RICHMOND, THE AMERICAN INTERNATIONAL UNIVERSITY IN LONDON, INC.

Patching Policy

Version 1.2 – March 2023

_____

Purpose

This policy is designed to protect Richmond University data through rigorous updating of the University server and workstation and mobile phone estate. Updates to both are considered patching, where a new version of the operating system or software products are installed.

Scope

This policy applies to all servers, workstations and mobile phones which are maintained by the IT Team.
Personal devices are covered by the Bring Your Own Device Policy.

Workstation patching

Workstations in offices, communal areas and classrooms, are set to auto update as defined and pushed down by Microsoft Windows Update Server. The WSUS server is configured to automatically approve security and critical patches. Any required Critical Or security updates will automatically install on Saturdays.

Server patching

Servers are configured to automatically download and install updated. Installation of updates will occur between Wednesday and Saturday depending on their group membership. Currently, Critical and Security update are set to be approved automatically on WSUS server, once they are available from Microsoft.

Laptop patching

Users with laptop devices that are mobile and might work remotely will still receive updates from the onsite WSUS server if they are onsite. This will also be available remotely whilst they are connected to the university local network using VPN. If the device is unable to communicate with WSUS server, the laptops are configured to check for updates directly from Microsoft Update Store.
Fixed laptops such as instructor's laptop in classrooms or laptops in meeting rooms, are configured to check and install updates on a weekly basis.

Apple iMac patching

Apple iMac devices automatically check for updates, including security and critical updates, on a weekly basis. All iMac devices have configured to install updates released by Apple as soon as they are available.

Policy

Microsoft release new patches for currently supported operating systems (OS) on a weekly basis – every Tuesday. The patching schedule for live servers is at 3 AM between Wednesday and Saturday.

- All information assets, either owned by the University 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. Our current SOC security software (XDR) would generally flag and protect the University from any such threats.
- 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 the IT procedures.
- Where IT 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. (SOC)
- Workstations - All desktops and laptops that are managed by the University must meet minimum security requirements in build and setup. Any exceptions shall be documented and reported to the IT Team.
- Servers - Servers must comply with the recommended minimum requirements that are specified by the University IT Team which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to the IT Team.
- Mobile Phones – New versions of the core operating system must be applied as recommended by the asset vendor. This extends to applications installed on the mobile phone, updates should be applied as suggested by the application vendor.

Third Parties

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

Failure to Comply

Incompetence, misconduct and/or performance issues will be addressed through standard HR policies.

Revision History

Version	Change	Author	Date of Change
1.0	Initial version	Paul Saunders	01-04-21
1.1	Changes under policy section	Nevena Khediri	21-02-22
1.2	Updates to reflect set-up in Chiswick and expansion of IT estate	Ibraheem Abdul-Razzaq	27-03-23