[Company]

PATCH MANAGEMENT POLICY

Management of patching

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Patch Management Policy

3.1 Purpose

The purpose of this policy is to ensure operating systems, application software and firmware is updated to address known security vulnerabilities in a timely manner.

3.2 Scope

All employees and third-party users.

All company software, hardware, and virtual services in scope of the ISO 27001 implementation as recorded in the company asset registers.

3.3 Principle

All software and hardware assets are updated to the latest versions in line with vendor provided guidance and industry best practice.

3.4 Patching Controls – End Point Devices

The use of automated patching where available and appropriate is used.

The patching status of end point devices is [redacted]

Where appropriate and available automatic tracking of end point patching is deployed with automatic alerting and reporting of devices that are non-compliant.

Where a device or asset is found to be non-compliant remedial action is taken.

3.5 Patching Controls – Production Systems

Patching of production systems follows the standard change management process.

The patching status of end point devices is [redacted]

Where appropriate and available automatic tracking of end point patching is deployed with automatic alerting and reporting of devices that are non-compliant.

Where a device or asset is found to be non-compliant remedial action is taken.

3.6 Patching Exceptions

An exception list is maintained, managed, and reported via the Management Review Team.

Where a patch cannot be applied, [redacted]

[redacted]

3.7 Patching Schedule

[redacted]

3.8 Patch Severity Rating and Timeframes to Deploy

Patch Severity Rating follows the Microsoft definitions -

https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system

Summarised as follows

Rating	Description	Our Timeframe to Patch
Cr t ca	[redacted]	[redacted]
Important	[redacted]	[redacted]
Moderate	[redacted]	[redacted]
Low	Impact of the vu nerab ty s comprehens ve y m t gated by the character st cs of the affected component. M crosoft recommends that customers eva uate whether to app y the secur ty update to the affected systems.	On eva uat on.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.