UNIVERSITY of BRADFORD

Vulnerability Management and Patching Policy

IT Services

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

UNIVERSITY of BRADFORD

Contents:

UNIVERSITY of BRADFORD

1. Introduction

1.1 The University of Bradford is responsible for ensuring the confidentiality, integrity, and the availability of its data which requires the information technology infrastructure components (hardware, software, and services) to be kept up to date with the latest security patches and feature updates.

1.2 The functional execution of this policy will limit the exposure and the effect of cyber-security threats and add new features, thereby reducing security risk.

2. Scope

This policy applies to:

2.1 All Systems Administrators and technical support staff who are responsible for the development and maintenance of systems and services in the University.

Elements in scope:

2.2 All University managed IT systems including, but not limited to, servers, workstations, laptops, network devices, surveillance, and door entry and building management systems.

2.3 All software on these systems, including firmware, BIOS, hypervisor, operating systems, middleware, and applications.

2.4 All information systems and information resources owned or operated by, or on behalf of, the University.

3. Policy

3.1 System owners (with the support of IT Services) must establish and maintain documented procedures for vulnerability and patch management.

3.2 Security updates must be applied within agreed timeframes: Vulnerabilities on externally facing servers must be patched within 14 days from when a patch or remediation option is available.

3.3 Exceptions will be permitted based on risk assessments. Any exceptions for patching and upgrades must be documented and the risk accepted by the risk owner and reviewed after three months.

3.4 Systems must be regularly checked for updates (as per patching guidelines; see section 6) and scanned for vulnerabilities to confirm that the required updates are being applied as intended, and vulnerabilities are discovered and remediated.

3.5 Whenever any system or device is connected to the University network, it presents a serious risk to the infrastructure, information security and the reputation of the University. The IT Security team will immediately request the removal of a compromised system from the network to avoid potential compromise.

3.6 System and software vulnerabilities will be remediated using the appropriate vulnerability and patch management process.

3.7 Where updating or installing patches is not possible, a risk assessment must be carried out to determine whether an alternative mitigation measure can be put in place, or whether the risk is on an acceptable level. This will involve assessing the likelihood of the vulnerability being exploited and the resulting impact on the University. The system owner concerned must work with the IT Risk and Compliance Manager to assess the risk, while the IT Security team must advise what mitigations (if any) can reduce the risk to an acceptable level. The Vulnerability Remediation team will be responsible for the coordination of the implementation.

3.8 Vulnerabilities that cannot be mitigated to an acceptable level of risk must be promptly escalated to the IT Director or Associate IT Director for review. Under the guidance of the Security team, the risk must be accepted by the service owner and approved for exemption. This must be logged in the Risk Register and reviewed after three months.

3.9 If none of the above measures are feasible, the insecure system must be disconnected from the University's network until an alternative acceptable solution is provided.

4. Exceptions

4.1 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 the IT Security team to determine whether it is necessary to apply the patch before it has been fully tested. Where the risk of system compromise is greater than the impact of deploying of a partially tested patch, a decision may be taken to release the patch early.

4.2 Patches may be released early or held back during periods when the University is about to close or in a period of change embargo. Arrangements must be made to patch on a different schedule or for the systems to be manually patched. This must be approved by the IT Security team. The system owner will collaborate with the Vulnerability Remediation team on the schedule.

4.3 Any exceptions must be documented and reviewed on a three-month basis.

5. Enforcement

5.1 Non-compliance with this policy may result in disciplinary action, including termination of access to IT systems, and may be subject to further action in accordance with the University's disciplinary procedures.

6. Related policies and standards / documentation

6.1 End user device patching guidelines (applicable for and available to the IT Services team).

6.2 Windows Server Infrastructure patching guidelines (applicable for and available to the IT Services team).

7. Glossary

- **BIOS (Basic Input / Output System):** Firmware used to initialise and manage hardware components during the computer startup process.
- **Embargo period:** A predefined timeframe where changes to IT systems are restricted to avoid disruptions, such as during University examinations and Clearing.
- **Firmware:** Software embedded into hardware devices, such as routers or surveillance systems, that provides low-level control of hardware components.
- **Hypervisor:** A virtualisation layer allowing multiple operating systems to run on a single physical machine.
- **Middleware:** Software acting as a bridge between an operating system and applications, facilitating communication and data exchange.
- **Patch:** A software update designed to fix security vulnerabilities, bugs, or improve system functionality.
- **Patch Tuesday:** A monthly event (usually the second Tuesday) when major software vendors, such as Microsoft, release security patches.
- **Remediation:** Actions taken to resolve identified vulnerabilities or security risks, such as installing patches or implementing alternative measures.
- **Risk assessment:** A process of identifying, analysing, and evaluating risks to determine their potential impact and how they should be addressed.

- **Risk Register:** A documented repository of identified risks, their assessments, mitigation measures, and monitoring outcomes.
- **Security updates:** Software releases specifically designed to address vulnerabilities that could be exploited by attackers.
- **System vulnerability:** A weakness in an IT system, device, or software that could be exploited to compromise security or functionality.
- **Vulnerability scanning:** The automated process of identifying potential security weaknesses in IT systems.
- **Externally facing servers:** Servers that are accessible from outside the University network, such as web servers, which are more vulnerable to external threats.
- **Exception:** A documented and approved deviation from the standard policy requirements, subject to regular review.
- **IT Security:** The team responsible for protecting the University's information systems and infrastructure from cyber threats.
- **Mitigation:** Temporary or alternative measures taken to reduce the severity or impact of a security risk.
- **Endpoints:** User devices such as laptops, desktops, or mobile devices connected to the University's IT infrastructure.
- **Change embargo:** A freeze on system changes during critical operational periods to ensure stability and reliability.

8. Document and version control information:

Version control information heading	Details
Owner	IT Director
Author	IT Risk and Compliance Manager
Approved by	IT Director
Date of approval of this version	13 March 2025
Next review date	March 2027
Version number	V1.0
Applicable statutory, legal, or national best practice requirements	CE+, IS0 27001, NIST
Equality impact assessment completion date	Not applicable
Data protection impact assessment completion date	Not applicable