the requirements of the selected Tier.
* Backups are encrypted to ensure information confidentiality. This includes remote backups and cloud services.
* All backups have at least one offline (i.e., not accessible via a network connection) backup destination.
* Procedures specify when a retrievable, exact copy of sensitive information must be created before movement of equipment.
* Procedures identify who is responsible for creating a retrievable exact copy of sensitive information before movement of equipment.

The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the data owner. The IT backup and recovery process for each system must be documented and periodically reviewed.

Vendor(s) providing off-site backup storage and recovery solutions must be cleared to handle the highest level of information stored.

Physical access controls implemented at off-site backup storage and recovery locations must meet or exceed the physical access controls of the source systems. Backups must be protected in accordance with the highest sensitivity level of information stored.

A process must be implemented to verify the success of the electronic information backup. Backups must be periodically tested to ensure that they are recoverable.

Signature cards held by the off-site backup storage and disaster recovery vendor(s) for access to backups must be reviewed annually or when an authorized individual leaves ABC Company.

Procedures between ABC Company and the off-site backup storage and disaster recovery vendor(s) must be reviewed at least annually.

Backups must have at a minimum the following identifying criteria that can be readily identified:

* System name
* Creation date
* Classification
* ABC Company contact information

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to IT management, IT system administrators, and the Chief Security Officer.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, APO12.02, APO12.07, APO13.07, DSS04.05, DSS04.05, MEA03.03

GDPR Article 25, 32

HIPAA 164.308(a)(7)(ii)(A)

ISO 27001 A.12.3

NIST SP 800-37 Appendix D

NIST SP 800-53 AU-9, CP-6, CP-9, CP-10

NIST Cybersecurity Framework PR.IP-4, RS.RP-1, RC.RP-1

PCI 9.5.1, 10.7, 12.10.1