Information Technology Executive Council (ITEC)

ITEC 7024-P

1.0 TITLE: Cloud Security Policy

2.0 PURPOSE: This policy establishes minimum information security requirements for Cloud Services.

3.0 SCOPE: This policy applies to Cloud Services administered by or outsourced to Contractors by affected Entities.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas branches, boards, commissions, departments, divisions, Entities, and third parties involved in processing, transmitting, or providing business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 REFERENCES:

5.1 CIS Critical Security Controls v8, as amended

5.2 CIS Controls Cloud Companion Guide, as amended

5.3 CSA Security Guidance v4, as amended

5.4 FIPS 140-3, as amended

5.5 ITEC 1100-P, as amended

5.6 NIST Cybersecurity Framework (CSF) 2.0, as amended

5.7 NIST Special Publication (SP) 800-210, as amended

6.0 DEFINITIONS:

6.1 Cloud Service: Refers to Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

6.2 Cloud Service Provider (CSP): A Contractor that provides a Cloud Service.

6.3 Infrastructure as a Service (IaaS): As defined in ITEC 1100-P.

6.4 Management Plane: Interfaces used for managing cloud assets.

6.5 Platform as a Service (PaaS): As defined in ITEC 1100-P.

6.6 Restricted-Use Information (RUI): As defined in ITEC 8010-P.

6.7 Software as a Service (SaaS): As defined in ITEC 1100-P.

7.0 POLICY: This policy governs the use of Cloud Services by all State of Kansas Entities. Individual Entities may impose supplemental restrictions through their specific policies, provided these do not conflict with this policy.

Entities must:

General Requirements for Cloud Services

7.1 Ensure that IaaS, PaaS, and SaaS services storing, processing, or transmitting RUI have either FedRAMP or StateRAMP moderate authorization, or a comparable alternative.

7.2 Ensure all IaaS, PaaS, and SaaS services are physically hosted within the United States or its territories.

7.2.1 Ensure exceptions to this requirement are made by authorized Entity leadership and only for pre-approved educational research activities. These activities must adhere to data-sharing agreements or comparable data control mechanisms that ensure the protection of RUI.

7.3 Ensure all support services for IaaS, PaaS, and SaaS systems are performed by individuals physically located within the United States or its territories.

7.4 Ensure Cloud Service Providers isolate the Entity's data and applications from other tenants within the same cloud environment.

7.5 Ensure contracts delegate security responsibilities for Cloud Services as detailed in Appendix A.

7.6 Prohibit the use of personal cloud services, including email and file storage, for Entity business purposes.

Encryption and Key Management

7.7 Use the most recent FIPS 140 certified encryption mechanisms to encrypt RUI at rest and in transit.

7.8 Establish and document processes and procedures for encryption key management, ensuring comprehensive control over all encryption keys.

7.9 Retain ownership of all encryption keys and implement best practices for their management, including enforcing key rotation policies, utilizing hardware security modules (HSMs), and establishing access controls to restrict access to encryption keys.

7.10 Rotate access keys at least quarterly, avoid reusing keys across applications, and do not store keys directly in code.

7.11 Ensure that private keys used for encryption are securely managed and not shared with third parties without proper authorization.

7.12 Securely manage private keys and API keys by regularly rotating them, avoiding hardcoding in code or configuration files, and storing them in approved key vaults.

API Management

7.13 Maintain an inventory of APIs used by the Entity that includes:

7.13.1 Name: Descriptive name clearly identifying the API's purpose.

7.13.2 Version: Track different versions and depreciation schedules.

7.13.3 Description: Summarize the API's functionality and value proposition.

7.13.4 Authentication Methods: Supported authentication mechanisms (e.g., OAuth, API keys).

7.13.5 Authorization Controls: Access control mechanisms restricting unauthorized access.

7.13.6 Rate Limiting and Throttling: Defined limits on API call frequency and resource consumption.

7.13.7 Protocols: Supported communication protocols (e.g., HTTP, HTTPS).

7.13.8 Endpoints: URLs for accessing the API and specific functionalities.

7.13.9 Request Formats: Data formats accepted for input (e.g., JSON, XML).

7.13.10 Response Formats: Data formats returned as output (e.g., JSON, XML).

7.13.11 Resource Schema: Description of data structures and field definitions accessed/manipulated through the API.

7.13.12 Dependencies: Any other APIs or functionalities required for the API to function properly.

7.13.13 Classification of Data Involved: Classification of the data handled by the API, including any RUI.

7.14 Implement security controls, including proper authentication, access control mechanisms, and secure storage of keys, to manage API usage.

