Information Technology Executive Council (ITEC)

NOTICE OF PUBLIC MEETING

REGULAR MEETING OF ITEC
Tuesday, December 17, 2024 – 1:30pm – 2:30pm

In Person and Virtual Meeting
Location:
Judicial Branch
Conference Room
301 SW 10th Ave
Topeka, KS 66612

Registration Link to Virtual Meeting, click here

ITEC Board Members:

Jeff Maxon, Executive Branch CITO (Chair)
Doug Polston, Regents Representative #1
Ken Harmon, Regents Representative #2
Adam Proffitt, Cabinet Agency Head #1
Amber Shultz, Cabinet Agency Head #2
Adrian Guerrero, Non-Cabinet Agency Head #1
Lynn Retz, Non-Cabinet Agency Head #2
Keith Scott, KCJIS
Greg Gann, County Representative
Mike Mayta, City Representative
Murray McGee, Information Network of Kansas (INK)
Steve Funk, Board of Regents
John Berghuis, Private Sector Representative

Non-Voting Members

Senator Rick Kloos, Senate
Senator Jeff Pittman, Senate
Representative Emil Bergquist, House
Representative Pam Curtis, House
Tom Day, Interim Legislative Branch CITO
Alex Wong Judicial Branch CITO
Vacant, Chief Information Technology Architect

THIS MEETING IS IN COMPLIANCE WITH K.S.A. 75-7202 AND AMENDMENTS THERETO.

ITEMS ON THE AGENDA ARE FOR POSSIBLE ACTION BY THE BOARD UNLESS OTHERWISE STATED.
ITEMS MAY BE TAKEN OUT OF ORDER.
ITEMS MAY BE COMBINED FOR CONSIDERATION.
ITEMS MAY BE REMOVED FROM THE AGENDA OR DELAYED AT ANY TIME.

WELCOME / CHAIRMAN COMMENTS

Call to Order	Jeff Maxon, E-CITO
Roll Call	Celena Ramirez

APPROVAL OF AGENDA

APPROVAL OF MINUTES

November 12, 2024

ACTION ITEM STATUS

Action Item Review	Jason Hildebrandt, OITS
Introduction of Chief Data Officer	Jeff Maxon, E-CITO
SB291 Statement of Work Update	Jeff Maxon, E-CITO
Information Security Council Update	John Godfrey, E-CISO

POLICY AND PROCEDURES DISCUSSION John Godfrey, E-CISO

Technical revision to Access Control Policy

Final Action on Tranche 02 Security Policies

- Cloud Security Policy
- Identification and Authentication Management Policy
- Media Protection Policy
- Mobile Device Policy

Discussion on Tranche 03 Security Policies

- Acceptable Use of IT Policy
- IT Maintenance Security Policy
- Personnel Security Policy
- Physical and Environmental Security Policy
- Security Awareness and Training Policy

COMMENTS FROM BOARD MEMBERS

CLOSING REMARKS

New Action Item Review	Jason Hildebrandt, OITS

ADJOURNMENT

NOTE: Any individual with a disability may request accommodation to participate in committee meetings. Requests for accommodation should be made at least five working days in advance of the meeting.

Action Item Log

AI#	Topic	Date Assigned	Owner	Update

Upcoming Meetings

ITEC:

January 21, 2024

February 18, 2025

March 18, 2025

Information Technology Executive Council
Regular Meeting of the ITEC Board

MINUTES

November 12, 2024

The Regular Meeting of the ITEC Board was held on November 12, 2024, virtually using Microsoft Teams. This meeting was properly noticed and posted in the Kansas Public Square prior to the meeting. https://publicsquare.ks.gov/

Board Members:
Present unless otherwise noted

Jeff Maxon, Executive Branch CITO (Chair)
Doug Polston, Regents Representative #1
Ken Harmon, Regents Representative #2
Adam Proffitt, Cabinet Agency Head #1
Amber Shultz, Cabinet Agency Head #2
Adrian Guerrero, Non-Cabinet Agency Head #1
Lynn Retz, Non-Cabinet Agency Head #2
Keith Scott, KCJIS
Greg Gann, County Representative
Mike Mayta, City Representative
Murray McGee, Information Network of Kansas
Steve Funk, Board of Regents [Absent]
John Berghuis, Private Sector Representative [Absent]

