elevaite365

TECH THAT MATTERS

Elevaite365

Cloud Security Policy

Version 1.0

PURPOSE

This policy establishes guidelines and procedures for the secure use, management, and governance of cloud services and resources within Elevaite365(herein referred to as the organization). It aims to protect sensitive data, maintain the integrity and availability of systems and applications, and mitigate risks associated with cloud computing environments.

SCOPE

This policy applies to all employees, contractors, vendors, and any other individuals who access or use cloud services and resources on behalf of the organization. It encompasses the selection, implementation, and ongoing management of cloud solutions, regardless of deployment models (e.g., public, private, hybrid) or service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service).

DEFINITION

- **CSP**: Cloud Security Provider
- **RBAC**: Role-Based Access Control
- **PII:** Personally Identifiable Information

ROLES AND RESPONSIBILITIES

1. **Cloud Security Administrator**: Responsible for configuring and maintaining security settings and controls within the cloud environment, including access management, encryption, and monitoring.
2. **Data Owner:** The individual or team accountable for the organization's data stored in the cloud, including data classification, access control, and data retention policies.

POLICY

1. System Owners will adhere to the Information Security Policies and Standards when utilizing cloud services.
2. System Owners should maintain a current inventory of assets hosted in cloud environments in accordance with the Asset Management Policy. The inventory should contain information such as organization criticality, data classification as defined in the Data Protection Policy, Service Level Agreements (SLAs), and business continuity requirements.
3. Data in cloud environments will be classified and protected as outlined in the Data Protection Policy.
4. System Owners will comply with geographic restrictions on data storage, processing, and transmission, including but not limited to regulatory requirements governing the flow of data
   across borders, international commerce and trade laws, and location-based restrictions on physical and logical access to the data.
5. Information and applications residing in multi-tenant hosting environments will have access restricted appropriately.
6. System owners will confirm that cloud service providers (CSPs) will have audit plans requiring at least a quarterly assessment of the effectiveness of information security measures. Upon request, cloud providers can show evidence of audit results and proof of compliance with industry and regulatory standards defined in the Third-Party Security Risk Management Policy.
7. Access to the information stored in external cloud environments will be subject to the same access controls as internally hosted applications and infrastructure defined in the Access Management Policy and Third-Party Security Risk Management Policy.

DATA STORAGE

Country of storage: Personal and other data is stored and processed in countries where data centers of the third-party supplier are located and in countries where premises are located. The organization does not transfer personal data to third countries. When a transfer to a third country is needed, it can be granted by adequate measures for information security valid in the organization and requirements in contracts with customers.

CLOCK SYNCHRONIZATION

All virtualized logical devices must be synchronized to the NTP server, a specific time source in the cloud according to the centralized clock. Clock synchronization is essential for the accuracy of system logs, which may be used as evidence in investigations. The organization synchronizes its cloud server infrastructure by using the default time synchronization configuration of the cloud infrastructure provider.

PRIVACY AND SECURITY CONTROLS FOR CLOUD HOSTING

The organization will assess a potential cloud service provider accessing organization-managed PII data to ensure the CSP can operate with any applicable capabilities and functionalities outlined below. The organization may include these in the questionnaire or other assessment methodologies of the potential CSP as deemed relevant in its evaluation.

NAME	REQUIREMENT
Electronic Discovery	Ensure that the cloud provider’s electronic discovery capabilities, processes, and policies do not compromise the privacy and security of PII data hosted by the CSP.
Continuous Monitoring	Where possible, ensure that hosted systems or services allow the organization to monitor them for uptime, availability, and security functionality.
Architecture	The organization should understand the applicable underlying technologies that the cloud providers use to host services and how they integrate with current CSP infrastructure if such integration exists.
Identity and Access Management	Ensure relevant safeguards are in place to secure authentication, authorization, and other identity and access-management functions in accordance with the requirements outlined in the Account Management Policy and Data Security Policy.
Software and Data Isolation	CSPs should certify that their systems’ structure or architecture in multi-tenant offerings can isolate hosted data and operations from other tenants where possible.
Availability	Establish an SLA with the CSP to notify them of service disruptions and the resumption of critical operations within an agreed-upon time.
Incident Response	Ensure that the cloud provider informs the organization within 24 hours after a breach is discovered that directly impacts agency resources or data.

POLICY REVIEW AND UPDATES.

This policy will be reviewed annually or updated as necessary to address technological changes, emerging threats, regulatory requirements, and organizational needs.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Aug 29 2025	Initial Release	Borhan,Linh	Linh	Borhan