Cloud Migration and Logging

7.15 Establish a comprehensive backout strategy prior to migrating any information system or production data to a cloud environment. This strategy must include defined procedures for reverting to previous states, addressing potential risks associated with failed migrations or deployments, and ensuring the integrity and availability of data throughout the transition process.

7.16 Ensure all cloud environments (IaaS, PaaS, and SaaS) have robust logging capabilities that track user activity, access, configuration changes, administrative actions, and security events.

7.17 Ensure all changes to cloud configurations follow the established change management process.

Entities using IaaS, must:

7.18 Implement granular Role-Based Access Control (RBAC) to manage access to IaaS resources.

7.18.1 Ensure that roles are defined based on the principle of least privilege.

7.18.2 Ensure that access rights are regularly reviewed and adjusted as necessary.

7.19 Enforce the use of Multi-Factor Authentication (MFA) for accessing IaaS management interfaces.

7.19.1 Ensure that MFA is required for any remote access to critical IaaS resources.

7.20 Ensure that Remote Desktop Protocol (RDP) is not directly exposed to the internet from any cloud environment.

7.20.1 Route all RDP access through a secure, controlled, and monitored access point, such as a VPN, bastion host, or secure jump server, to mitigate the risk of unauthorized access.

7.21 Implement micro-segmentation within IaaS environments to create smaller, isolated segments within the network, where possible.

7.22 Configure network security settings and tools to isolate and segment networks into different security zones based on the level of trust and access required.

7.23 Monitor and restrict communications between environments to only authenticated and authorized connections. Review authorized connections at least annually and document justification for allowed services.

7.24 Implement data lifecycle management practices within IaaS environments, ensuring that data is securely stored, transmitted, and disposed of at each stage of its lifecycle. Include mechanisms for secure data deletion that align with legal and regulatory requirements.

7.25 Automate the backup process for all critical data and configurations within the IaaS environment.

7.26 Regularly test backups at least monthly and ensure that recovery procedures are well-documented and understood by relevant personnel.

7.27 Ensure that cloud backups are not stored in the same regional environment as the production system.

7.28 Store all backups in a separate cloud account from the production system to isolate and protect backup data from potential security breaches or failures in the production environment.

7.29 Configure backups to be immutable, preventing alteration, overwriting, or deletion within the defined retention period.

7.30 Adopt Infrastructure as Code (IaC) practices to enhance the efficiency, security, and scalability of IaaS resource management, where possible.

7.31 Ensure that IaC scripts are subject to the same security controls as other code, including version control, code reviews, and testing.

7.32 Assess and manage the security risks associated with third-party tools and services integrated into the IaaS environment. Ensure that these integrations follow the same security standards as the core IaaS services.

7.33 Conduct routine vulnerability scans at least weekly of container images.

7.34 Remediate identified vulnerabilities within containers or their images prior to placing them into production.

7.35 Ensure container images are fully patched before deployment.

7.36 Harden all host and guest operating systems, and hypervisors according to Configuration Settings defined within the EBIT Configuration Management Policy.

7.37 Use specialized, secure workstations exclusively for performing system administration tasks in IaaS environments.

7.38 Use a dedicated account to perform backups, ensuring privileges are restricted to backup data only and not for making configuration changes.

<u>Entities using PaaS, must:</u>

7.39 Implement granular access controls within PaaS environments to restrict access to specific resources, services, or data based on user roles and responsibilities.

7.40 Ensure that these access controls are regularly reviewed and updated as needed.

7.41 Integrate robust Identity and Access Management (IAM) practices within PaaS environments, ensuring that users are authenticated using strong methods, such as Multi-Factor Authentication (MFA), and that least privilege principles are enforced.

7.42 Ensure that development, testing, staging, and production environments within PaaS are segregated to prevent accidental or unauthorized access to production data or resources.

