**<Your Company Logo>**

**Patch Management 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 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)

[**Responsibilities 6**](#_4x9ezfieu1o7)

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

[Laptops 6](#_17dp8vu)

[Servers 6](#_3rdcrjn)

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

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

[**Responsibility 8**](#_fxvzxllev4xj)

[**Reference 8**](#_1ksv4uv)

[**Related Documents 8**](#_8udt57nez86p)

# 

# Purpose

This policy is provided to define the requirements for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware.

# 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.

# Responsibilities

**Asset Owners​:**

1. Responsible for implementing patch management controls in the company.

**ISMS Manager:**

1. Create documentation.
2. Monitor the quality of the procedures’ execution.

# Policy

A patch is a software update comprising code inserted (i.e., patched) into an executable program code. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:

1. Updating software;
2. Fixing a software bug;
3. Installing new drivers;
4. Addressing new security vulnerabilities;
5. Addressing software stability issues.

## Laptops

1. Every employee’s responsibility is to monitor notifications about new updates available for their OS and install them on their laptops.
2. Automated updates should be enabled on each employee’s laptop.

## Servers

1. The Patch management is established based on the vulnerability management process (described within <Company> Vulnerability Management Policy). After conducting the vulnerability-defining process (Vulnerability scanning and Penetration testing) the asset owners must be notified about current vulnerabilities on their assets.
2. Asset owners are responsible for timely patching every vulnerability according to instructions from the performer of the vulnerability scanning or penetration testing.
3. Any upgrade must be tested before deployment if it is related to critical assets or if it can influence any of the critical assets.

The suggested action items for Patch Management are:

1. Keep the inventory of the critical systems, including the operating systems and software versions, physical location, IP addresses, etc up to date.
2. Assess the vulnerability and risk and classify the risk accordingly. Find servers and systems which are vulnerable and company-critical.
3. Evaluate all missing software updates according to the risk they pose. Missing software updates that pose an unacceptable risk to the company’s resources must be implemented within a commensurate time with the risk.
4. Possible not to apply every patch immediately due to unexpected results within its business operations even though the patch is deemed critical by the vendor. Patches may be considered to have an adverse impact and disrupt business operations. In this case, the decision must be justified and documented and all delays regarding patch management must be authorized by the relevant stakeholders.
5. Compensating controls must be in place within the company if awareness through media (e.g. online reports, vendors, etc.) about vulnerabilities that are identified but do not have an available security patch.

Compensating controls include but are not limited to:

* 1. Raising awareness about the vulnerability within <Company>;
  2. Turning off services or capabilities related to the vulnerability;
  3. Adapting or adding access controls; or
  4. Increased monitoring to detect or prevent actual attacks.

# 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.12.6 Technical Vulnerability Management

# Related Documents

* <Company> Vulnerability Management Policy