PATCHING POLICY

Classification: **Internal**

This document may only be shared with interested parties outside of [Company Name] with the owner's written permission.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of This Document

This policy defines patch management practices across the [Company Name], ensuring that data is protected against out-of-date software and vulnerabilities.

Responsibilities

Information Security Group (ISG)

- The ISG will ensure the maintenance and enforcement of this policy and perform regular checks to ensure its effectiveness.

IT Department

- IT will ensure that all devices are scanned regularly for compliance and vulnerabilities.
- All vendor updates shall be assessed for criticality and applied at least weekly.
- Critical updates should be applied as quickly as safely possible.

Change Advisory Board (CAB)

- The CAB will evaluate and approve emergency patches as detailed in the Change Management Policy.
- Will review any exceptions proposed to the patching policy.

Third Parties

- All vendors supporting systems on behalf of the [Company Name] must ensure that vulnerability patching is undertaken promptly, or they must notify [Company Name] IT and IS as soon as possible

Staff

- All staff are responsible for updating applications or operating systems on personal devices used for [Company Name] business to ensure they are on the most recent versions and do not present a security threat to the organisation.

Policy

Why patch

- Without effective patch management, there is the risk of security incidents caused by hackers, viruses and malware exploiting known system vulnerabilities.
- Out-of-date software and drivers can make systems unstable and degrade their performance.

Patch and Security Updates

Service	**Update Frequency**
Microsoft Servers / Workstations	Every 2nd Tuesday of the month, Microsoft releases patches.

	Non-critical updates are done once every 30 days (4th Tuesday of the month) – after testing.
Firewalls	Upgrades are automatically applied upon vendor release at midnight to minimise end-user disruption.
Network Access Points	Are automatically applied upon vendor release.
Printers	Vendor updates are pushed out automatically wherever available.
Mobile Phone Updates	Automatically applied to mobile devices upon vendor release.

Critical Patches

- Any critical patches should be reviewed upon manufacturer release and implemented as soon as practical and no later than ten working days after release.

Exceptions

- If the [Company Name] determines a compelling need to make an exception to the controls outlined in this policy, a request can be made by contacting the IT team. Exceptions must be escalated to the CAB to ensure any additional controls are implemented, and the business accepts any residual risk.