Non-Voting Members:
Present unless otherwise noted

Senator Rick Kloos, Senate Representative [Absent]
Senator Jeff Pittman, Senate Representative [Absent]
Representative Emil Bergquist, House Representative [Absent]
Representative Pam Curtis, House Representative
Tom Day, Interim Legislative Branch CITO
Alex Wong, Judicial Branch CITO
Vacant, Chief Information Technology Architect

THIS MEETING IS IN COMPLIANCE WITH
KSA 75-7202 AND AMENDMENTS THERETO.

Public attendees

Burns, Hope [OITS]
Godfrey, John [OITS]
Finney, Vince [OITS]
Hildebrandt, Jason [OITS]
Ramirez, Celena [OITS]
Reiter, Brian [OITS]
Ramirez, Celena (OITS)
Robison, Cole [OITS]

WELCOME / CHAIRMAN COMMENTS

Jeff Maxon, E-CITO, called the meeting to order at 1:30pm.

APPROVAL OF Agenda

Jeff Maxon introduced a motion to approve the agenda. Greg Gann moved to approve the agenda. Secretary Adam Proffitt seconded the motion. The motion passed.

APPROVAL OF MINUTES

Jeff Maxon introduced the November 12, 2024, meeting minutes for discussion. Secretary Amber Shultz, moved to approve the minutes. Secretary Proffitt seconded the motion. The motion passed.

ACTION ITEM STATUS

Jason Hildebrandt, Assistant IT Architect, reported that there were no new action items.

NASCIO Presentation on IT Consolidation

Doug Robinson, Executive Director of the National Association of State Chief Information Officers, highlighted insights on IT environments and consolidation initiatives across the country.

- He highlighted the importance of consolidation and optimization, which has been a priority for state CIOs since 2007.
- Doug shared data from a recent survey involving 49 states, indicating that 90% of state CIOs operate under a chargeback model for service delivery.
- He discussed the shift from an owner-operator model to a broker model, where CIOs act on behalf of agencies to procure services, particularly cloud services.
- Doug emphasized the need for consolidation of infrastructure and services to reduce complexity and improve cybersecurity.
- He noted that challenges include organizational resistance to change, funding for consolidation efforts, and the need for clear plan and stakeholder engagement.

POLICY AND PROCEDURES DISCUSSION

John Godfrey, CISO, presented the following policies for final discussion and new polices were introduced:

- Configuration Management Policy with minor edits to clarity the expectation for coordination and reporting. Secretary Proffitt moved to approve the policy. Doug Polston seconded the motion. The motion passed.
- IT Asset Management Policy no feedback was received. Ken Harmon moved to approve the policy. Adrian Guerrero seconded the motion. The motion passed.
- Software Usage Restriction Policy no feedback was received. Greg Gann moved to approve the policy. Lynn Retz seconded the motion. The motion passed.

The upcoming policies were introduced, and feedback was encouraged on these policies:

- Information Security Program Policy
- Information Security Risk Management Policy
- Information Sharing Policy
- Vulnerability Management Policy
- Network Privilege Access Agreement

COMMENTS FROM BOARD MEMBERS

Jeff Maxon mentioned the possibility of extending future meetings to accommodate ongoing discussions and policy approvals. There was a suggestion to send out adjustments and feedback on policies between meetings to facilitate focused discussions.

CLOSING REMARKS

New Action Item Review – Jason Hildebrandt reported that there were no new action items.

ADJOURNMENT

Adrian Guerrero introduced a motion to adjourn the meeting. Ken Harmon seconded the motion.

Adjourned at 2:43 pm.

