**<Your Company Logo>**

**Network Security 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>** |

# 

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_arxqdy8knprl)

[**Table of Contents 5**](#_ukruovgntws6)

[**Purpose 5**](#_c1g4bgtkjdjs)

[**Scope 6**](#_3dy6vkm)

[**Policy 6**](#_1t3h5sf)

[Network Device Configuration 6](#_6y5ig62sdi8c)

[Network Documentation 6](#_hgps6mfz0l21)

[Networking Devices 6](#_fxq95tusphc6)

[Servers 6](#_gwmg2hidjrto)

[Security Assessments 7](#_iz57b4j2k9dk)

[**Disciplinary actions 7**](#_oo4pebgvtuk2)

[**Change, Review, and Update 7**](#_6cu0cv3y3y7n)

[**Responsibility 7**](#_fxvzxllev4xj)

[**Reference 7**](#_1ksv4uv)

[**Related Documents 7**](#_oqj2g9kzbmil)

# 

# Purpose

The purpose of this policy is to establish the technical guidelines for network security and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the company's comprehensive set of security policies.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses <Company> information assets or information resources and services.

# Policy

## Network Device Configuration

* Authentication on Network devices must be configured according to <Company> Password Management Policy. Special considerations are to be made due to the nature of the device.
* Administrative access to systems must be limited to only those with a legitimate business need.

## Network Documentation

The company requires that network documentation be updated at least quarterly or after big changes. At a minimum, network documentation should include:

* <Company> Network diagram

## Networking Devices

Network devices’ configuration checks should be implemented consistently. The following requirements apply to the company's implementation of network devices:

* Network devices must provide secure administrative access (through encryption) with management access limited to only networks where management connections would be expected to originate.
* Clocks on all network devices should be synchronized using NTP or other means.
* Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the router should be limited to the greatest extent possible.
* Unused services and ports must be disabled on network devices.
* Access to administrative ports on the network devices must be restricted to known management hosts and otherwise blocked with a firewall or access control list.

## Servers

The following requirements apply to Company servers:

* Unnecessary files, services, and ports should be removed or blocked.
* Servers, even those meant to accept public connections, must be protected by a firewall or access control list.
* A standard installation process should be developed for the company’s servers.
* Management access to servers must be available only to authorized users from a protected network perimeter or a specified list of IP addresses.

## Security Assessments

Security testing be performed on the following recurring schedules:

* Vulnerability Scanning must be performed biweekly
* Penetration Testing must be performed at least once per year

System administrators are responsible for the patch management process.

# 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.13.1.1 Network Controls

# Related Documents

* <Company> Password Management Policy
* <Company> Network Diagram