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 document is to establish the organisation's obligation to ensure compliance with all the relevant legal and contractual requirements in order to avoid breaches related to Information Security Management System (ISMS). It also explains the organisation's approach to meet those requirements, and ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing information security, and that implementation is in accordance with the established policies and processes.

SCOPE

This control applies to the review of the organisation's approach to managing information security including people, processes, and technologies within the scope of the organisation's Information Security Management System (ISMS).

REFERENCE

ISO/IEC 27001 Standard	9.1 Monitoring, measurement, analysis and evaluation Annex A 5.31 Legal, statutory, regulatory and contractual requirements Annex A 5.32 Intellectual property rights Annex A 5.35 Independent review of information security Annex A 5.36 Compliance with policies, rules and standards of information security

RESPONSIBILITIES & AUTHORITIES

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

The Management Representative (MR) shall ensure that regular reviews and compliance monitoring of the organisation's ISMS are carried out.

PROCEDURE

A. Legal and Contractual Requirements

The organisation relies upon the following stakeholders to identify the applicable legal and contractual requirements which are relevant to them within the context of information security.

Source	Areas Covered
Clients	Contractual requirements, client's IT security policies, standards and any instructions on security matters that may be issued by the client subsequently

Source	Areas Covered
Suppliers	Contractual requirements, terms and conditions, guidelines and instructions
Regulatory authorities	Regulatory framework and requirements in all relevant countries where the organisation conducts business, transfers information or use products and services where laws and regulations can affect the organisation
Industry bodies	Industry guidelines and best practices
Professional associations for information security and privacy	General information, latest trends, issues and best practices

The MR shall ensure access to the relevant source materials as indicated above for reference purposes. This may be through electronic form. Assessment of the risk implications of any new requirements and changes/developments in legal and contractual requirements will be discussed during the information security quarterly meetings. The assessment will include the following aspects:

- Degree of change to the ISMS and its associated policies, procedures, controls and plans needed to meet the requirements;
- Urgency of meeting the requirements;
- Consequences of not meeting the requirements including potential legal and contractual sanctions and substantial penalties;
- Available options for meeting the requirements; and
- Specific processes and individual responsibilities to meet the requirements.

Details of the applicable legal and contractual requirements will be updated in the Legal, Regulatory and Contractual Requirements Register.

B. Software License Compliance

All software used within the organisation must be on the list of approved software maintained by the MR. Installation and use of software on organisation's systems will be subject to IT supervision. Software must always be obtained from a source authorised by the copyright holder and information such as license agreement, license keys, number of licenses and software manuals must be maintained.

A review of installed software against recorded licenses must be carried out at least once a year as part of the asset audit to ensure that all software in use within the organization is correctly licensed. This may highlight opportunities for license re-use and identify any cases where additional licenses need to be purchased. In the event that a license is no longer required by a user (perhaps due to termination or reassignment), the terms of the software license must be reviewed to understand if and how it may be reused. If permitted by the license, the software may be redeployed to another user in order to ensure that best value is obtained for the organization.

The need for use of free or open-source software will be determined and approved by management. In the event that is have been approved for use within the organisation, the use of the software is dependent upon complying with its terms.

C. Protection of Intellectual Property Rights and Copyrighted Materials

The risks of personnel and third parties failing to uphold the organisation's own intellectual property rights should also be managed. All employees shall sign confidentiality or non-disclosure agreements as part of their employment terms and conditions. Suppliers requiring access to our business information and systems shall be required to sign the same as part of their contract.

It is important for all employees to know what IP the organization holds that needs to be protected from infringement. The following considerations must be remembered if our IP is to be protected:

- Remain vigilant for instances where our copyrights, patents, trademarks or designs are being used without permission
- Report all suspected infringements to the management
- Make sure that everyone understands what is and isn't permitted with respect to our IPs

Additionally, the organisation may make use of a variety of types of third-party IPs other than computer software, and it is important that copyright considerations are considered with respect to these assets too. These may include training videos, product documentation, presentations, photographs, customer logos on marketing materials, etc. Care must be taken to ensure that copyright is understood and not infringed in their use. The license provided may allow certain types of use without permission being obtained and this must be checked first. Where it is desired to make use of copyrighted materials outside of the terms of the license, clearance must be obtained from the copyright holder. The permission must be obtained in writing and kept in a safe place.

