Title:	Software Management Policy
Version:	1.1
Date:	December 2024
Reviewed:	December 2024
To be reviewed:	December 2025
Classification:	Public

1. Introduction

This Software Management Policy is a sub-policy of the Information Security Policy and sets out the principles and expectations for the security aspects of managing software by DMT staff and end users where relevant.

2. Definitions

Software management: any procurement, development, installation, regulation, maintenance or removal of software that takes place on computers owned by, managed by or for the DMT.

Computers: includes all end user computing devices, including tablets and smartphones, as well as servers, whether or not they are in a designated DMT place of work.

3. General software management principles

All software, including operating systems and applications must be actively managed.

There must be an identifiable individual taking current responsibility for every item of software formally deployed. Individuals installing software themselves are responsible for that installation. Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

Staff are responsible for ensuring the on-going security of their software and must ensure that security patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities).

4. Software procurement

When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls. These could include manual controls required during operation.

When software for use by the DMT is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.

It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

5. Software installation

Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage.

Automated installs should be used wherever possible - in line with current procedures.

Media / files must be stored securely and managed.

Individual users installing software on their own computers do so at their own risk.

Change control procedures must be followed and proper records maintained.

6. Software regulation

Use or installation of unlicensed software and using software for illegal activities could be construed to be a disciplinary offence.

Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.

7. Software maintenance

Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible - commensurate with the risk. High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk.

Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their DMT network connectivity withdrawn.

8. Software removal

Software that is not licence compliant must be brought into compliance promptly or uninstalled. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service. Change control processes and procedures must be used, commensurate with the risk.

When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence.