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

The purpose of this procedure is to describe the necessary awareness and competence of people performing roles within the context of the organisation's Information Security Management System (ISMS).

SCOPE

This procedure applies to employees who work under the control of the organisation and covers information security related awareness and competencies.

REFERENCE

ISO/IEC 27001 Standard   7.2 Competence / 7.3 Awareness
Annex A 6.3 Information security awareness, education and training

DEFINITION

Competence – ability to apply knowledge and skills to achieve intended results.

RESPONSIBILITIES & AUTHORITIES

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

The Management Representative (MR) and HR are responsible to ensure that relevant personnel have the necessary awareness and competencies to effectively perform their information security roles and responsibilities.

PROCEDURES

   A. Onboarding of New Staff

     New hires shall complete an information security awareness training within 1 month from their joining date to have the general understanding of the following (non-exhaustive):

- Information security policies and objectives
- Their contribution to an effective ISMS, and the benefits of improved performance
- Possible consequences of breaching information security rules
- Importance of meeting contractual, regulatory and statutory requirements that apply to them

- The importance of ensuring and maintaining of information security and protection of personal data
- Applicable risk assessment and risk treatment
- Applicable information security processes and controls
- Information security weaknesses / vulnerabilities / events and incidents reporting and management

New staff awareness training will be documented using the *ISMS-PPL-02-F1 Staff Induction.*

B.   Security Awareness Programme

New and existing staff, and contractors who have access to the entity's ICT systems must complete a security awareness training at least annually. Attendance record shall be maintained for this. The security awareness training must minimally cover:

- awareness and compliance with applicable information security rules and obligations, as defined in policies, standards, applicable laws and regulations;
- individual's roles and responsibilities towards securing or protecting information belonging to the entity;
- basic information security knowledge (such as identifying social engineering attacks and identifying security incidents), processes (such as sensitive data handling and reporting security incident) and baseline controls (such as password security and malware controls);
- lesson learnt from past security incidents so as to reduce the recurrence of similar incidents; and
- contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

C.   Competency Development

In addition to the annual security awareness training, certain information security roles require specific competencies on information security. Those employees who have specific information security roles must be assessed for such competency requirements, and the evidence of their skills and competencies must be documented in the *ISMS-PPL-02-F2 Competency Matrix*. Proof of competencies must be maintained in the personnel file.

For employees who are not fully competent based on the Competency Matrix, *ISMS-PPL-02-F3 Competency Plan* for them must be documented to list down those actions to be taken to achieve the necessary competence, and evaluate the effectiveness of actions taken to close the competency gap.

FORMS

ISMS-PPL-02-F1   Staff Induction
ISMS-PPL-02-F2   Competency Matrix
ISMS-PPL-02-F3   Competency Plan