St George's, University of London
Patch Management Policy

1. Introduction

1.1 The University 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 all IT estate whether it is IT systems 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 security patches and software version levels on all SGUL owned devices and services supplied by third parties.

2.2 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

3. Scope

3.1 This policy applies to:

- Workstations, servers, networks, hardware devices, software and applications owned by SGUL and managed by SGUL IT. This includes third parties supporting SGUL IT systems.
- Systems that contain company or customer data owned or managed by SGUL 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 SGUL's networks.
- Third party suppliers of IT systems

4. Policy

4.1 University controls

- All IT systems either owned by SGUL 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.
- Where CAB 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 SGUL IT must meet the Laptop and Workstation Build Policy minimum requirements in build and setup. Any exceptions shall be documented and reported to SGUL IT Head of IT.

    - Servers

        - Servers must comply with the recommended minimum requirements that are specified by SGUL IT which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to SGUL Head of IT

- 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 SGUL Head of IT

4.2 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 much 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

4.3 Roles and Responsibilities

- SGUL IT

    - Will manage the patching needs for the Windows and Linux estate that is connected to SGUL domain.
    - Will manage the patching needs for Network devices, including firewalls, routers and switches
    - Will manage the patching needs for VoIP infrastructure
    - 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.
    - Shall run scheduled patch scans and reports.

- Change Advisory Board.

    - Responsible for approving the monthly and emergency patch management deployment requests.
- End User.

    - The end user has a responsibility to ensure that patches are installed when requested on the desktop, and the machine is rebooted when required. Any problems must be reported to SGUL IT.

- 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 “Policy”. Where this is not possible, this must be escalated to the Head of IT.

5. Monitoring and Reporting

5.1 Those with patching roles as 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.

5.2 The Policy will be reviewed and updated to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

For advice
Please contact either the Head of IT. Queries can be emailed to itav@sgul.ac.uk