ITEC BOARD MEMBERS

Jeff Maxon
Executive Branch CITO

Doug Polston
Regents Representative

Ken Harmon
Regents Representative

Adam Proffitt
Dept of Administration

Amber Shultz
Kansas Department of Labor

Adrian Guerrero
Kansas Board of Nursing

Lynn Retz
Kansas Corporation Commission

Keith Scott
KS Criminal Justice

Greg Gann
Sedgwick County

Mike Mayta
City of Wichita

Murray McGee
Information Network of Kansas (INK)

Steve Funk
Board of Regents

John Berghuis
Private Sector Representative

NON-VOTING MEMBERS

Senator Rick Kloos
Senate Representative

Senator Jeff Pittman
Senate Representative

Emil Bergquist
House Representative

Pam Curtis
House Representative

Tom Day
Legislative Branch Interim CITO

Alex Wong
Judicial Branch CITO

Vacant
Office of Technology Services

Information Technology Executive Council (ITEC)

ITEC 7010-P

1.0 TITLE: Access Control Policy

2.0 PURPOSE: This policy establishes security requirements and ensures appropriate mechanisms for the control, administration, and tracking of access to State information assets.

3.0 SCOPE: This policy applies to all information systems, networks, applications, and data owned, operated, or managed by an Entity. It covers all access points, user interactions, and data processing methods, whether performed on-premises, remotely, or through third-party services. The policy includes all forms of access – user, system, and administrative – and applies to any devices interacting with Entity information assets, whether State-owned or personal.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, and any 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 Information Technology Executive Council (ITEC) Policy 8010-P

5.2 Kansas Statutes Annotated (K.S.A.) 75-7244, and amendments thereto

5.3 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5

6.0 DEFINITIONS:

6.1 Account Administrator: As defined in the ITEC 8010-P.

6.2 Administrator: An individual, group, or organization responsible for setting up and maintaining systems, implementing secure baseline configurations, incorporating secure settings, and conducting configuration monitoring activities.

6.3 Information Systems: A discrete set of information resources organized for collecting, processing, maintaining, sharing, or disposing of information.

6.4 Information System Account(s): Unique identifiers granting access to information systems, typically involving usernames and passwords or other authentication methods.

6.5 IT Assets: As defined in IT Asset Management Policy.

6.6 Privileged Account: An Information System Account with elevated access and permissions compared to standard user accounts.

6.7 System Service Account: A special user account that an application or service uses to interact with an Information System.

7.0 POLICY:

This policy governs access control for 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:

Account Management

7.1 Manage Information System Accounts securely and consistently through the establishment of documentation that must include:

7.1.1 Inventories of permitted account types for each Information System.

7.1.2 Assignment of Information System Account managers and backup account managers.

7.1.3 The conditions for group and role membership.

7.1.4 Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes for each account.

7.1.5 Use automated tools, where feasible, to manage Information System Accounts.

7.1.6 Establish documented procedures for creating, disabling, enabling, modifying, and removing accounts.

7.1.7 Configure Information Systems to automatically log account creation, modification, disabling, and removal transactions.

7.1.8 Define and document roles responsible for account management notifications, including:

7.1.8.1 24 hours of accounts no longer being required.

7.1.8.2 24 hours before users are terminated or transferred.

7.1.8.3 24 hours when system usage or need-to-know changes for a user.

7.1.9 Establish responsibility for ensuring accounts are disabled immediately:

7.1.9.1 New accounts that have not been logged into for thirty (30) days or more.

7.1.9.2 Login credentials in accordance with K.S.A. 75-7240(b)(2), and amendments thereto.

7.1.9.3 Accounts that are no longer associated with a user.

7.1.9.4 Accounts that have been inactive for ninety (90) days or more.

7.1.9.5 Accounts that are in violation of State or Entity policies.

7.1.9.6 Emergency and temporary accounts must be disabled or removed within 24 hours after the conclusion of the emergency or temporary need; and

7.1.9.7 Accounts of users who pose a significant security and/or privacy risk and for which reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm.

7.2 Document all changes to Information System Accounts, including creation, disabling, enabling, modification, or removal, in an auditable format.

7.3 Ensure access to Information Systems must be formally requested through a documented process and approved by authorized Entity staff.

7.4 Ensure only authorized personnel must approve access requests based on documented business needs and user role requirements.

Account Reviews and Access Controls

7.5 Conduct access reviews to ensure appropriate access levels and compliance with security policies, identifying and addressing unauthorized or outdated privileges.

