	No of Pages	1 of 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	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 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES	3
PROCEDURE	3
A Due Diligence Assessment	3
B Supplier Agreements	4
C Performance Evaluation	5
D Managing Changes in Supplier Services	6
FORM	6

	No of Pages	3 of 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	Revision	1.0

PURPOSE

This document describes how due diligence assessments of suppliers who may be relevant to the organisation's Information Security Management System (ISMS) will be carried out, and how their performance will be evaluated.

SCOPE

This is applicable to the initial assessment of suppliers and the evaluation of their performance who may be relevant to the organisation's ISMS e.g., IT managed services provider, software/solutions/tools provider, asset disposal vendor. *For cloud service providers, refer to ISMS-ORG-09 Information Security for Use of Cloud Services.*

REFERENCE

ISO/IEC 27001 Standard	Annex A 5.19 Information security in supplier relationships
	Annex A 5.20 Addressing information security within supplier agreements
	Annex A 5.21 Management information security in the ICT supply chain
	Annex A 5.22 Monitoring, review and change management of supplier services

RESPONSIBILITIES & AUTHORITIES

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


The Management Representative (MR) shall ensure that this procedure is maintained and remain relevant to the context of the organisation.

PROCEDURE

A Due Diligence Assessment

The following assessment related to information security must be completed preferably before a decision to purchase, and any commitment is made:

1. Review the commercial details of the offering under consideration, including terms of sale and contract terms including length, supplementary services, renewal and termination.
2. Establish to what extent the offering meets the requirements for the product or service. If sufficient requirements are not met, the supplier should not be used and this procedure terminates.

	No of Pages	4 of 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	Revision	1.0

3. Use the *Supplier Due Diligence Assessment Form* and record the details of the assessment, including date, assessor name, product or service name and requirements and classification of data that may be shared with the supplier, including whether personal data will be processed.
4. Find out what information is available about the information security controls used by the supplier, including information security policy / privacy policy and relevant certifications such as ISO/IEC 27001, ISO/IEC 27701, Cybersecurity Trustmark, Data Protection Trustmark, PCI DSS among others.
5. Understanding of the information security risks associated with the use of the supplier shall be ensured. The risks could be associated to:
 - a. The organisation's information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;
 - b. The types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organisation's information;
 - c. The supplier's use of the organisation's information and other associated assets, including risks associated from potential malicious supplier personnel;
 - d. Malfunctioning or vulnerabilities of the products (including software components and subcomponents used in these products) or services provided by the suppliers; and
 - e. Any risks of non-compliance to applicable privacy laws and regulations.

The information will be used to identify the required security safeguards that the supplier must be assessed on.


6. When all relevant information has been obtained and recorded, reach a decision about whether the supplier should be contracted with for the specific requirements under consideration.
7. A register of approved suppliers shall be maintained using *Approved Suppliers List*.

B Supplier Agreements

1. A contract or agreement shall be signed with the selected supplier. The clauses regarding information security and data protection, if applicable, are to be clearly defined. The supplier shall also be required to sign the Non-Disclosure Agreement prior to the start of engagement unless a confidentiality clause is already covered in the agreement with them.

Though the agreement may vary among the different types of suppliers, the organisation shall ensure that the following terms are considered, where appropriate:

- a. Description and classification of information to be provided or accessed and methods of providing or accessing them; rules for acceptable use and unacceptable use, if necessary;
- b. Legal, statutory, regulatory and contractual requirements including intellectual property rights and copyright;


	No of Pages	5 of 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	Revision	1.0

