Digital Architecture | Digital Technology Services
Security Patching policy

Contents

Document control

Version number	Authors	Notes	Date
0.1	Dave Thornley	Draft	22/05/2017
0.2	Dave Thornley	Updated with changes from Infrastructure team review	02/06/2017
1.0	Dave Thornley	Policy finalised and released	08/06/2017
1.1	Dave Thornley	Policy updated following PSOM	11/01/2021

Security patching policy

1. Introduction

Sheffield Hallam University is responsible for ensuring the confidentiality, integrity, and availability its data and that of personal data stored on its systems. The University has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data stored on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

2. Purpose

This policy covers the deployment of security patches to Operating Systems and infrastructure applications such as web servers or databases used on managed University IT systems. It sets out why, how and when security patches will be deployed and how exceptions will be managed.

Patching is an essential process that provides a first line of defence against attacks. The deployment of patches causes some service disruption and risk and this policy aims to balance the risks and impact of patching with the need to keep up to date in an increasingly challenging technology environment.

This policy ensures that security patches and updates are applied across IT services to ensure the maximum protection from malware or attackers seeking to exploit known vulnerabilities in systems.

3. Scope

This policy applies to security updates that do not change the functionality of software or operating systems.

This policy covers the following IT equipment.

- Managed Desktop workstations on the University network
- Servers managed by DTS in University datacentres, cloud services or any other location.

This policy covers security patches released by manufacturers, primarily Microsoft, Red Hat, Adobe and Oracle however it should be applied to any security patches released for software in use in the University.

4. Policy

Managed equipment in the University will be operated so that

- Only versions of software that are actively supported by the manufacturer are in use.
- Appropriate security patches can be identified and deployed to all equipment within 1 month of release.
- Patching does not lead to unnecessary risks or downtime of IT systems and services.
- Availability of patches will be reviewed at least monthly to identify any requiring action.

5. Roles and Responsibilities

The policy roles and responsibilities are

- The Cloud, Networks and Infrastructure Team are responsible for patching Windows Server and managed Linux servers.
- The Security Team are responsible for patching Windows desktops and laptops.
- The Security Team are responsible for assessing routine compliance with this policy and providing guidance in the matters of security and patch management.
- CAB is responsible for approving monthly patch management change requests and for reviewing and approving Time-based variations to the policy (See Exceptions)

6. Monitoring and Reporting

Records of patch deployment and outcomes should be created and retained by the team deploying patches for use in any post deployment security incident investigation.

7. Exceptions

Exceptions to this policy must be agreed by the relevant authority below and documented. Risk reduction measures may be put in place where exceptions pose a risk to the operation of the University.

- Time-based exceptions, for example Change Restriction periods. These are approved by CAB with the agreement of the Security Team and will be documented in the CAB records.
- Device-based exceptions, for example where a device cannot be managed to the requirements of this policy. These are approved by the Security Team and recorded in the Security Risk Register.
- Patch-based exceptions
    - Where faster rollout is needed, for example a patch to a critical and actively exploited vulnerability. These are approved by CAB with the agreement of Security Team and documented in the CAB records.
    - Where delayed rollout is needed, for example a patch that causes problems in the University environment. These are approved by the Security Team and documented in the Security Risk Register.