UNIVERSITY OF WINCHESTER

# Knowledge and Digital Services Patch Management Policy

| | |
|---|---|
| **Document Title:** | Knowledge and Digital Services Patch Management Policy |
| **Responsible Role and Department:** | Director of KDS<br>Knowledge & Digital Services |
| **Approving Body:** | Executive Leadership Team (ELT) |
| **Date of Approval:** | 07 January 2025 |
| **Date Effective From:** | 07 January 2025 |
| **Review Date:** | 01 January 2028 |
| **Indicate whether the document is for public access or internal access only.**<br>**Indicate whether the document applies to collaborative provision?**<br>*(Strikethrough text, as appropriate)* | **Public Access**<br>~~**Internal Access Only**~~<br>~~**Applies to Collaborative Provision**~~ |

**Summary:**

This policy details how the university will ensure that any digital devices or services are patched and updated to ensure the best possible cyber security stance.

TABLE OF CONTENTS

# 1. Introduction

1.1. This policy applies to systems, services, and devices, and does not apply to people.

1.2. The purpose of this document is to outline the requirements for all security and vulnerability patch management that will take place across the University's IT infrastructure. All security patching is required to follow this policy, where possible; in such cases where this is not possible, policy exceptions will be issued on a case-by-case basis by the IT Change Group via Chairs Action, or by the Director of Knowledge and Digital Services where larger disruption or risk is identified.

1.3. The University of Winchester has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems, including systems and services provided by third parties but managed by the University of Winchester, or operated and managed by third parties.

1.4. The University has an obligation to provide suitable protection of all its IT estate; whether physical, virtual, on-premises, or in the cloud.

# 2. Scope

2.1. All IT systems owned and operated by the University of Winchester.

2.2. All IT systems used by the University of Winchester but managed by third parties.

2.3. Any device which is used to access business data (e.g., Microsoft 365) as well as the University's infrastructure will be deemed 'in-scope'. This includes any personal devices that are used across the University (see our 'Bring Your Own Device' policy for more details).

2.4. IT systems refer to:

2.4.1. End User Devices (e.g., laptops, desktops, tablets, mobile phones, etc.)

2.4.2. Servers (physical, virtual, and cloud-based)

2.4.3. Operating Systems (both Microsoft and non-Microsoft)

2.4.4. Network Equipment (e.g., Firewalls, Switches, Routers, Access Points, etc.)

2.4.5. Hardware (e.g., VR Headsets, Hardware Appliances, CCTV, IoT, EPOS, Chip & Pin, etc.)

2.4.6. Software (including dependencies, e.g., Apache Tomcat, Java, etc.)

2.4.7. Firmware in any physical or virtual hardware device, or subcomponent thereof

2.5. This policy also includes any future device, software or service that the University is responsible for.

# 3. Responsibilities

3.1. The Director of KDS is accountable for ensuring that all software update and patching policies are adhered to.

3.2. The Head of Digital Services is accountable for ensuring that all software deemed 'in-scope' is kept up-to-date and suitably maintained through regular software updates and patching.

3.3. System owners are accountable for ensuring that all software and hardware that they manage which is in-scope is maintained through regular software updates and patching.

This may require support from Knowledge & Digital Services, or any third party vendors they own the contract for.

3.4. The University's KDS Digital Services teams are accountable for ensuring that all in-scope software they manage is maintained through regular software updates and patching. This may be delegated to other KDS teams, where appropriate.

3.5. The University's Digital Services teams are accountable for routinely assessing compliance with the patch management policy and will provide guidance to all relevant stakeholders in relation to any identified issues of security and/or patch management.

3.6. Third-party suppliers are accountable for ensuring that all software they provide and manage is maintained through regular software updates and patching, before, during, and after their operational deployment.

3.6.1. In this event, a named contact from the third-party must be provided alongside the data owner from the relevant team to ensure compliance with the patch management policy is met.

3.6.2. This also includes any cloud services whereby university data may be retained for a period after the university ceases to use the service.

3.7. Should any software/service provided by a third-party supplier use common underlying software libraries (e.g., Java or Apache Tomcat), they must ensure that the software is compatible with any minor releases without re-certification and must certify compatibility with new major releases at least 60 days before the previous version reaches end-of-life.

