PATCH MANAGEMENT POLICY

1. Introduction

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.

2. Definitions

IT systems include:

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

3. Scope

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

4. Roles & Responsibilities

DTS	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.
Change Advisory Board	Responsible for approving out of band requests for patching e.g. emergency deployment requests.
End User	Responsible for adhering to policy and reporting any issues to the DTS Service Desk.

Information Security Group (ISG)	Record exceptions as per section 7.

5. Policy

5.1. All IT systems shall be manufacturer supported and have up-to-date and security patched operating systems and application software.

5.2. Security patches must be installed to protect assets from known vulnerabilities.

5.3. Patches rated 'Critical' by the vendor must be installed within 7 days of release from the operating system or application vendor unless prevented by University change control procedures.

5.4. Patches rated 'High' by the vendor must be installed within 14 days of release from the operating system or application vendor unless prevented by University change control procedures.

5.5. Patches rated 'Low' or 'Medium' by the vendor must be installed within 28 days of release from the vendor, unless mitigating controls are in place to prevent the exploit being realised, in which case it may be deferred to the nearest maintenance window.

5.6. A shorter timeframe may be mandated based on the assessed severity and potential/actual impact.

5.7. All servers shall comply with recommended minimum requirements (default operating system level, patching levels, service packs etc.) as specified by DTS. Exceptions shall be documented in the risk register and reported to the DTS Directorate.

5.8. Patching of systems will be centrally-managed wherever possible, unless there are clear business reasons for patching to be performed locally.

5.9. Users shall reboot their device/s when prompted to do so.

- Users may defer rebooting a device a maximum of two times (critical rated patches excepted) within the first 10 days of a patch being deployed by DTS, after which time it shall be automatically rebooted.

6. Monitoring and Reporting

Reporting metrics that summarise the outcome of each patching cycle shall be compiled and maintained by DTS. These shall be used to evaluate patching levels and assess current levels of risk.

7. Exceptions

There are some systems that cannot be patched. For example systems that are end of life or that require a precise version of software to operate. Exceptions must be risk assessed, have formal documented approval and be recorded by ISG. Compensating controls will be applied, as necessary, and may be considered as sufficient mitigation.

8. Non-Compliance

A device that poses an unacceptable level of risk may be disabled or removed from the production environment. They will only be reconnected once it is proven that they have been brought up to date and are secure.

9. Related policies, procedures, guidelines & regulations

- Information Security Policy.
- Vulnerability Management Policy
- Information Risk Management Policy

Policies superseded by this policy

Patch Management Policy v1.0

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
2.0	Policy re-written	DTS	Annually	DTS	TBD	TBD	TBD
2.1	Critical patches applied in 7 days (not 14). Now University wide policy . ISG to record exception (section 7). 5.9 added.	DTS	Biennially	ISG	Sep 20	TBD	TBD
2.2	"Must" replaces "shall" (*must be installed*) in 5.3, 5.4 & 5.5 following policy review at DAG and ISG meetings.	DTS	Biennially	University Policy Group	Nov 20	Nov 20	Nov 22

Appendix A - Microsoft Platforms

Patch Testing and Release

DTS begin testing Microsoft patches upon their release on the second Tuesday of every month (week 2). Patches are initially applied to an early release group consisting of a subset of staff laptops/desktops, lab PCs, and non-production servers (week 2). If no issues are discovered during this testing period, DTS shall approve the patches for release to non-production servers (week 3) and to production servers, staff laptops/desktops, and lab PCs (week 4).

If problems are discovered with the patches or there are reports from external sources, the impact will be risk assessed and a decision made to determine whether the release should be held back or rollbacked until the issues are resolved.

Patches shall be applied at scheduled maintenance times/windows (wherever possible) in order to avoid any potential impact on people and services using the infrastructure.

Deviations to Patch Release

When an exploit to a vulnerability is published prior to the deployment of a patch, a risk assessment will be carried out by DTS to determine whether it is necessary to apply the patch before it has been fully tested. Where the risk of system compromise is considered to be greater than the impact of deploying a partially tested patch, a decision will be taken to release the patch early.

Patches may be released early or held back during periods when the University is about to close or on a period of change freeze.

Appendix B – Non-Microsoft Platforms

Patching Information

Users responsible for the maintenance of desktops and servers that run non-Microsoft Operating Systems must ensure that those systems are set to frequently check for updates, and that they are running on a platform that is being supported by the vendor/community.

Classification, Testing and Deployment

Security patches that address vulnerabilities exploitable either remotely or without the use of a user account should be rated as critical and patched in a timely manner. Priority of patching critical vulnerabilities must always be given to systems that are available from off campus.

Where possible patches will be applied only at scheduled maintenance times, in order to avoid any potential impact on people and services using the infrastructure. Where vulnerabilities are found to apply to University infrastructure, advice may be sought from the University's third party suppliers to determine whether it is feasible to use a work-around solution to enable the patches to be applied according to the normal maintenance schedule. If advice and the outcomes of a risk assessment determine that the patch should be applied immediately, remedial action will be taken.