Patch Management Policy

Version 2.0

Version:	**2.0**
Dated:	**22 September 2020**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	4/9/17	P. Jones	Creation of document
0.2	27/9/17	T. Dyhouse	QA of V0.1 addition of CAB measures
0.3	Oct 2017	P. Jones	Updates from CGR and split into two documents.
1.0	May 2018	Ali Mitchell	Format and added in Third Party Suppliers
1.1	November 2019	Ali Mitchell	New template. Amended list of IT components at 3.1. Formatting and added in references to risk registers and non-compliance. Workstations at para 3.1 changed to end user devices.
1.2	January 2020	Ali Mitchell	Added in Martyn Brake to review distribution
1.3	June 2020	Ali Mitchell	Added in Martyn Goldsborough to review distribution
1.4	29/7/20	Ali Mitchell	Amended 4.1 research para, 5.1 and 5.2. Added in paragraph on associated policies

Review Distribution

Name	Title
Mike Maling	Operations and Security Manager
Ira Goel	IT Risk and Compliance Manager
Martyn Goldsborough	Information Security Manager
Simon Hallett	Security Architect
Brenda Waterman	Information Governance Manager and DPO
Dave Bunting	Service Performance Manager
Martyn Brake	Research IT Manager

Approval

Version	Position	Signature	Date
1	Members of the Information Governance and Security Steering Group (IGSSG)	Various	May 2018
2	Chief Information and Digital Officer	Via Teams & Email	Sept 2020

Contents

1. Introduction

1.1 The University of Exeter has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties.

1.2 The university has an obligation to provide appropriate and adequate protection of the entire IT estate whether it is an IT system on premise, in the Cloud or systems and services supplied by third parties.

1.3 Effective implementation of this policy reduces the likelihood of compromise which may come from a malicious threat actor or threat source.

2. Purpose

2.1 This document describes the requirements for maintaining up-to-date operating system patching, security patches and software version levels on all the University of Exeter owned IT estate and services supplied by third parties.

3. Definitions

3.1 The term IT systems includes:

- End user devices (laptops, workstations, iPads, PDAs, tablets and mobile phones)
- Servers (physical and virtual)
- Networking equipment (LAN, WAN, Wi-Fi, switches, firewalls, routers etc.)
- Hardware
- All Software (applications, databases, platforms etc.)
- Cloud Services

4. Scope

4.1 This policy is applicable to all UoE employees, and is mandatory reading for all staff responsible for information security within the University (e.g. security officers, security administrators, security auditors, systems administrators, researchers etc.); it should be understood and used by them as necessary to perform their duties.

- Workstations, laptops, mobile phones, PDAs, iPads, tablets, servers, networks, hardware devices, software and applications owned by the University of Exeter. This includes third parties supporting University of Exeter IT systems
- Systems that contain company or customer data owned or managed by Exeter IT regardless of location. Again, this includes third party suppliers
- CCTV systems where recordings are backed up to the University's networks
- Point of payment terminals using University of Exeter's networks
- Third party suppliers of IT systems as defined in Section 3
- Research devices and technologies – compliance to this policy as much as possible. However, depending on the specific nature of the devices and technologies used for research it is recognised that there will need to be some exceptions. These exceptions

will be assessed by the IT Security and Compliance team on a case by case basis, and where compliance is not possible, these will be recorded as risks and managed in accordance with the IT Risk Management process.