3.8. In the event that a third-party supplied software, service or device is scheduled to become 'end-of-life', the third-party supplier must ensure that the University is notified a minimum of 90 days before the end-of-life date.

3.9. In the event that a third-party supplier is changing their underlying infrastructure or hosting of a service or system, the third-party supplier must ensure that the University is notified a minimum of 90 days before the change takes place.

3.10. Third-party suppliers must agree to this policy as part of the purchase process.

3.11. End users are accountable for adhering to this policy and reporting any issues to the KDS Service Desk.

# 4. Software Updates & Patching

4.1. All IT systems (as defined in Section 2), including those being developed and supported by third parties, must be licensed appropriately, supported by the manufacturer, and be running patched and up-to-date operating systems and/or application software (excluding those with a policy exception, see Section 5 below).

4.2. If necessary, a consistent maintenance window should be established to ensure routine patching and maintenance can occur without impacting business continuity. This should be determined by the data owner, data maintainer and, if required, IT Governance.

4.3. Any IT system that is no longer appropriately licensed or supported by the manufacturer will be removed from the network (excluding those with a policy exception, see Section 5 below).

4.4. Routine and/or standard operating system, hardware or software updates should be completed within a standard Service Level Agreement (SLA) period of 14 days after their release.

4.5. To protect the University's IT systems, any known vulnerabilities should be remediated and patched in a suitable time frame. Patches should be deployed based on the following classifications:

4.5.1. If the update/patch is to resolve a critical or high severity vulnerability, it must be patched within 7 days.

4.5.2. If the vendor does not specify the severity level of the vulnerability or vulnerabilities being patched, it must be patched within 14 days.

4.5.3. If the vendor specifies a CVSSv3 score of 7 or higher for a vulnerability being patched, it must be patched within 14 days.

4.6. In the event that a patch cannot be deployed within the above patch windows, or there is no available patch for a vulnerability, then emergency mitigations should be applied where possible.

4.7. Third-party suppliers must be willing to provide evidence of suitable patch management policy and capabilty before IT systems are deployed to the University network and brought into operation.

4.7.1. Evidence that the above has been provided, implemented (if not by UoW) and complied with, must be provided whenever there is a renewal related to the system, software or device

4.7.2. Additionally, the same evidence must be provided to the university within five working days of being requested at any time during the life of the system, software or device.

4.8. Any new systems being brought into operation must be patched to the currently agreed baseline to ensure risk to the University network has been minimized.

# 5. Policy Exceptions

5.1. In the event that this policy cannot be followed, a policy exception must be put in place and recorded.

5.2. The following information must be collected as part of this exception:

5.2.1. The risk if this asset is not patched within the standard Service Level Agreement (SLA).

5.2.2. Whether the risk has been recorded as part of a risk register.

5.2.3. What additional mitigations can be put in place to reduce risk.

5.2.4. Any alternative systems/software that could be used instead of this asset.

5.3. Policy exceptions are not to be open-ended, and must be reviewed every three months, and at worst annually.

5.3.1. By reviewing the policy exceptions frequently, the risk can be re-evaluated, and additional mitigations can be discussed, if necessary.

5.4. These exceptions should be acknowledged and signed-off on by the data owner, maintainer (where possible) and a senior member of the department (such as the Head of Digital Services or Director of Knowledge and Digital Services).

5.4.1. Following this, approval must be given from IT Governance.

# 6. Communications around patching

6.1. Knowledge & Digital Services will communicate when standard "patch wondows" are going to be used.

6.2. Knowledge & Digital Services will be responsible for ensuring communication to all potentially impacted customers should an emergency or critical patch is planned.

6.3. Knowledge & Digital Services will communicate and work with any local designated "system managers" where a patch is needed to support a tool or system.

# 7. Non-Compliance

7.1. Any asset that poses an unacceptable risk to the university may be isolated, disabled or removed from the network. Where this involves a solution with a local system owner this will be communicated and planned with said system owner. Where there is a conflict between system owner and this policy, and Knowledge & Digital Services are unable to progress the Chief Operating Officer will be approached to determine action.

7.2. Once evidence is provided that the asset in question has been brought up to date and appropriately secured, it can then be reconnected or re-deployed to the network.