Microsoft Patch Management

This document outlines the procedure within PAS for the assessment and deployment of Microsoft patches and updates.

Microsoft Patches

'Patch Tuesday' is the second Tuesday of each month, on which Microsoft regularly releases security patches. The Network manager is responsible for patching all Microsoft products within one month of the patch being released.

Patches should be tested and deployed based on the schedule below:

Severity Rating	Definition
Critical	Patch testing should begin immediately after released and deployed company-wide starting on Friday night and finished no later than Sunday morning
Important	Patch testing should begin no later than Friday after the patch has been released and deployed company-wide on the following Wednesday after 10:00pm.
Moderate	Patch testing should begin within two business weeks after the patch has been released and deployed company-wide on the following Wednesday after 10:00pm.
Low	Patch testing should begin within three business weeks after the patch has been released and deployed company-wide on the following Wednesday after 10:00pm.

Impact Durations

Any patches found with compatibility issues will need to be reviewed by both the Network Manager and the Technical Director before they can be exempt from being deployed.

If it is found that the risk is too high to exempt the patch, the Development team will need to plan to resolve the compatibility issue within one month of the initial findings.

A workaround may be implemented as long as it does not impact security compliance.

Hosted Server Patch Deployment

Deployment of patches to the hosted environment will, by default, only be applied during the planned maintenance windows and against the defined schedule. Should the Network Manager deem that a critical patch needs to be applied to the hosted environment outside of this schedule, this will be escalated to the Technical Director.