5. Policy

5.1 University controls:

- All IT systems (as defined in section 3), either owned by the University of Exeter or those in the process of being developed and supported by third parties, must be manufacturer supported and have up-to-date and security patched operating systems and application software
- Security patches must be installed to protect the assets from known vulnerabilities
- Any patches categorised as 'Critical' or 'High risk' by the vendor must be installed within 14 days of release from the operating system or application vendor unless prevented by University IT Change Control (CAB – Change Advisory Board) procedures
- Medium rated vulnerabilities must be patched within 21 calendar days and low 28 calendar days
- Where CAB procedures prevent the installation of 'Critical' or 'High risk' security patches within 14 days a temporary means of mitigation must be applied to reduce the risk and also noted in the IT Operations and Security risk register
    - End user devices
        - All equipment as detailed in paragraph 3.1 that are supplied by the University or by a third party for University business must meet the Centre for Internet Security Level 1 standards https://www.cisecurity.org/cis-benchmarks/ for build and setup.
    - Servers
        - Servers must comply with the recommended minimum requirements that are specified by Exeter IT Design team which includes the default operating system level, service packs, hotfixes and patching levels
- Research devices and technologies must conform to the patching regimes as stated above unless specific information security standards (e.g. DSPT, ISO27001 or regulatory controls) stipulates different requirements. Where there are different regulatory requirements these must be raised with the IT Design team via itsecurityandcompliance@exeter.ac.uk

5.1.1 Any exceptions must be raised with the Exeter IT Head of IT Security and Compliance by emailing itsecurityandcompliance@exeter.ac.uk

5.2 Third Party Suppliers

5.2.1 Security patches must be up to date for IT systems which are being designed and delivered by third party suppliers prior to going live. Third party suppliers must apply patches as stipulated in 5.2.2 below and be prepared to provide evidence of up-to-date patching before IT systems are accepted into service and thus become operational. All contracts placed with third party suppliers for equipment as specified in paragraph 3.1 must have patching regimes included and appropriate Service Level Agreements.

5.2.2 Once the IT systems are operational the following timescales apply:

- Critical or High-Risk vulnerabilities – 14 calendar days
- Medium – 21 calendar days
- Low – 28 calendar days

5.2.3 Any exceptions to this policy must be reported to the IT Security and Compliance team by emailing itsecurityandcompliance@exeter.ac.uk

6 Roles and Responsibilities

6.1 Exeter IT

6.1.1 Enterprise Device Management team

- Will manage the patching needs for the Windows estate that are using and connected to the University of Exeter domains

6.1.2 Operations team

- Will operate and manage the University's Change Advisory Board (CAB) which is responsible for approving all patch management deployment requests

6.1.3 IT Security and Compliance team

- Will ensure any non-compliance with this policy is documented in the Exeter IT risk register
- Are responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management

6.1.4 Exeter IT end users

- Must also conform to the requirements stipulated in section 6.2 below.

6.2 End Users

- Will be responsible for ensuring patches are installed on all devices as stipulated in para 3.1 above, regardless of which operating systems are in use (e.g. Apple MAC, Linux, Android and Apple IOS. This includes any non-domain devices and users must ensure these are rebooted when required. Any problems must be reported to Exeter IT via the Student Information Desk (SID)

6.3 Third Party Suppliers

- Will ensure security patches are up-to-date for IT systems which are being designed and delivered prior to going operational
- Once the IT systems are operational third party suppliers must ensure vulnerability patching is carried out as stipulated in section 5.2. Where this is not possible, it must be escalated to the University's Head of IT Security and Compliance by emailing itsecurityandcompliance@exeter.ac.uk

7. Monitoring and Reporting

7.1 Those with patching roles as detailed in paragraph 6.1 and 6.3 above and any end users who use and connect to any devices that are not connected to the University domain must compile and maintain reporting metrics that summarise the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current levels of risk. These reports must be made available to the IT Security and Compliance, Operations and Security teams and Internal Audit function upon request.

8. Supporting Policies

8.1 This policy should be read in conjunction with other associate policies such as:

- Anti-malware
- Bring Your Own Device
- Information Security for Portable and Removable Media Devices
- Remote Access
- Firewalls
- Encryption
- Secure by Design Process

9. Policy Review and Maintenance

9.1 This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

10. Help and Advice

10.1 To log non-conformance with this policy or for any other questions, please contact the IT Security and Compliance team itsecurityandcompliance@exeter.ac.uk