7.5.1 Review user accounts annually.

7.5.2 Review privileged accounts semi-annually.

7.5.3 Review group accounts or shared user IDs annually.

7.5.4 Change shared authenticators immediately when members are removed from the share or group account.

7.6 Restrict and control the use of Privileged Accounts, limiting their number and access to the minimum necessary, and ensuring all privileged access is logged and auditable.

7.7 Implement continuous monitoring of access logs for all critical systems or systems that process, store, or transmit Restricted Use Information (RUI) to detect unauthorized access attempts and anomalies.

Account Creation and Registration

7.8 Establish and document the formal account creation and registration processes that include:

7.8.1 Ensuring user IDs are unique and not shared.

7.8.2 User IDs are granted to a specific user only and must not be used by anyone but the individual to whom they have been issued.

7.8.3 Prohibit group accounts and shared IDs unless documented and approved by the Entity Information Security Officer or their designee, with an associated risk assessment and justification.

7.8.4 Provide access strictly according to job description, function, or role, ensuring access is granted on a “need-to-know” or “need-to-use” basis.

7.8.5 User accounts must be configured to allow periodic review by the Entity Information Security Officer and the Account Administrator through reports, dashboards, or other appropriate means.

7.8.6 Access control rules and rights for each user or group of users must be defined and documented.

7.8.7 Users must be forced to change the password during the initial login sequence.

Vendor and Contractor Access

7.9 Require a signed contract defining scope, terms, duration, and conditions of access before granting access to vendors or contractors.

7.10 Require a fully executed nondisclosure agreement (NDA) before granting access to vendors or contractors.

Privileged Access Management

7.11 Restrict Privileged Accounts to the minimum required for successful management and operation.

7.12 Require and enforce Multi-Factor Authentication (MFA) for all privileged access.

7.13 Ensure privileged access actions are traceable to unique user accounts.

7.14 Require users with privileged access to undergo special training and sign the Network Privilege Access Agreement.

7.15 Implement the same process for granting privileged access as the user registration procedure.

7.16 Ensure that user IDs do not give any indication of the user's privilege level (i.e., administrator).

7.17 Require privileged accounts are used only for duties or actions that require elevated privileges.

7.18 Ensure all privileged access is logged and audited.

7.19 Ensure privileged accounts must not have an email account or mailbox provisioned or associated with them.

System Service Accounts

7.20 Ensure System Service Accounts must be approved and documented for proper business use before creation.

7.21 Review and approve all System Service Accounts annually.

Data Flow Control and Separation of Duties

7.22 Control data flow within and between Information Systems, including segmentation, access controls, and security tools to protect data in transit and at rest.

7.23 Enforce segregation of duties to prevent any single individual from having control over all critical access control aspects, including account creation, privilege assignment, and access review.

7.24 Identify duties that create the potential for malevolent activity without collusion.

7.25 Define and document system access authorizations to support separation of duties.

7.26 Immediately disable the account involved in an access control violation. Report the incident to the Entity Information Security Officer after which an investigation must be conducted.

Least Privilege and Login Attempt Limitations

7.27 Enforce the principle of least privilege, limiting access to what is necessary for job functions and explicitly authorizing access to security functions.

7.28 Limit unsuccessful login attempts to five (5) within a 10-minute period, locking accounts for 30 minutes or until manually released by:

7.28.1 An Administrator,

7.28.2 An authorized service desk member, or

7.28.3 The user via an Entity-defined challenge question or password reset process.

7.29 Log all unsuccessful logon attempts and password resets.

7.30 Configure Information Systems to prevent non-privileged users from executing privileged functions or disabling, circumventing, or altering security safeguards.

System Use Notification Banners and Session Locks

7.31 Configure systems to display Entity-defined system use notifications with privacy and security notices consistent with applicable laws, executive orders, circulars, directives, policies, regulations, standards, and guidance.

