	No of Pages	1 of 4
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CONFIGURATION MANAGEMENT	Doc No	ISMS-TECH-04
	Revision	1.0

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



	No of Pages	2 of 4
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CONFIGURATION MANAGEMENT	Doc No	ISMS-TECH-04
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE.....	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES.....	3
PROCEDURE.....	3
A. STANDARD TEMPLATES	3
B. CONFIGURATION MANAGEMENT AND CHANGE CONTROL.....	4
C. MONITORING AND REVIEW OF CONFIGURATIONS.....	4

	No of Pages	3 of 4
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CONFIGURATION MANAGEMENT	Doc No	ISMS-TECH-04
	Revision	1.0

PURPOSE

This document describes the main principles on which standard configurations must be based and sets out the rules for their use, to ensure hardware, software, and services function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

SCOPE

This control applies to configurations (including security configurations) of hardware, software and services (e.g., cloud services).

As the company operates in a shared office space, configuration of shared infrastructure (e.g., office network, firewalls, switches, access points) is outside the company's control and is excluded from this procedure. Configuration responsibilities are limited to internally managed assets and cloud-based systems.

REFERENCE

ISO/IEC 27001 Standard Annex A 8.9 Configuration management

RESPONSIBILITIES & AUTHORITIES

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


The MR/IT shall enforce the defined and approved configurations for hardware, software, and services, for newly installed systems as well as for operational systems over their lifetime.

PROCEDURE

A. Standard Templates

The organization shall ensure all internally managed ICT component, including cloud resources, software applications, and endpoint devices, are securely configured prior to deployment and during their lifecycle. Key guidelines include:

- All configurations must be defined, reviewed, and documented using standard templates or infrastructure-as-code (IaC) where applicable.
- Where available, configurations must align with:
 - Vendor security hardening guides
 - Guidance from reputable cybersecurity authorities (e.g., CIS, NIST)
 - The organization's own security policies
 - Security requirements from client contracts or applicable regulations

	No of Pages	4 of 4
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CONFIGURATION MANAGEMENT	Doc No	ISMS-TECH-04
	Revision	1.0

Configuration templates must consider:

- Minimising privileged or administrator access
- Disabling unused/default/test accounts
- Removing or disabling unused services, ports, and components
- Changing default credentials immediately after deployment
- Enabling timeouts for inactive sessions
- Ensuring time synchronization (e.g., NTP) in cloud or VM instances
- Configuring service accounts as non-interactive
- Verifying license compliance where applicable

B. Configuration Management and Change Control

All system and software configurations must be:

- Recorded using approved documentation or tooling (e.g., version control, cloud configuration systems)
- Linked to asset owners or responsible personnel
- Version-controlled to allow rollback if required
- Reviewed and approved in accordance with the organization's Change Management Policy.

C. Monitoring and Review of Configurations

Configurations must be routinely reviewed to ensure they remain secure and aligned with:

- Evolving threat landscapes
- Updates or changes in software versions
- New vendor guidance or regulatory requirements

Where feasible, the organization shall implement automated tools (e.g., security configuration management tools, IaC scanners, cloud posture management tools) to:

- Detect deviations from the approved configuration baseline
- Alert on or auto-correct non-compliant settings
- Log and report deviations for follow-up

Deviation or non-compliance must be investigated, and corrective actions taken according to the incident response or change management process, as appropriate.