Owner :	Jed Hewson
Reference Number :	1SMTS-INF-POL006
Approved Date :	2024-08-14
Next Review Date :	2024-11-01
Version :	5

Information Security Management and Use of Cloud Services Policy and Procedure

1. Policy Statement:

This policy establishes guidelines and procedures to ensure the secure and responsible use of cloud

services within the organisation. The objective is to protect sensitive information, maintain data integrity, and mitigate risks associated with the adoption of cloud solutions.

2. Scope:

This policy applies to all employees, contractors, and third-party service providers who have access to or utilize cloud services on behalf of the organization.

2.1. Cloud Solution Selection Criteria:

a. Compliance and Legal Requirements:

- Ensure that selected cloud services comply with relevant laws, regulations, and industry standards of data protection and privacy.

b. Data Classification and Handling:

- Classify data based on sensitivity and select cloud services that align with the organization's data handling policies.

c. Security Features:

- Evaluate the security features offered by cloud service providers (CSPs), such as encryption, access controls, and multi-factor authentication.

d. Service Level Agreements (SLAs):

- Review and negotiate SLAs with CSPs to ensure they meet the organization's performance, availability, and security requirements.

e. Data Ownership and Portability:

- Clarify data ownership and portability terms within cloud service agreements to maintain control over organizational data.

2.2. Risk Management:

a. Risk Assessment:

- Conduct regular risk assessments to identify and evaluate potential risks associated with the use of cloud services.

b. Data Encryption:

- Encrypt sensitive data during transmission and storage to protect against unauthorized access.

c. Incident Response and Reporting:

- Establish procedures for reporting and responding to security incidents related to cloud services promptly.

d. Vendor Risk Management:

- Regularly assess and monitor the security practices of cloud service providers, ensuring they adhere to the organization's security standards.

2.3. Security Controls:

a. Access Control:

- Implement strong access controls, including identity management, to regulate user access to cloud resources.

b. Data Loss Prevention (DLP):

- Employ DLP measures to prevent unauthorized disclosure of sensitive information within cloud services.

c. Security Monitoring and Logging:

- Set up continuous monitoring and logging to detect and respond to security incidents promptly.

d. Regular Audits and Assessments:

- Conduct regular audits and assessments of cloud service configurations and security controls to identify and rectify vulnerabilities.

2.4. Employee Training and Awareness:

- Provide comprehensive training to employees on the secure use of cloud services and raise awareness about potential risks and best practices.

2.5. Compliance:

- Ensure adherence to this policy by conducting periodic reviews and audits to validate compliance.

2.6. Policy Review and Update:

- Regularly review and update this policy to reflect changes in technology, regulations, and organizational requirements.

2.7. Document Control:

- Maintain documentation of cloud service usage policies, risk assessments, and security controls for reference and audit purposes.

2.8. Enforcement:

- Violation of this policy may result in disciplinary action, including termination of employment or contract.

3. Policy Acceptance and Acknowledgement

All employees, contractors, and third parties must acknowledge their understanding and acceptance of this policy upon hire or engagement with the organization. Failure to comply with this policy may result in disciplinary action

4. Risk Management

All risks identified and associated with this policy/procedure are recorded on the Risk Management Register (Risk Management Register) and managed according to the Risk Management Process (Risk Management Process)

5. Corrective Action

The company's Corrective Action Procedure will be activated if this policy fails to meet the objectives.

6. Updating, Distribution and Communication of this Document

This policy can be updated by the Process Owner following the procedure defined in the Document and Control of Records Process **(Control of Documentation Process).**

The distribution of this process document is circulated to the following persons:

- *Chief Executive Officer*
- *Chief Operations Officer*
- *QMS Management Representative*
- *ISMSR*
- *Bookkeeper*

7. Management Review

Management should review this document on a continual improvement basis for suitability, adequacy and effectiveness, at least no less than once every twelve months.

Reports required for the reviewing of input and output of this process are:

- *Follow-up actions from previous management reviews*
- *Risk Registers*
- *Information Security Incident Management Reports*

The output from the Management Review will include:

- *Improvements in the effectiveness of the Information Security Management System and its processes*
- *Resources needed*
- *Improvements in the process related to the provision of service to the business*
- *Updates to Information Security Plans*

Linked documents:

Supplier Questionnarie

Information_Security_Management_and_Use_of_Cloud_Services_Policy_and_Procedure
Reviewed : 2024-08-14