**Backup Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_vkeoqln0mkwt) **3**

[**Scope**](#_ylg5wprwz8xn) **4**

[**Policy**](#_kck89ytof92) **4**

[**Identification**](#_wqegp173zllr) **4**

[**Timing**](#_xcz68ke3ksz0) **4**

[**Storage**](#_wimpo446bwp9) **4**

[**Testing**](#_7zh4et73021j) **4**

[**Change, Review, and Update**](#_w1o88vxspwq8) **5**

[**Disciplinary Action**](#_lk70sm2hx9ta) **5**

[**Responsibility**](#_c5uzzlc5mr9z) **5**

[**Related Documents**](#_rw27bz2px5aw) **5**

# **Purpose**

*[Company’s]* Backup Policy describes how often service and customer data are backed up. All original customer data on infrastructure operated by us should be backed up.

# **Scope**

This Backup Policy applies to all critical equipment and data owned and operated by us.

# **Policy**

## **Identification**

* The IT Manager working with the management must identify specific items relating to the business that must be backed up regularly and the backup frequency.
* All backup activities should be logged.

## **Timing**

*[Company]* configures full, daily backups of databases. The retention period for backups is 14 days.

## **Storage**

The access to backups is controlled and prohibited from unauthorized access. In addition, cryptography controls are in place to ensure the security of backup storage.

## **Testing**

* The backup testing is initiated exclusively by IT Manager.
* The testing of backups is done at least annually as a part of our Disaster Recovery testing.
* Any errors found during the backup testing must be communicated with IT Manager.
* The test results should be documented, and the backup process shall be modified to avoid similar discrepancies in the future.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed. However, all staff is responsible for following the Data Protection Policy.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Disaster Recovery Plan
* Data Protection Policy