**<Your Company Logo>**

**Encryption Policy**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

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 summarize the difference and is not a substitute for reading the full text.

# 

# ***Table of Contents***

[**The Path to Compliance 1**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 1**](#_bor2nqthjwhg)

[**Need Expert Assistance? 1**](#_j1ad4z2lk78s)

[**Version Control Table 3**](#_arxqdy8knprl)

[**Table of Contents 4**](#_2s8eyo1)

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

[**Scope 5**](#_44sinio)

[**Policy 5**](#_2jxsxqh)

[Encryption Strategy 5](#_z337ya)

[Encryption of Data at Rest 5](#_3j2qqm3)

[Encryption Key Management 6](#_1y810tw)

[**Disciplinary actions 6**](#_4i7ojhp)

[**Change, Review, and Update 6**](#_2xcytpi)

[**Responsibility 6**](#_1ci93xb)

[**Reference 6**](#_3whwml4)

[**Related Documents 6**](#_2bn6wsx)

# 

# Purpose

The purpose of this policy is to outline the <Company> standards for the use of encryption technology so that it is used securely and managed appropriately.

# Scope

This policy covers all data stored on or transmitted across corporate systems.

# Policy

## Encryption Strategy

The following represents the <Company> encryption strategy:

* If disk encryption is used, logical access should be managed independently of native operating system access control mechanisms.
* All information must be encrypted by communication protocols such as HTTPS/TLS1.2 (or higher) when transmitted outside of our company.
* Using only laptops and desktops that have encrypted hard drives.
* Decryption keys should not be tied to user accounts.
* Protect cryptographic keys used for encryption of confidential data against disclosure and misuse.
* Restrict access to cryptographic keys to the fewest number of custodians necessary.
* Store cryptographic keys securely in the fewest possible locations and forms.
* Generate strong cryptographic keys to protect confidential data.
* Secure cryptographic key distribution.
* Secure cryptographic key storage.
* Perform cryptographic key rotation periodically.

## Encryption of Data at Rest

Encryption of data at rest is required to store confidential data, such as any data located on company-owned or company-provided systems, devices, media, etc. This includes the following options for stored data:

* Whole disk encryption
* Encryption of partitions/files
* Encryption of disk drives
* Encryption of backups
* Database encryption

## Encryption Key Management

The following recommendations apply to the Company private SSH keys.

* Management of keys must ensure that data is available for decryption when needed.
* Keys must be backed up.
* Keys must be securely stored.
* Keys must be protected through their whole life cycle against modification, loss, unauthorized access/use or disclosure.
* Keys must never be transmitted in cleartext.
* Keys are to be treated as confidential data.
* Keys must not be shared.
* Keys must be used and changed at a minimum annually.

# 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 A.10.1.1 Policy on the Use of Cryptographic Controls
* ISO 27001 A.10.1.2 Key Management

# Related Documents