Cloud Security Policy

Document version : 1.0

Document No. : ISMS-PL-14

Document owner: ISMR/ISMA

Last updated: 03-04-2024

Document control

Document approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved by
IT Security	***Head of Department***	***Chief Technology Officer***
Date : 03-04-2024	**Date :** 03-04-2024	**Date :** 03-04-2024

Version History

The following table lists all the revisions made to this document:

Version	Date	Description	Revised By
1.0	03-04-2024	Initial version	Napasorn S.

HUMANICA

Table of contents

HUMANICA

Cloud security policy

Purpose

- To ensure the security of all cloud-based services, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), within our organization.
- To maintain the integrity, confidentiality, and availability of data and services while enabling the organization to leverage the benefits of cloud technology effectively and securely.

Scope

- All employees, contractors, and third-party vendors who access or manage cloud services on behalf of the organization. It encompasses all cloud-based applications, platforms, and infrastructure utilized for business operations.

Cloud security policy

1. **Identity and Access Management (IAM)**
    - An IAM system shall be utilized to manage user identities, permissions, and authentication in cloud services.
    - User access should be regularly reviewed and revoked when no longer required refer to *System Access Control Policy*.
2. **Access controls**
    - Access to cloud resources must be granted on a need-to-know basis, following the principle of least privilege refer to *System Access Control Policy*.
    - Accessing cloud management service must enforce multi-factor authentication (MFA).
3. **Data protection**
    - All data stored or processed in the cloud must be classified based on its sensitivity level refer to *Information Classification and Handling Policy*. Access controls and encryption mechanisms shall be applied accordingly.
    - Encryption must be enforced for data both in transit and at rest within the cloud environment.
    - Data residency requirements must be considered when selecting cloud service providers. Data shall only be stored in compliant with relevant regulations.
4. **Logging and monitoring**
    - Comprehensive logging of cloud activities must be implemented, including user access, configuration changes, and administrative actions refer to *Log Management Procedure*.
    - Continuous monitoring of cloud environments for security threats, vulnerabilities, and unauthorized activities must be conducted to detect and respond to security incidents promptly.
5. **Incident response**
    - A documented incident response plan must be in place to address security breaches, data leaks, or other security incidents involving cloud services.
    - Employees must be trained on incident response procedures and their roles in mitigating and reporting security incidents.

- An incident report should include incident identification, classification based on severity, containment and mitigation strategies, forensic investigation for root cause analysis, stakeholder communication, and comprehensive incident reporting.
- Refer to *Security Incident Management Procedure*.

6. **Network security**
   - Network security measures, including firewalls, intrusion detection systems (IDS), and virtual private networks (VPN), shall be implemented to protect data in transit refer to *Network Management Policy*.
7. **Vulnerability management**
   - Regular patching of cloud infrastructure and applications shall be performed to mitigate known vulnerabilities refer to *Vulnerability Management Procedure*.
8. **Vendor management**
   - Establish criteria for selecting and assessing third-party vendors that provide cloud services. Evaluate vendors' security capabilities, compliance with industry standards. Define contractual agreements and service level agreements (SLAs) to formalize security responsibilities and expectations refer to *Third Party Security Policy*.
9. **Compliance and audit**
   - Regular audits and assessments shall be conducted to ensure compliance with industry regulations, standards, and contractual obligations refer to *Compliance Standard*.
10. **Review and update cloud security policy**
    - This policy shall be reviewed and updated periodically to address evolving threats, technologies, and regulatory requirements. Any revisions to the policy shall be communicated to all relevant stakeholders.

Cloud exit strategy

Exiting the cloud, refers to migrating data, applications, or infrastructure from a cloud environment (such as public cloud services Huawei, AWS, or other Cloud) back to an on-premises environment or to a different cloud provider. The decision to exit the cloud system shall consider as follows.

1. **Cost analysis**
   - Evaluate the total cost associated with the current cloud infrastructure compared to on-premises alternatives or other cloud providers. Ensure that the costs of exiting the cloud, including data migration into the analysis.
2. **Data portability**
   - Assess the ease of migrating data out of the current cloud environment. Ensure that data is stored in formats that are compatible with the chosen destination and consider any data transfer costs and bandwidth limitations.
3. **Application compatibility**
   - Determine whether the applications hosted in the cloud can be seamlessly transitioned to on-premises infrastructure or to a different cloud provider. Consider factors such as dependencies, API compatibility, and any custom configurations.

4. **Compliance and regulatory requirements**
   - Ensure that exiting the cloud does not violate any compliance regulations or contractual obligations. This includes considerations such as data privacy laws, and industry-specific regulations.
5. **Security implications**
   - Assess the security implications of migrating data and applications out of the cloud. Consider how sensitive data will be protected during the migration process and whether on-premises infrastructure or another cloud provider can provide equivalent or better security controls.
6. **Performance and scalability**
   - Evaluate whether on-premises infrastructure or an alternative cloud provider can meet the performance and scalability requirements of the workload. Consider factors such as network latency, resource availability, and the ability to scale resources dynamically.
7. **Business continuity and disaster recovery**
   - Develop a comprehensive plan for business continuity and disaster recovery during the migration process. Ensure that critical systems remain operational throughout the transition and that data integrity is maintained.
8. **Vendor lock-in mitigation**
   - Implement strategies to mitigate vendor lock-in risks, such as using open standards and avoiding proprietary technologies that may hinder the portability of applications and data.
9. **Transition timeline and resources**
   - Develop a detailed migration plan outlining the timeline, resources, and responsibilities involved in exiting the cloud. Consider factors such as downtime, data synchronization, and the availability of skilled personnel.
10. **Stakeholder communication**
    - Communicate the decision to exit the cloud effectively to all stakeholders, including employees, customers, partners, and regulatory authorities. Address any concerns and provide updates throughout the migration process to ensure a smooth transition.

Supporting documents

1. Information Classification and Handling Policy
2. System Access Control Policy
3. Network Management Policy
4. Third Party Security Policy
5. Security Incident Management Procedure
6. Vulnerability Management Procedure
7. Log Management Procedure
8. Cryptographic and Key Management Policy
9. Encryption Standard
10. Compliance Standard

End of document