	No of Pages	1 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
	Doc No	ISMS-ORG-09
INFORMATION SECURITY FOR USE OF CLOUD SERVICES	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 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY FOR USE OF CLOUD SERVICES	Doc No	ISMS-ORG-09
	Revision	1.0

TABLE OF CONTENTS

PURPOSE	3
SCOPE	3
REFERENCE	3
RESPONSIBILITIES & AUTHORITIES	3
PROCEDURE	3
A Due Diligence Assessment	3
B Cloud Service Agreements	4
C Use of Cloud Services	4
D Managing Changes	5
FORM	5

	No of Pages	3 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY FOR USE OF CLOUD SERVICES	Doc No	ISMS-ORG-09
	Revision	1.0

PURPOSE

The purpose of this document is to specify and manage information security for the use of cloud services.

SCOPE

This is applicable to the acquisition, use, management and exit from cloud services.

REFERENCE

ISO/IEC 27001 Standard Annex A 5.23 Information security for use of cloud services

RESPONSIBILITIES & AUTHORITIES

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


The Management Representative (MR), IT and DPO 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 subscribe or any commitment is made:

1. The organization shall review the cloud services' information security arrangements so that the risks associated with the cloud's access to / hosting of the data may be minimized appropriately. The *Cloud Supplier Questionnaire* must be completed for this purpose stating the minimum technical and organizational measures as well as relevant compliance with applicable security standards such as ISO/IEC 27001, ISO/IEC 27701, Data Protection Trustmark, APEC-PRP, Multi-Tiered Cloud Security (MTCS), PCI DSS among others among others.
2. The organisation must have a clear understanding of the following:
 - Roles and responsibilities of the cloud service provider (CSP) and the organisation as the cloud service customer;
 - Which information security controls are managed by the CSP and which are managed by the organisation as the cloud service customer;
 - How to obtain and utilize information security capabilities provided by the CSP;
 - How to obtain assurance on information security controls implemented by the CSP;

	No of Pages	4 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY FOR USE OF CLOUD SERVICES	Doc No	ISMS-ORG-09
	Revision	1.0

- How to manage controls, interfaces and changes in services when an organisation uses multiple cloud services, particularly from different cloud service providers;
 - Procedure for handling information security incidents that occur in relation to the use of cloud services;
 - Its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks; and
 - How to change or stop the use of cloud services including exit strategies for cloud services.
3. Understanding of the information security risks associated with the use of the cloud services shall be ensured. Any information security risks shall be assessed and recorded in line with *ISMS-PR-01 Information Security Risk Assessment & Risk Treatment*.

B Cloud Service Agreements


Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, the organisation should review cloud service agreements (e.g., terms and conditions or any equivalent published documentation) with the cloud service provider(s).

The cloud service agreement should address the confidentiality, integrity, availability and information handling requirements especially for personal data. The following provisions for the protection of organisation's data and availability of cloud services must be evident:

- Providing solutions based on industry accepted standards for architecture and infrastructure;
- Managing access controls of the cloud service to meet the requirements of the organisation;
- Implementing malware monitoring and protection solutions;
- Processing and storing the organisation's sensitive information in approved locations (e.g., particularly country or region) or within or subject to a particular jurisdiction;
- Providing dedicated support in the event of an information security incident in the cloud service environment;
- Ensuring that the organisation's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier;
- Supporting the organisation in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;
- Providing appropriate support and availability of services for an appropriate time frame when the organisation wants to exit from the cloud service;
- Providing required backup of data and configuration information and securely managing backups and restoration as applicable, based on the capabilities of the cloud service provider; and
- Data purging and deletion during service provision or at termination of service.

C Use of Cloud Services

The asset owner tagged to the cloud service should define how cloud services should and should not be used, and ensure that the use of the cloud service complies with the organisation's information security policies and controls including but not limited to:

	No of Pages	5 of 5
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY FOR USE OF CLOUD SERVICES	Doc No	ISMS-ORG-09
	Revision	1.0

- Access controls
- Authentications
- Event logging
- Data retention and secure deletion
- Availability requirements
- Vulnerability management
- Information security incident management

The organization may rely on the validity of the cloud's relevant certification to industry standards like ISO/IEC 27001, ISO/IEC 27701, Data Protection Trustmark, APEC-PRP, Multi-Tiered Cloud Security (MTCS), PCI DSS, and may decide to end the subscription in the event its services no longer meet the organisation's requirements.

D Managing Changes

The organisation shall closely monitor notifications / alerts from the CSP and review changes in the terms and conditions for the use of the cloud services for any substantive customer impacting changes including but not limited to:

- Changes to the technical infrastructure (e.g., relocation, reconfiguration, or changes in hardware or software that affect or change the cloud service offering);
- Processing or storing information in a new geographical or legal jurisdiction;
- Use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

Re-assessment of risks shall be done for any changes in line with *ISMS-PR-01 Information Security Risk Assessment & Risk Treatment*.

FORM

ISMS-ORG-09-F1 Cloud Supplier Questionnaire