NetGain
systems

No of Pages	**1** of **5**
Document Classification:	Internal
Effective Date	1 Aug 2025
Doc No	ISMS-TECH-07
Revision	1.0

SOFTWARE INSTALLATION AND PATCH MANAGEMENT

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This procedure sets out the measures to be implemented to securely manage software installation on operational systems to ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

This procedure also sets out the rules governing the installation of software by users.

SCOPE

This control applies to installation of software on operational systems and software installation by users on their company-issued devices.

REFERENCE

ISO/IEC 27001 Standard	Annex A 8.19 Installation of software on operational systems

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

MR/IT shall ensure that this control is followed.

PROCEDURE

1. Installation of Operational Software

The MR shall ensure the following for operational software to be used within the organization:

- Licensing requirements are addressed
- The software works effectively
- Use of the software can be supported
- A record is kept of installed software

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release. Software patches should be applied when they can help to remove or reduce vulnerabilities. The organisation shall securely manage changes and installation of software on operational systems following the guidelines below:

- Ensuring that only approved executable code and no development code or compilers is installed on operational systems.

- Only installing and updating software after extensive and successful verification or testing, if applicable.
- Updating all corresponding program source libraries.
- Maintaining an audit log of all updates to operational software.
- Archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. For any open-source software used in operational systems, it should be maintained to the latest appropriate release of the software.

All installed software programs will be registered in the name of the organisation. In the event that a software program is no longer required, the software will then be removed and where necessary, the license will be re-used elsewhere within the organization.

2. Installation of Software by Users

Users must not install any unauthorized software in company-issued devices, whether or not it is free, shareware or commercial. This includes evaluation versions of software programs. Standard users will not have administrative rights by default. Compliance checks to analyse the software installed in the company-issued equipment will be carried out by IT as part of the yearly asset audit, and unlicensed / unauthorized software found in company-issued user devices will be deleted.

3. Patch Management

Only supported hardware, software, and vendor tools are to be used within the organization's operational environment. All systems and components under the organization's control must be regularly updated with applicable security patches to mitigate known vulnerabilities.

Systems covered include:

- Cloud infrastructure
- SaaS platforms and observability/security tools
- Custom-developed applications and CI/CD tools
- Endpoints issued by the organization (e.g., laptops) have automatic security updates enabled

An up-to-date inventory of software, systems, and cloud components shall be maintained to facilitate accurate vulnerability assessment and patch deployment. Patch applicability shall be determined through:

- Continuous monitoring of official vendor security bulletins, advisories, and mailing lists
- Review of alerts from threat intelligence feeds, clients, and security communities
- Evaluation of patch relevance based on system presence and exposure
- Testing of patches in non-production environments prior to deployment, where feasible

All security patches shall be deployed according to the timelines stipulated below:

Type	**Description**	**Timeline**
Critical	Patches addressing high-impact security vulnerabilities that could lead to data breaches, unauthorized access, or service compromise	Within 24 hours
Non-critical	Patches related to functional improvements, bug fixes, or performance enhancements not involving security flaws	Within 4 weeks

For cloud-managed infrastructure (e.g., PaaS, IaaS, or virtual machines), the organization shall:

- Enable and monitor cloud provider patching services
- Maintain responsibility for OS-level and application-level patching unless explicitly managed by the provider
- Apply IaC (Infrastructure-as-Code) practices to ensure patched base images are used when provisioning infrastructure