Algospark Security Patch Policy

Version: 0.03
Last updated: 15 November 2023
By Darren Wilkinson

Purpose
This document describes the requirements for maintaining up-to-date operating system security patches and software version levels.

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

Scope
This policy applies to: workstations, servers, networks, hardware devices, software and applications owned and managed by Algospark. This includes third parties supporting Algospark IT systems.

- Systems that contain company or customer data owned or managed by Algospark.
- CCTV systems where recordings are backed up to the University's networks.
- Third party suppliers of IT systems.

Patch Management Policy

- All IT systems, either owned by Algospark 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.
- All desktops and laptops that are managed by Algospark must meet the Laptop and Workstation Build Policy minimum requirements in build and setup. Any exceptions shall be documented and reported to the Data Protection Officer.
- Servers must comply with the recommended minimum requirements that are specified by Data Protection Officer which includes the default operating system level, service packs, hotfixes and patching levels. Any exceptions shall be documented and reported to the Data Protection Officer.
- 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

Roles and Responsibilities

- Algospark IT will manage the patching needs for the Windows, Apple Mac OS and Linux estate. 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.
    - Approving the monthly and emergency patch management deployment requests.
- End User: responsibility to ensure that patches are installed and the machine is rebooted when required. Any problems must be reported to Algospark 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. Where this is not possible, this must be escalated to the Data Protection Officer.

Monitoring and Reporting
Those with patching roles 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 the Data Protection Officer on request.

Policy Review and Maintenance
The 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.