D. Independent Review of Information Security

The MR shall plan and initiate periodic independent reviews which should include assessing opportunities for improvement and the need for changes to the approach to information security.

Such reviews shall be carried out by individuals independent of the area under review and will be done through:

- Yearly internal audit in line with *ISMS-PR-03 Internal Audit*
- Yearly audit by an independent certification body engaged to achieve / maintain the organisation's ISO/IEC 27001 certificate

The MR shall ensure that the individuals carrying out these reviews have appropriate competence and are not in the line of authority to ensure they have the independence to make an assessment. For example, for internal audit, the assigned internal auditor shall not be under the same department / function that he/she is auditing to maintain impartiality.

The results of the independent reviews are reported to the management and records are maintained. If the independent reviews identify that the organisation's approach and implementation to managing information security is inadequate, corrective actions shall be initiated in line with *ISMS-PR-05 Control of Nonconformity and Corrective Action.*

In addition to the yearly internal audit and audit by certification body, the top management and/or the MR may consider arranging separate independent reviews when:

- Laws and regulations which can significantly affect the organisation change;
- Significant incidents occur;
- The organisation starts a new business or changes a current business;
- The organisation changes the information security controls and procedures significantly.

Trained internal auditors that conduct internal audits may also be assigned to carry out the separate independent reviews, when necessary. The MR shall ensure that the individual assigned to conduct the review is independent of the area under review.

E. Compliance with Policies, Rules and Standards for Information Security

The ISMS Steering Committee shall review compliance with policies, rules and standards for information security during the quarterly information security meetings. If any non-compliance is found as a result of the review, the manager in-charge of the area shall identify the causes of the non-compliance and implement corrective actions in line with *ISMS-PR-05 Control of Nonconformity and Corrective Action.* The ISMS Steering Committee shall review corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses during the next quarterly meeting, unless there is an urgent need to re-group before the next meeting. Results of these reviews and actions carried out shall be recorded in the quarterly information security meeting minutes.

Security reviews of the critical systems shall be conducted to periodically to evaluate the adequacy of the security policies, standards and controls to address new security threats and changes to the business operations and systems. The reviews of critical systems will be conducted in line with *ISMS-TECH-03 Management of Technical Vulnerabilities.*

F. Performance Evaluation and Improvement

Appendix A defines an initial starting point for the areas of the ISMS that will be monitored and measured and in broad terms how this will be done. In analysing and evaluating the results of the monitoring and measurement activities described in Appendix A, it is important that the right people are involved so that correct interpretation can be reached. The most appropriate forum for this will in most cases be the quarterly information security meetings and the yearly management reviews where any issues can be addressed and the need for continual improvement actions can be determined. Further metrics may be defined which will help to clarify the causes of issues in particular areas. These will be added to the table above and suitable reports created, if required.

FORMS

ISMS-ORG-12-F1	Legal, Regulatory and Contractual Requirements Register
ISMS-ORG-12-F2	Objectives Monitoring Table
ISMS-ORG-12-F3	Information Security Meeting Minutes

APPENDIX A AREAS TO BE MONITORED AND MEASURED

Area Monitored	Metric	Collection method	Collection frequency	Who collects and analyses	Evidence of Results
Achievement of objectives	*Refer to ISMS Manual Appendix D*			MR	Objectives Monitoring Record
Risks	Number of risks, by priority	Risk assessment results	At least once a year and when significant changes occur	MR	Risk Assessment & Risk Treatment Worksheet
Threats / vulnerabilities	Number of new threats notified / new vulnerabilities detected	Threat Intelligence Vulnerability Assessment	At least once a year	MR / IT	Threat Intelligence Report VA Report
Training	Number of employees trained for information security	Training record	At least once a year	MR / HR	Attendance / Training Record
Nonconformities	Number of non-conformities identified	NC & CA Log	Continuous	MR	Nonconformity and Corrective Action Log
Internal and external audits	Number of internal and external audit carried out	Audit reports	Yearly	MR	Audit Reports
Management review meeting Information security meetings	Number of meetings held	Minutes of meeting	Yearly Quarterly	MR	Meeting Minutes
Hacking attempts / anomalies	Number of recognised attacks	Log files Alerts	Continuous	System Admin	Logs
Use of critical resources	Threshold vs Utilisation and Forecast	Utilization Monitoring Forecasting	At least once a year planning and forecasting	MR / IT	Capacity Plan