**[Company]**

**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 after that.

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

#

# ***Table of Contents***

[**Version Control Table**](#_acsm13oho249) **2**

[**Table of Contents**](#_ukruovgntws6) **3**

[**Purpose**](#_67i62vthxmjc) **4**

[**Scope**](#_sebszm58trwj) **4**

[**Policy**](#_5rj02xnd3hsl) **4**

[Information backup](#_5pm7n5y25pd2) 4

[Timing](#_99fv2rmh4ohy) 4

[Testing](#_1vryqmwmfit7) 4

[Storage](#_jzx8fyyws11) 5

[Retention period](#_qfg8bf4wu78f) 5

[**Disciplinary actions**](#_tfm2t62n6ro) **5**

[**Change, Review, and Update**](#_gfxmghp2iiwl) **5**

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

[**Reference**](#_1ksv4uv) **5**

[**Related Documents**](#_a2bhg29tumfn) **5**

#

#

# Purpose

The purpose of this policy is to identify all critical assets, requirements, and retention periods for [company] critical systems.

# Scope

This policy applies to all [company] employees, contractors, third parties who access internal information and business processes.

# Policy

## Information backup

* The backup must be done of selected critical assets in the first place. All company key systems must be backed up as a complete system with imaging processes to enable the quick recovery of the entire system.
* The company must back up the data in case of data changes, so a continuous backup approach is the best.
* The considerations must be in place to define the importance of having backups of backups. So, there will be a redundancy to ensure that another can take its place if one backup fails.
* Any vendors providing offsite backup storage must be cleared to handle the highest level of information stored.
* Backups must have at a minimum the following identifying criteria that labels can readily identify:
	+ System name;
	+ Creation Date;
	+ Sensitivity Classification.

## Timing

* The information’s importance must determine the frequency and extent of backups and the acceptable risk determined by the data owner.
* The backups for critical resources must be taken at least once every 24 hours.

## Testing

Backups’ integrity is periodically tested by performing a data restoration process to ensure that the backup is appropriately working. The IT team selects and evaluates a random sample of system backups by restoring it in the test environment. The fixed systems are then verified to ensure that the backup data is functional.

## Storage

* Backup copies of operating systems and other critical information system software shall not be stored in the exact location as the operational software.
* The access to backups is controlled and prohibited from unauthorized access. The cryptography controls must be in place to ensure the security of backup storage.

## Retention period

The backup stays valid for 3 months only by default, so it is unnecessary to keep them longer.

# Disciplinary actions

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

# 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 the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.12.3.1 Information Backup

# Related Documents