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

1 PURPOSE

This document specifies the key information security roles, responsibilities and authorities for the organisation's ISMS, and sets out the organization's guidelines to ensure that incompatible duties are identified and proper segregation is implemented to minimise risk.

2 SCOPE

This control applies to all projects, systems, and processes that constitute the organization's information assets, including the people who have access to these information assets.

3 REFERENCE

ISO/IEC 27001 Standard	Annex A 5.2 Information Security Roles & Responsibilities Annex A 5.3 Segregation of Duties

4 KEY INFORMATION SECURITY ROLES

In general, responsibilities that apply to all employees and other persons working under or on behalf of the organisation, and other interested parties are set out within the relevant policies and procedures of the Information Security Management System (ISMS). However, there are critical roles that need to be defined and allocated within the context of the ISMS. These typical roles with their relevant responsibilities and levels of authority are as follows:

ISMS Role	Description	Responsibilities & Authorities
Top Management	Person who directs and controls the organisation at the highest level as reflected in the Organisation Chart (CEO)	● Ensuring that policies and objectives are established and are compatible with the strategic direction of the organisation ● Ensuring the integration of the ISMS requirements into the business processes, and that the ISMS achieves its intended outcomes ● Ensuring that the resources needed for the ISMS are available ● Promoting continual improvement ● Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility to contribute to ISMS effectiveness ● Ensuring that personnel: o are properly briefed on their information security roles and continue to have the appropriate information security skills and qualifications

ISMS Role	Description	Responsibilities & Authorities
		○ are provided with guidelines which state the information security expectations of their role within the organisation ○ are mandated to fulfil the information security policies of the organisation ○ comply with the terms and conditions of employment, contract or agreement, including the organisation's information security policies and appropriate methods of working ○ where practicable, are provided with a confidential channel for reporting violations of information security policies or procedures ("whistleblowing") ○ are provided with adequate resources and project planning time for implementing the organisation's information security processes and controls.
Management Representative (MR)	Primary role with a dedicated focus on ISMS	● Ensure that ISMS requirements are established, implemented and maintained in accordance with ISO/IEC 27001 Standard ● Ensure the information security policies and objectives are implemented, monitored and measured ● Ensure employee awareness, understanding and compliance with relevant policies, processes and controls ● Interact with external agencies like certification body and other interested parties with respect to ISMS ● Control of documented information related to ISMS ● Ensure that internal audits and relevant compliance checks are happening as per the defined interval ● Report on the performance of the ISMS to top management, and as a basis for improvement, arrange and facilitate management review meetings
Data Protection Officer (DPO)	A required appointment in line with Singapore Personal Data Protection Act (PDPA)	● Develop and oversee the data protection policies, processes, practices and measures within the organisation and ensure compliance with Personal Data Protection Act ("PDPA") and accompanying regulations

ISMS Role	Description	Responsibilities & Authorities
		• Keeping up to date with organisation's compliance with data protection obligations, and data protection developments • Foster a data protection culture among employees and communicate personal data protection policies to stakeholders • Manage personal data protection related queries and complaints, and handles access and correction request to personal data • Alert management to any risks that might arise with regard to personal data and report data protection performance to management • Liaise with the Personal Data Protection Commission ("PDPC") and other relevant stakeholders on data protection matters, where necessary (e.g., mandatory notification for notifiable data breach)
Information Security Steering Committee	Representatives from key departments and/or process owners to drive the ISMS	• Assist the MR in monitoring and assessing the organisation's policies and practices to ensure compliance with the organisation's ISMS • Identify information security risks, propose measures to manage the risks, implement information security controls and check for compliance within their area of responsibilities • Provide evidences of implementations and practices of the organisation's information security policies, procedures and controls • Coordinate with stakeholders and manage information security related queries and complaints • Participate in the quarterly information security meetings • Alert the MR to any risks that might arise with regard to information security and report on performance within their area of responsibilities
Incident Response Team (IRT)	The team in the organisation that handles information security incidents, and manage business continuity in a disruption	• Drive and coordinate all incident response activities with the aim to minimize damage and recovery quickly • Collect and analyse evidence, determine root cause and implement rapid system and service recovery • Document all incident response activities, especially investigation, discovery and recovery tasks, and develop reliable timeline for each stage