7.42.1 Implement strict controls to manage and monitor data flows between these environments.

7.43 Ensure multi-tenant environments are logically and/or physically isolated to prevent unauthorized data leakage.

7.44 Apply sanitization or deidentification routines on RUI before loading it into any non-production environment.

7.45 Implement data masking or tokenization techniques within non-production environments to protect sensitive data while allowing developers and testers to work with realistic datasets.

7.46 Enforce secure coding practices within PaaS environments, ensuring developers adhere to guidelines that mitigate common vulnerabilities such as SQL injection and cross-site scripting (XSS).

7.47 Ensure that static and dynamic application security testing (SAST/DAST) is conducted to identify and mitigate security vulnerabilities in code prior to deployment.

7.48 Ensure that Service Level Agreements (SLAs) with PaaS providers include specific security requirements, such as uptime, data protection measures, and incident response times.

7.49 Implement capacity planning to ensure that the PaaS environment can scale securely to meet the needs of the organization.

7.50 Define and enforce controls around resource allocation within PaaS environments to ensure optimal and secure use of cloud resources while preventing abuse.

7.51 Assess the security of any third-party services or components integrated into the PaaS environment. Ensure that these integrations do not introduce new vulnerabilities and are subject to the same security standards as the core PaaS platform.

<u>Entities using SaaS, must:</u>

7.52 Ensure that access to SaaS applications is managed using Role-Based Access Control (RBAC), with roles defined based on the principle of least privilege.

7.53 Regularly review and update access roles at least annually to reflect changes in personnel or responsibilities.

7.54 Define and enforce data retention policies within SaaS applications that comply with legal, regulatory, and business requirements. Ensure that data is securely archived or deleted according to these policies.

7.55 Ensure that data disposal processes are in place to securely delete data from SaaS environments when it is no longer needed, including ensuring that all backups and copies are also securely deleted.

7.56 Ensure that SaaS providers perform regular backups of critical data and configurations.

7.57 Ensure that these backups are securely stored and that recovery procedures are tested periodically.

7.58 Work with SaaS providers to establish and maintain a disaster recovery plan that includes clear procedures for data recovery in the event of a system failure, data corruption, or other emergencies.

7.59 Ensure that Service Level Agreements (SLAs) with SaaS providers include specific security and availability metrics, such as uptime guarantees, response times for security incidents, and data breach notification timelines.

7.60 Ensure that SaaS providers have defined and documented incident response procedures. These procedures must be coordinated with the Entity's own incident response plans and include clear communication channels with the Entity in the event of a security incident affecting SaaS environments.

8.0 RESPONSIBILITIES:

8.1 Heads of Entities must establish procedures to ensure compliance with this policy.

8.2 The Chief Information Security Officer (CISO), Executive Branch, is responsible for maintaining this policy.

9.0 ENFORCEMENT:

9.1 Non-compliance with this policy may result in disciplinary action, including termination of employment for severe violations.

9.2 Written approval from the Kansas Information Security Office (KISO) is required for any exception to this policy.

10.0 CANCELLATION: This policy cancels and supersedes all previous versions.

Appendix A – Cloud Responsibility Matrix

Responsibility	SaaS	PaaS	IaaS
Responsibility of the Entity			
Information and Data	Entity	Entity	Entity
Devices (mobile and workstations)	Entity	Entity	Entity
Accounts and Identities	Entity	Entity	Entity
Access Reviews	Entity	Entity	Entity
Shared Responsibility			
Identity and Directory Infrastructure	Shared	Shared	Entity
Applications	CSP	Shared	Entity
Network Controls	CSP	Shared	Entity
Logging and Monitoring	Shared	Shared	Entity
Encryption	Shared	Shared	Entity
Incident Response	Shared	Shared	Entity
Compliance with Regulatory Requirements	Shared	Shared	Shared
Auditing	Shared	Shared	Shared
Backup Management	Shared	Shared	Entity
Disaster Recovery	Shared	Shared	Entity
Patch Management	Shared	Shared	Entity
Responsibility Transferred to CSP			
Physical Hosts	CSP	CSP	CSP
Physical Network	CSP	CSP	CSP
Physical Data Center	CSP	CSP	CSP

VPN and Secure Connections	CSP	CSP	Entity