7.31.1 Ensure the system use banner states the following:

7.31.1.1 Users are accessing an information system owned by the State of Kansas.

7.31.1.2 Information System usage may be monitored, recorded, and subject to audit.

7.31.1.3 Information System usage may be disrupted, delayed, or blocked as part of security operations.

7.31.1.4 Unauthorized use of the State Information System is prohibited and subject to criminal and civil penalties.

7.31.1.5 Use of the State Information System indicates consent to monitoring and recording.

7.32 Ensure that publicly accessible systems:

7.32.1 Display system-use information and conditions before granting further access.

7.32.2 Display references, if applicable, to monitoring, recording, or auditing that align with privacy accommodations for such systems.

7.32.3 Include a description of the authorized uses of the system.

7.33 Ensure system-use banners remain until the user acknowledges usage conditions.

7.34 Each Entity must configure session locks on Information Systems to automatically log out a user after 30 minutes of inactivity. Reauthentication must be required to reactivate any local, network, or remote access session.

7.35 For publicly accessible Information Systems, Entities must document the types of authorized actions that can be performed without identification and authentication. Each Entity may decide that there are no user actions that can be performed on Entity systems without identification and authentication.

Public Access and Information Posting

7.36 Designate authorized individuals for posting information to the Entity's public webpages and social media platforms.

7.36.1 Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

7.37 Ensure content is reviewed to exclude non-public information prior to posting.

7.38 Conduct quarterly reviews of the Entity's content on public webpages and social media and remove information that is non-public.

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.

Final Action on Security Policies

Information Technology Executive Council

[DRAFT] Policy XXXX-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.

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

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.

Encryption and Key Management

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

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

7.8 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.

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

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

7.11 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

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

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

7.12.2 Version: Track different versions and deprecation schedules.

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

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

7.12.5 Authorization Controls: Access control mechanisms restricting unauthorized access.

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

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

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

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

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

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

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

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

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

Cloud Migration and Logging

7.14 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.

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

7.16 Centralize logs, store them securely, and retain them according to the retention policy.

7.17 Ensure copies of all available logs are sent to the Kansas Information Security Office (KISO) Security Operations Center (SOC).

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

Entities using IaaS, must:

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

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

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

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

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

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

7.21.1 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.

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

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

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

7.25 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.

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

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

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

7.29 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.

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

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

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

7.33 Use resource tagging to track the usage and cost of IaaS resources by project, department, or application. Ensure that resource allocation aligns with business priorities and that unnecessary resources are decommissioned promptly.

7.34 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.

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

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

7.37 Ensure container images are fully patched before deployment.

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

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

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

Entities using PaaS, must:

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

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

7.43 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.

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

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

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

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

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

7.48 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).

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

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

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

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

7.53 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.

Entities using SaaS, must:

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

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

7.56 Implement and enforce Multi-Factor Authentication (MFA) for all users accessing SaaS applications, especially those with access to RUI or administrative functions.

7.57 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.

7.58 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.

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

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

7.61 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.

7.62 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.

7.63 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

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Identification and Authentication Management Policy

2.0 PURPOSE: This policy establishes minimum requirements for implementing identification, authentication, and authorization controls to ensure only authorized individuals, systems, and processes can access Information Assets and Information Systems.

3.0 SCOPE: This policy applies to all systems, including but not limited to internet applications, VPN infrastructure, load balancers, domain controllers, telephony systems, and any other services accessible from the internet. It applies to privileged and non-privileged accounts, contractors, third-party service providers, and external users who interact with or utilize these systems and services.

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 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, as amended

5.2 NIST Special Publication (SP) 800-53 Revision 5, as amended

6.0 DEFINITIONS:

6.1 Authenticators: Include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.

6.2 Cryptographic Module: A set of hardware, software, and/or firmware implementing security functions, including cryptographic algorithms and key generation methods, within a defined boundary.

6.3 Device Authenticators: Include certificates and passwords.

6.4 Identity Proof: The process of collecting, validating, and verifying a user's identity information to establish credentials for system access.

6.5 IT Asset: As defined in the IT Asset Management Policy.

6.6 Mission Critical Information Systems: Systems where loss, misuse, disclosure, unauthorized access, or modification of information would significantly impact an Entity's core mission.

6.7 Multi-Factor Authentication: An authentication system requiring more than one distinct factor for successful authentication, such as something you know (password), something you have (token), something you are (biometric), or somewhere you are (geolocation).

