Insert the organization logo by clicking on the image icon

Data Backup Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Data Backup Policy Template | | |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  | |
| **Publish Date:** |  | | |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97461150)

[2. Scope 4](#_Toc97461151)

[3. Policy 4](#_Toc97461152)

[4. Restoration 5](#_Toc97461153)

[5. Backup of Network and Critical Devices 5](#_Toc97461154)

[6. Policy Enforcement 5](#_Toc97461155)

Objective

The purpose of this policy outlines the controls and measures associated with data backup plans and programs that protect <entity name>’s IT assets and will help in business continuity.

Scope

The scope of this policy all <entity name>’s information, software, hardware, databases, applications/programs, network resources are applicable to the <entity name> to conduct its business.

Policy

1. Backup should be conducted regularly that will ensure business continuity in the event of an interrupted process.
2. All data being backed up should be recorded, stored securely in accordance with Law No. (16) Of 2014 concerning Protection of State Information and Documents.
3. Data being backed-up must be encrypted.
4. Backup files copies and documentation should be stored off-site in a secure location and must be transferred to the off-site location on regular bases, preferably at least once daily.
5. Backup data must be stored and secured physical location in compliance with the Access Control and Physical Security Policy.
6. A periodic testing of software backup should be conducted preferably once a year at both in-site and off-site to that backup are in useable condition for recovery. Unreadable backup data must be reported to the IT team.
7. Redundancy of backup data system in case of failure of primary backup system.
8. Backups movements must be monitored and logged. Only authorized users can carry out the deposit and removal of backup data from storage location.
9. Copies of backup files and documentation must be identified and agreed level of security while being moved to or from off-site storage.
10. Backup retention period must be based on relevant regulatory requirements and documented in operations procedures.
11. When a computer is changed or replaced, consideration should be given to backup data and media formats to ensure that they can still be restored and useable.
12. Access to backup data should be able of being retrieved within a time scale documented in Disaster Recovery Policy.
13. A Service Level Agreement (SLA) should be defined and documented once a third-party has the authority to access or store backup media, system, file.
14. Automated backup functions in software packages must be used where applicable.
15. Systems should be backed up immediately in case of any upgrade, changes done to the system or application.
16. The system backup strategy should be formally documented and approved by the system and data owners.
17. Sanitizing data backup must be performed by an authorized user and approved by management level.

Restoration

1. An authorization must be obtained from Data Owners to restore data from a backup media and files that would overwrite existing production data
2. Escalation procedure must be established in case of system failure and made aware to system administrator.
3. Documents, reports, and backup media source must be identified and documented for a system reconstruction.
4. Restoration of a previous configuration should be established and documented.
5. Restoration of current configuration should be within recovery timescale agreement.

Backup of Network and Critical Devices

1. Critical devices availability with sufficient capacity and speed for backup must be established and documented.
   * Maintain a replacement for equipment on-site for critical devices. For example, UPS, LAN interfaces cards, cabling, connectors, etc.
   * Sufficient provision for the re-routing of network messages in the component event failure.
   * Protect critical network servers and LAN components using Uninterruptible Power Supplies (UPS). In accordance with Access Control and Physical Security Policy.

Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-