Corporate Ref.	FEIT 006
Level	Tier 3
Senior Responsible Officer	Chief Operating Officer
Version	2
EIA	N/A
Approved by	SMT
Approved date	15/10/2020
Superseded version	1
Review date	15/12/2024

Edinburgh College

Patch Management Policy

Version Control

Version	Author	Date	Changes
3.2	Digital Infrastructure Service Lead	24/10/2023	Rebranded to new template with minor updates

1. INTRODUCTION

Edinburgh College 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.

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

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

2. PURPOSE

This document describes the requirements for maintaining up-to-date operating system security patches and software version levels on all the Edinburgh College owned IT estate and services supplied by third parties.

3. DEFINITIONS

The term IT systems includes:

- Workstations
- Servers (physical and virtual)
- Firmware
- Networks (including hardwired, Wi-Fi, switches, routers etc.)
- Hardware
- Software (databases, platforms etc.)
- Applications (including mobile apps)
- Cloud Services

4. SCOPE

This policy applies to:

- Workstations, servers, networks, hardware devices, software and applications owned by Edinburgh College and managed by Edinburgh College. This includes third parties supporting Edinburgh College IT systems.

- Systems that contain company or customer data owned or managed by Edinburgh College regardless of location. Again, this includes third party suppliers.
- CCTV systems where recordings are backed up to the College's networks.
- Point of payment terminals using Edinburgh College's networks.
- Third party suppliers of IT systems as defined in Section 3.

5. POLICY

College controls

All IT systems (as defined in section 3), either owned by Edinburgh College 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, and a log retained.

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 College procedures.

Where College procedures prevent the installation of 'Critical' or 'High risk' security patches within 14 days a temporary means of mitigation will be applied to reduce the risk.

Workstations

All desktops and laptops that are managed by Edinburgh College must meet the manufacturers' laptop and workstation build requirements in build and setup. Any exceptions shall be documented and reported to the Edinburgh College Directors/Assistant Principals or Chief Operating Officer.

Servers

Servers must comply with the recommended minimum requirements that are specified by Edinburgh College which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to the Chief Operating Officer.

Third Party Suppliers

Security patches must be up-to-date for IT systems which are being designed and delivered by third party suppliers prior to going operational. Third party suppliers must be prepared to provide evidence of up-to-date patching before IT systems are accepted into service and thus become operational.

Once the IT Systems are operational the following patching timescales apply:

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

6. ROLES AND RESPONSIBILITIES

Edinburgh College IT Team

The IT team will manage the patching requirements for the Windows, Apple Mac OS and any other estate that is connected to the Edinburgh College domain.

They 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, with logs being made available on request.

End User

The end user has a responsibility to ensure that patches are installed and the machine is rebooted when required. Any problems must be reported to the IT team.

Third Party Suppliers

Will ensure security patches must be up-to-date for IT systems which are being designed and delivered by third party suppliers 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 – Policy. Where this is not possible, this must be escalated to the Chief Operating Officer.

7. MONITORING AND REPORTING

Those with patching roles as detailed in Section 5 above are required to 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 level of risk. These reports shall be made available to Internal Audit upon request.

8. POLICY REVIEW AND MAINTENANCE

The policy will be reviewed and updated every year, or as required to ensure that the policy remains aligned with changes to relevant laws, contractual obligations and best practice.

9. FOR ADVICE

IT - itrequest@edinburghcollege.ac.uk
0131 297 9090