ISMS Role	Description	Responsibilities & Authorities
		• Conduct post-incident review and gather lessons learned from the incident with the aim to prevent its recurrence • Act as the point of contact for business continuity issues and ensure that business continuity activities are carried out within their areas of responsibilities as per the organisation's business continuity plans (BCPs) • Initiate, execute and maintains business continuity and disaster recovery plans • Conduct test on effectiveness of BCPs and identify resource requirements
Risk Owner	The role indicated in the Risk Assessment who cooperatively identifies and manage organisation risks and their cross-functional impacts	• Ensure that risk assessments are conducted at planned intervals and when there are significant changes in the organisation • Responsible for the monitoring and management of risks • Maintain and review risk treatment plans • Liaise with the owner(s) of the information asset(s) affected by the risk(s) • Escalate to management where one or more of their risks is not adequately addressed • Review the level of residual risk after treatment actions have been implemented
Asset Owner	The role indicated in the Asset Inventory who has the primary operational responsibility for one or more information assets tagged to him/her	• Responsible for specific, named information assets • Maintain and review security controls for allocated asset(s) • Participate in risk assessments concerning their asset(s) • Ensure the relevant entry in the asset inventory is kept up to date • Implement controls with regard to the information assets under their control • Assign access rights • Other duties as defined in the organisation's ISMS such as in the Acceptable Use Policies and Procedures.
System Admin	The role indicated in the Access List in-charge of the daily operation of systems and handles things like systems monitoring and setting up, deleting and	• Defending systems against unauthorized access • Monitoring traffic for suspicious activity • Configuring and supporting security tools • Provide technical security advice to users • Understanding and solving problems as automated alerts occur

ISMS Role	Description	Responsibilities & Authorities
	maintaining user accounts	• Adding and assigning users and network permissions
Internal Auditor (may engage external party)	Trained internal auditors to fulfil the internal audit requirements of the ISO/IEC 27001 Standard	• Plan, establish, implement and maintain an audit programme including the frequency, methods, responsibilities, planning requirements and reporting • Define the audit criteria and scope for each audit • Conduct internal audits at planned intervals • Ensure the audit process is objective and impartial • Report the results of audits to relevant management • Retain documented information as evidence of the audit programme and the audit results • Conduct follow-up audit to verify effectiveness of actions taken to address reported issues
Users (In general)	A person who utilizes the organisation's computer or network service and other information assets, often has a user account and is identified to the system by a username	• Be aware of and comply with all information security policies of the organisation relevant to their role • Report any actual or potential information security breaches • Contribute to risk assessment, where required • Take immediate action necessary to prevent an information security incident from occurring or escalating, where possible • Other duties as defined in the organisation's ISMS such as in the Acceptable Use Policies and Procedures.

5 RESPONSIBILITY MATRIX

Overall responsibilities for the management of the various sections of the ISO/IEC 27001 (Information Security Management System) Standard are shown in the following RACI table. This defines the type of responsibility of each role in each area according to whether the listed role is:

R= Responsible A= Accountable C= Consulted I= Informed

Role: / ISO/IEC 27001 / ISO/IEC 27701 Sections	Top Management	MR / DPO / ISMS Steering Committee	Internal Auditor	Asset Owner / Risk Owner / System Admin / Users	IRT
Context	A	R	I	I	I
Leadership	A/R	R	I	I	I
Planning	A/R	R	C	C	C

Role: / ISO/IEC 27001 / ISO/IEC 27701 Sections	Top Management	MR / DPO / ISMS Steering Committee	Internal Auditor	Asset Owner / Risk Owner / System Admin / Users	IRT
Support	A	R	I	I	I
Operation	A	R	C	R	C
Performance evaluation	A	R	R	R	R
Improvement	A	R	R	R	R
Information security controls	A	R	C	R	R

6 SEGREGATION OF DUTIES

Some activities expose the organization to a degree of risk that, unless controlled, they have the potential to allow an unscrupulous individual to commit fraud or other act that is detrimental to the organization. There is also the possibility of accidental creation, deletion or change of data if sufficient checks and balances are not in place to detect and prevent it.

It makes sense therefore that the organization should limit its risk by ensuring that combinations of activities that allow the potential for such occurrences are avoided and the activities spread across two or more individuals.

The approach to segregation of duties (SoD) mandates separation between individuals performing different duties. The basic concept underlying SoD is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

- Initiating, approving and executing a change
- Requesting, approving and implementing access rights
- Designing, implementing and reviewing code
- Developing software, testing and administering production systems
- Using and administering applications
- Implementing and auditing information security controls

For most of the organisation's processes, it would require separation between execution, verification and approval. Where there aren't enough people / groups to separate all incompatible duties or for efficiency reasons, the SoD requirements may be relaxed for separation between operational duties as long as they are subject to independent authorization or verification. In some cases, separation may not be required between control duties such as verification and approval, which may be delegated to the same authority.

Whenever such simplifications are made, compensating controls such as monitoring activities, audit trails and management supervision can be introduced to reduce the risk of errors, omissions, irregularities and deficiencies.