6.8 Organizational User: An Employees or individuals with employee-like status, such as contractors, volunteers, or detailees from other Entities.

6.9 Non-Organizational User: Individuals or Entities interacting with public-facing systems to complete Entity transactions.

6.10 Privileged Accounts: As defined by the Access Control Policy.

7.0 POLICY: This policy governs the management of identification and authentication for Information System Accounts and IT Assets by all Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

Identification and Authentication

7.1 Uniquely identify and authenticate Organizational Users, associating unique identification with processes acting on behalf of the user.

7.2 Implement and enforce Multi-Factor Authentication for Organizational Users accessing:

7.2.1 Applications exposed to the Internet,

7.2.2 Contractor hosted applications, and

7.2.3 Remote access to the Entity's internal network.

7.3 Uniquely identify and authenticate desktop and laptop computers before establishing remote or network connections.

Management of System Identifiers

7.4 Document and implement processes for managing system identifiers (user-IDs and device-IDs) by:

7.4.1 Obtaining authorization from designated Entity representatives (e.g., director, manager, supervisor).

7.4.2 Selecting identifiers that identify the individual, group, role, service, or device.

7.4.3 Preventing re-use of identifiers for 10 years.

7.4.4 Managing individual identifiers according to their work status (e.g., employee, contractor).

Management of Authenticators

7.5 Implement processes for managing authenticators for individual, group, role, service, or device identifiers by:

7.5.1 Verifying identities during initial authenticator distribution.

7.5.2 Establishing initial authenticator content for Entity-issued authenticators.

7.5.3 Documenting and implementing procedures for authenticator distribution, handling lost or compromised authenticators, and revoking authenticators.

7.5.4 Changing default authenticators after initial installation.

7.5.5 Protecting authenticator content from unauthorized disclosure and modification.

7.5.6 Changing authenticators for group or role accounts when users are removed.

Password-Based Authentication Controls

7.6 Ensure Information Systems that use password-based authentication enforce the following:

7.6.1 Maintain and update a list of commonly used, expected, or compromised passwords at least every three (3) years and when passwords are suspected to be compromised.

7.6.2 Verify passwords against the list of commonly used, expected, or compromised passwords when users create or update them.

7.6.3 Transmit passwords only over FIPS 140 validated cryptographic modules.

7.6.4 Store passwords using approved salted key derivation functions, preferably using a keyed hash.

7.6.5 Require immediate selection of a new password upon account recovery.

7.6.6 Allow users to select long passwords and passphrases, including spaces and all printable characters.

7.6.7 Employ automated tools to assist users in selecting strong passwords.

7.6.8 Enforce password composition and complexity rules as outlined in Appendix A.

Public Key-Based Authentication

7.7 Ensure authorized access to private keys.

7.8 Map authenticated identities to individual or group accounts.

7.9 For public key infrastructure (PKI) use, validate certificates by verifying certification paths to trusted anchors, including checking certificate status, and maintain a local cache of revocation data.

Authentication Protection

7.10 Configure Information Systems to obscure authentication information during the logon process to prevent unauthorized use.

Re-Authentication Requirements

7.11 Configure systems to require re-authentication:

7.11.1 Upon session termination, device lock, or network termination.

7.11.2 When switching from Non-Privileged to Privileged Accounts.

7.11.3 After 15 minutes of inactivity.

7.11.4 After a password reset.

Identity Proofing

7.12 Identity-proof users requiring logical access based on system sensitivity, criticality, and applicable regulatory or contractual requirements.

7.13 Resolve user identities to unique individuals to prevent impersonation and unauthorized access.

7.14 Uniquely identify and authenticate Non-Organizational Users or processes acting on behalf of Non-Organizational Users.

