An Daras Multi Academy Trust

Information Security

Patch Management Policy

The An Daras Multi Academy Trust (ADMAT) Company
An Exempt Charity Limited by Guarantee
Company Number/08156955

Status: **Approved**	
Recommended	
Statutory	Yes
Version	v1.0
Adopted v1.0	**July 2022**
Reviewed/Approved	**25 June 2025**
Next Review	**June 2026**
Advisory Committee	Audit
Linked Documents and Policies	Cyber Security Essentials Accreditation Other ADMAT Cyber/IT/Information Security Policies

1. Purpose

An Daras Trust has a responsibility for ensuring the security requirements of its information assets are met. As defined in its information security policy, these requirements include confidentiality, integrity and availability. Malware that exploits software vulnerabilities presents the risk of breaching security requirements. Processes defined in this policy will reduce the risk of software vulnerabilities being exploited by malware threats. This internal policy applies to all physical and software assets listed in the Trust's information asset register.

2. Responsibilities

All employees with direct access to the Trust information technology systems are expected to conform to this policy.

An Daras Trust's IT service provider - currently ICT4 - are responsible for providing support in complying with this policy.

The Trust Operations Officer is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

3. Workstations

An Daras ensures that all its workstations are running an operating system that is actively supported by the vendor according to its development life cycle. Workstations running retired or legacy operating systems are removed from service as soon as possible. Automatic updates are enabled for all workstations' operating system, updating at the default frequency defined by the vendor.

4. Patching Schedule

An Daras aims to install all security patches within 14 days of release and aims to install patches not related to security within 90 days.

5. Problematic Patches

An Daras Trust's IT service provider - currently ICT4 - will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.

6. Software Licensing

An Daras Trust does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms.

7. Legacy Software

An Daras takes all reasonable measures to ensure that the software it uses is supported by its vendor. There may be occasions where no alternative software is available; in this case the software must be approved by our current IT Service provider and marked as unsupported in the Trust information asset register.

8. Monitoring and Internal Audit

An Daras in co-ordination with its current IT Service provider conducts annual vulnerability scans to ensure compliance with this policy.