

PATCH MANAGEMENT POLICY

This document forms the University's *Patch Management Policy* which supports the *Information Security Policy*. It details requirements for maintaining up-to-date software version levels and operating system security patches on all University of Reading IT systems.

Compliance with this policy will help ensure that consistent controls are applied across the University to minimise exposure to 'known' vulnerabilities.

Where possible, all University of Reading IT systems shall be updated to the latest patch/security releases.

IT systems include:

- Computers
- Software (platforms, applications, databases etc.)
- Networks (switches, routers etc.)
- Servers (physical and virtual)

This policy applies to all IT systems at the University of Reading.

Patch centrally managed systems.

Record unpatched systems.

Remove/quarantine non-compliant systems as appropriate.

Responsible for routinely assessing compliance with the patching policy and providing guidance to all stakeholder groups in relation to issues of security and patch management.