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 – Minimum Password Requirements

Setting	Description	MFA Enabled	MFA Not Enabled	Service Account
Minimum Password Length	Specifies the minimum number of characters required for a user account password.	12 characters	15 characters	15 characters
Password Complexity	Ensures that new passwords meet basic complexity requirements. When this setting is enabled, passwords must meet the following minimum requirements.	Contain three (3) of four (4): • Uppercase • Lowercase • Numeral • Non-alpha	Contain three (3) of four (4): • Uppercase • Lowercase • Numeral • Non-alpha	Contain three (3) of four (4): • Uppercase • Lowercase • Numeral • Non-alpha
Minimum Password Age	Specifies the minimum number of days a password must be used before it can be changed.	1 day	1 day	1 day
Maximum Password Age	Defines the maximum number of days a password can be used before it expires.	365 days	180 days	365 days
Password History	Specifies the number of unique passwords that must be used before an old password can be reused.	24 previous passwords	24 previous passwords	24 previous passwords
Account Lockout Duration	Specifies the maximum number of consecutive failed login attempts before the account is locked.	5 attempts	5 attempts	5 attempts
Account Lockout Threshold	Specifies the length of time a locked account remains unavailable. If set to 0, it remains locked until manually unlocked by an administrator.	15 minutes or more without administrator intervention	15 minutes or more without administrator intervention	15 minutes or more without administrator intervention

Account Lockout Counter	Specifies the time period before the account lockout threshold resets to zero.	15 minutes	15 minutes

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Media Protection Policy

2.0 PURPOSE: This policy establishes requirements for protecting data in all forms and media throughout their lifecycle based on sensitivity, criticality, value, and the impact of a loss of confidentiality, integrity, and availability on applicable stakeholders.

3.0 SCOPE: This policy applies to all digital and non-digital media used to store, process, or transmit Restricted-Use Information (RUI).

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 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, as amended

5.2 NIST Special Publication (SP) 800-53 Revision 5, as amended

5.3 NIST SP 800-88 Revision 1, as amended

6.0 DEFINITIONS:

6.1 Digital Media: Includes diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

6.2 Non-Digital Media: Includes paper and microfilm.

6.3 Organizational User: As defined in the Telework Security Policy.

6.4 Sanitization: A process to remove information from media such that data recovery is not possible, including the removal of all labels, markings, and activity logs.

7.0 POLICY: This policy governs the safeguarding and sanitization of data, regardless of form or media, by all Entities. Entities may impose supplemental restrictions through their specific policies, but such policies must not contradict the provisions outlined here.

Entities must:

Clean Desk and Clear Screen

7.1 Protect digital and non-digital information from unauthorized access and disclosure.

7.1.1 Secure file cabinets or other appropriate containers when sensitive information is left unattended.

7.1.2 Clear desks during non-working hours to prevent unauthorized access and disclosure of sensitive information.

7.1.3 Ensure documents containing sensitive information are not left unattended on printers, copiers, or fax machines.

7.1.4 Invoke screen-lock before leaving secured work areas.

Media Access

7.2 Implement security measures to restrict access to digital and non-digital media to authorized personnel.

Media Marking

7.3 Mark digital and non-digital media with appropriate classification labels, distribution limitations, and handling caveats.

7.3.1 Media containing only data that is classified as Public requires no marking or labels.

7.3.2 Media marking is recommended but optional when media remains within the Entity-controlled enclave and is not transported outside.

Media Storage

7.4 Securely store digital and non-digital media.

7.5 Classify and label media to indicate the sensitivity of the information.

7.6 Use secure delivery methods with tracking for media transport.

Media Transport

7.7 Use strong encryption to safeguard sensitive information stored on digital media during transport outside controlled areas.

7.8 Enclose sensitive hard copy information in opaque, sealed envelopes or containers.

7.9 Maintain accountability and restrict transport activities to authorized personnel.

7.10 Document activities associated with the transport of system media.

7.11 Inform Organizational Users of their responsibilities and provide them with necessary tools and training to protect assets during transport.

Media Sanitization

7.12 Sanitize digital and non-digital media per NIST SP 800-88 Revision 1 before disposal or reuse.

7.13 Require Data Custodians and Data Owners to document and verify sanitization and disposal actions.

Media Use

7.14 Implement physical and logical security controls to protect the confidentiality and integrity of Entity data storage media throughout their lifecycle.

