Backup Procedure

|  |  |
| --- | --- |
| 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

The Backup Policy provides management direction and guidance to ensure systems and data are properly backed up. This procedure specifies the steps and actions performed to meet the requirements of ABC Company’s Backup Policy.

# II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in ABC Company's Backup Policy.

# III. Scope

This procedure applies to all ABC Company Staff who perform and are responsible for backing up Information Systems.

# IV. Procedure

Physical security. Backups, including off-site and recovery backups, are placed in a physical location that restricts access to authorized individuals. Vendor(s) providing off-site backup storage and recovery solutions have been cleared to handle the highest level of information stored. Signature cards held by the off-site backup storage and disaster recovery vendor(s) for access to backups are reviewed annually or when an authorized individual leaves ABC Company. Procedures for secure transfer between ABC Company and the off-site backup storage and disaster recovery vendors are reviewed annually and more frequently if needed.

Documentation. Documentation is created and updated as needed. The location of sensitive information is identified so it can be backed up. Documentation specifies Information Systems to be backed up, Information System name, creation date, classification, and ABC Company contact information. In addition, documentation includes responsible personnel, storage requirements, encryption used, backup type (i.e. incremental or full), frequency (e.g. hourly, daily, weekly, monthly, etc.), steps to restore data from backups, and other important information. Documentation identifies Staff responsible for creating a retrievable exact copy of sensitive information before movement of equipment. The IT backup and recovery process for each system are documented and reviewed on an annual basis and when changes are made to the environment. Backup documentation includes relevant manufacturer recommendations.

Alerts, advisories, and vulnerability announcements. Manufacturer alerts, advisories, and vulnerability announcements are monitored. Patches and updates related to backups are installed in a timely manner per the Patch Management Policy.

Time. An accurate time and date is important for system and event logs. A trusted time source for Network Time Protocol (NTP) has been selected and proper authentication is used when performing backups.

Backups. All system data is automatically backed up on regular basis. All backups have at least one offline (i.e., not accessible via a network connection) backup destination.

Logging and monitoring. Logging of backups is performed per the Logging Policy. On a daily basis backup logs are reviewed and appropriate action taken.

Testing. Backups are periodically tested by restoring files and performing steps needed to ensure the backup restore was successful. Testing verifies the necessary files, applications, and configurations were properly restored.

Configurations. A copy of important device configurations is saved at a separate and secure location to assist in a recovery effort if needed. Backup settings are pre-defined and not changed without proper approvals.

Backup changes. A restore test is performed after a change or modification to backup hardware, software, or configurations. The test includes restoring from backups made prior to the change as well as conducting a test backup and restore using the new or modified hardware, software, or configurations.

Manufacturer resources. Manufacturer resources provide additional guidance on backups and specific backup functionality and procedures.

Disposal. Refer to the Disposal Policy for information on the reuse or disposal of backups and related media.

# V. Enforcement

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

# VI. Distribution

This procedure is to be distributed to all ABC Company Staff who administer and perform backups.

**Procedure History**

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