# PATCH MANAGEMENT POLICY

Prodigy IT Solutions has a responsibility to ensure all its managed servers and devices are updated with critical / security patches, we are committed to ensuring the protection of all equipment covered under our managed services contract through the use of software updates, monitoring and routine maintenance.

## SCOPE

Devices covered under this policy:

All Windows servers (or devices defined as a 'server' under the terms of the Managed Services Contract)
Managed laptops and workstations with our Advanced RMM installed
Hardware where monitoring or managed services are in place (e.g. switches / routers / firewalls)

Please note Prodigy IT Solutions are not liable for any devices or software outside of this scope.

Updates covered under this policy:

Microsoft Windows updates
Hardware security or critical firmware updates
Third party software updates (where applicable)

Please note that managed patching of third party software only applies to customers with Cyber Essentials certification and only covers a limited set of applications.

## LAPTOP / WORKSTATION PATCHING PROFILE

Prodigy run a Laptop / Workstation patching profile which runs client updates on a weekly basis. Schedules for running these updates will be approved with your assigned engineer prior to deploying any updates. If you require any changes to this schedule, then notify your assigned engineer to discuss.

**Pop-Up messages**

Prior to your patch window commencing you will receive a pop-up message advising that patches are scheduled to be installed. This message will be displayed 2 hours prior to the patch window, if you dismiss the message you will be reminded every 30 minutes until patching commences, this pop up allows you the option to start the patching immediately or otherwise allows plenty of warning to save open documents. If your patch window is scheduled out of hours, then you will not see these messages however they still act as a useful reminder should you be working on your machine.

**Wake devices from Sleep and Hibernation states**

The patch management agent will automatically attempt to wake your device during the defined patch management window, if your device is powered down or the system is unable to wake the device then patches will be applied when it next becomes available.

## SERVER PATCHING PROFILE

Patches for servers are also installed on a weekly basis. All servers should be available and online during the approved maintenance window.

## SERVERS / LAPTOPS & WORKSTATIONS

### INSTALLATION FAILURES

If a patch fails to install within a predefined window after their release, Prodigy will receive notification and will take manual action to ensure that the patch installs.

### APPROVAL POLICY

#### SECURITY / CRITICAL UPDATES

As standard, all Security and Critical updates are approved after 3 days. We defer these updates by 3 days to allow for post release issues to be resolved. Once approved, patches will then become available for install during your next patch maintenance window.

Depending on when the patch was released this it can take between to 3 - 10 days to deploy to your device.

In the event of a high-profile vulnerability we would manually approve and deploy critical updates.

#### DEFINITION UPDATES

Microsoft definition updates are approved and deployed immediately for all affected devices, these include virus definitions and Office definitions which protect against the latest junk email and malicious links. These updates do not require interaction from the end user.

#### NON-CRITICAL UPDATES

Non-critical Microsoft updates are approved 14 days after release. These updates include general system updates which help to resolve non-critical or non-security related bugs. Prodigy does not hold itself accountable to deploy non-critical updates but makes best efforts to ensure all system are patched to a reasonable level.

#### FEATURE UPDATES

Feature updates are typically released on a semi-annual basis and upgrade the OS to a new version. Each version is only supported for a limited time and Microsoft will no longer release security updates for unsupported versions. As such, Prodigy will upgrade devices when required to ensure that they remain on a supported version.

Each feature update brings a lot of changes so in order to minimise issues, these updates may be delayed and will be approved manually. Prodigy will install and test feature updates internally before approving them for your systems when suitable.

#### THIRD PARTY SOFTWARE UPDATES

Prodigy are able to manage patches for a limited set of commonly used third party applications such as some web browsers and document readers. These patches are approved and deployed to devices where the customer is maintaining compliance with Cyber Essentials security standards.

### WHEN WILL MY SYSTEMS BE PATCHED?

Our standard patch window takes place between 02:00 – 04:00 GMT. As part of the on-boarding process, an engineer will discuss with you which day of the week is most suitable for these updates to take place.

In most cases once updates have been applied, that device will automatically be rebooted.

Where an automatic reboot is not appropriate, we instead raise a ticket notifying us that a reboot is required, an engineer will contact you to organise this at your convenience.

## MANAGED HARDWARE

On managed hardware such as networking equipment and storage, automated and scheduled updates are used if available. Where this is not possible, firmware upgrades are installed on a 6-monthly basis.

Common devices where automatic/scheduled updates are available:

- Unifi – Routers, switches and access points
- Meraki – Routers, switches and access points
- Synology NASs