- c. Obligation of each contractual party to implement an agreed set of controls including access control, and the supplier's obligations to comply with the organisation's information security requirements;
 - d. Indemnities and remediation for failure of contractor to meet requirements;
 - e. Incident management requirements (especially notification and collaboration during incident investigation and remediation);
 - f. Necessary trainings and awareness;
 - g. Relevant contacts, including a contact person for information security issues;
 - h. Any screening requirements for supplier's personnel;
 - i. Evidence and assurance mechanisms of third-party attestations, where applicable;
 - j. Right to audit the supplier processes and controls related to the agreement;
 - k. Having contingency measures e.g., backup, where applicable;
 - l. Having a change management process that ensures timely notification of the organisation for any changes and the possibility for not accepting such changes, where applies;
 - m. Physical security and information transfer controls commensurate to the information classification;
 - n. Termination clauses including records management, return of assets, secure disposal, and any ongoing confidentiality obligations; and
 - o. Ensuring, at the end of the contract, necessary handover support.
2. Agreements with suppliers who are involved in personal data ("Data Intermediary / Data Processor") should include, where applies:
- a. Clearly spell out the supplier responsibilities taking into account the type of personal data processed (if any);
 - b. Specify that personal data is only processed on the organisation's instructions;
 - c. Require compliance with all applicable policies and procedures concerning information security and personal data handling and protection;
 - d. State that the organisation has the right to audit the supplier's compliance with applicable legislation and/or regulation relating to personal data, where needed; and
 - e. Call for independently audited compliance acceptable in the industry. For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001, ISO/IEC 27701, Data Protection Trustmark (DPTM), APEC-CBPR, or APEC-PRP can be considered.

C Performance Evaluation

Several ways may be used in evaluating whether the suppliers are meeting their contractual obligations. This can be demonstrated by any of the following whichever is the most appropriate for the nature of engagement.

1. The supplier may provide the organization with their self-assessment report or internal audit report that its practices meet the contractual obligations. Where required, the organization may perform audit or inspection of the external provider to verify that they are carrying out its roles and responsibilities properly.

	No of Pages	6 of 6
	Document Classification:	Internal
	Effective Date	1 Aug 2025
SUPPLIER DUE DILIGENCE ASSESSMENT & PERFORMANCE EVALUATION	Doc No	ISMS-ORG-08
	Revision	1.0

2. The supplier may provide the organization with an independent report or valid certification assessed by an independent auditor relevant to information security such as ISO/IEC 27001, ISO/IEC 27701, Cybersecurity Trustmark, Data Protection Trustmark, APEC-CBPR, APEC-PRP, PCI DSS among others among others.

3. The supplier will be evaluated against a set of evaluation criteria.

Evaluation of the suppliers shall be done at least once a year for contract duration exceeding 1 year or at the end of the contract if duration is less than 1 year, prior to any renewal, and recorded in the *Supplier Performance Evaluation*.

For any issues noted during the evaluation, the supplier will be given 30 calendar days to rectify the findings unless reasonable justification is provided for extension of the timeline. If no rectifications have been made as per the agreed timeline, the supplier shall be delisted from the *Approved Suppliers List* and the organization may start the due diligence assessment process again in selecting a suitable replacement.

D Managing Changes in Supplier Services

The organisation shall regularly monitor, review, evaluate and manage change in supplier services including:

- Enhancements to the current services offered;
- Development of any new applications and systems;
- Modifications or updates of the relevant supplier's policies and processes;
- New or changed controls to resolve incidents and improve information security;
- Changes and enhancements to networks;
- Use of new technologies;
- Adoption of new products or newer versions or releases;
- New development tools and environments;
- Changes to physical location of service facilities;
- Change of sub-suppliers;
- Sub-contracting to another supplier;

Agreements shall be reviewed for suitability and adequacy in terms of information security relevant requirements. Re-assessment of risks shall be done for any changes to the provision of product / service by suppliers. Any new or changed information security risks shall be assessed and recorded in line with *ISMS-PR-01 Information Security Risk Assessment & Risk Treatment*.

FORM

ISMS-ORG-08-F1	Supplier Due Diligence Assessment
ISMS-ORG-08-F2	Approved Suppliers List
ISMS-ORG-08-F3	Supplier Performance Evaluation