# Patch management policy for small business

## Small business variant: paste over the same-numbered sections of the general policy

## 1 Purpose and scope

**1.1** [Company name] keeps its computers, phones, network devices and cloud services up to date so that known security flaws are closed quickly.

**1.2** Scope: laptops, desktops, servers, tablets, mobile phones, firewalls, routers, and every cloud service (IaaS, PaaS and SaaS) that staff use for company work, whether the company or a person owns the device. Personal devices that open company data are in scope.

**1.3** Software that the maker no longer supports is removed. Where it cannot be removed, the IT lead records why and when it will go.

## 2 Roles and responsibilities

**2.1** IT lead ([name], backup [name]): owns this policy and the monthly check. If an outside IT provider ([provider]) does the work, the IT lead is still accountable and keeps the provider's monthly written report.

**2.2** Every employee: installs prompted updates within [3] days and restarts when asked.

**2.3** Director ([name]): hears about any update that is more than 14 days late.

## 3 Asset inventory

**3.1** One spreadsheet or tool lists every device and cloud service, its owner, whether it updates itself, and the date of the last check.

**3.2** A new device is added on the day it is issued.

## 4 Severity and patch windows

| Update type | Window |
|---|---|
| Fixes a flaw the maker calls critical or high | 14 days from release |
| Listed as exploited in the CISA Known Exploited Vulnerabilities catalog | 3 days if the system is reachable from the internet, otherwise 14 days |
| Everything else | Next monthly cycle |

**4.1** Automatic updates are switched on wherever the product allows it. The IT lead checks every month, on the Wednesday after the second Tuesday, that nothing is waiting.

## 5 Testing and staging

**5.1** The IT lead's own device and one volunteer's device get updates first, then everyone else after [2] working days. Servers are updated outside working hours with a backup taken first.

## 6 Maintenance windows

**6.1** Servers and network devices: [day, time]. Laptops: restarts allowed any weekday before [time].

## 8 Reporting and metrics

**8.1** Monthly note to the director: devices checked, devices late, reason, date fixed.