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Mobile Device Policy

2.0 PURPOSE: This policy establishes specific security requirements for mobile devices.

3.0 SCOPE: This policy applies to all mobile devices owned or leased by the Entity.

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 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, as amended

5.2 NIST Special Publication (SP) 800-53 Revision 5, as amended

6.0 DEFINITIONS:

6.1 Mobile Devices: Portable computing devices that (1) have a small form factor easily carried by a single individual, (2) operate without a physical connection (e.g., wirelessly transmit or receive information), (3) possess local, nonremovable or removable data storage, and (4) include a self-contained power source. Examples include smartphones, tablets, and e-readers.

6.2 Mobile Device Management: The administration of mobile devices such as smartphones, tablets, and laptops, typically implemented through a third-party product with management features for mobile devices.

7.0 POLICY: This policy governs mobile device security. Entities may impose supplemental restrictions through specific policies, but such policies must not contradict the provisions outlined here.

Entities must:

Mobile Device Hardening

7.1 Enforce encryption of data at rest.

7.2 Remove or render information inaccessible from mobile devices after no more than 10 incorrect authentication attempts.

7.3 Configure mobile devices to automatically lock after being idle for no more than 10 minutes.

7.4 Centralize control of mobile devices through MDM or another centralized management solution.

Mobile Device Approved Application Stores

7.5 Establish, document, and communicate a list of approved applications stores through which mobile devices may obtain approved applications.

Mobile Device Approved Applications

7.6 Establish, document, and communicate a list of approved applications for installation and use on mobile devices used for Entity business purposes.

7.7 Develop an application validation process to test for device, operating system, and application compatibility issues.

7.8 Prohibit non-approved applications from being installed on Entity-owned mobile devices or used for Entity business purposes, regardless of device ownership.

Mobile Device Application Management

7.9 Maintain all mobile applications used for Entity business at the latest vendor-supported levels.

7.10 Implement security-related updates and upgrades for all Entity-owned devices as part of their change management processes.

Mobile Device Approved Cloud Services

7.11 Establish, document, and communicate a list of approved cloud services for use with mobile devices for Entity business purposes.

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

7.13 Prohibit the use of personal email accounts, personal storage accounts, and other personal cloud services for Entity business purposes.

Mobile Device Backup

7.14 Establish mechanisms and requirements to back up mobile devices to mitigate the risk of losing Entity information.

7.15 Prohibit backing up Entity information to personal computers, personal storage devices, and personal cloud services.

Mobile Device Security Awareness Training

7.16 Provide training and awareness activities for mobile device users on threats and recommended security practices, incorporating them into the Entity's security and awareness training.

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.

Security Policies for Discussion

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Acceptable Use of IT Policy

2.0 PURPOSE: This policy establishes minimum requirements for the acceptable use of IT Resources to protect users and IT Resources. Inappropriate use exposes the State network to risks such as ransomware, viruses, system compromises, data breaches, and legal liabilities. This policy does not cover every possible scenario and does not relieve anyone accessing an IT system from their obligation to exercise good judgment.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers who access, manage, or maintain IT Resources on behalf of the State of Kansas. It covers all activities related to the use, management, and security of IT Resources, including hardware, software, networks, and data.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 K.S.A. 21-5611

5.2 K.S.A. 21-5839

5.3 K.S.A. 21-6002

5.4 NIST CSF 2.0

6.0 DEFINITIONS:

6.1 Information Resources: Information and related resources, such as the internet, personnel, equipment, funds, and IT Assets.

6.2 IT Assets: The hardware, software, data, and other technology components that make up the IT infrastructure of an Entity.

6.3 Organizational Users (Users): As defined in Security and Privacy Awareness Training Policy.

6.4 System Owner: The individual or department responsible for the overall ownership, operation, and security of a particular IT system.

7.0 POLICY: This policy governs security-focused configuration management for all Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

7.1 Ensure Organizational Users are individually responsible for appropriate use of IT Resources assigned to them.

7.2 Ensure IT Resources are provided for official business purposes. Organizational Users must only access IT Resources necessary for their assigned duties.

7.3 Ensure Organizational Users do not attempt to access or provide resources to access restricted portions of the network, operating systems, security software, or administrative applications without prior authorization from the System Owner or delegate.

7.4 Prohibit Organizational Users from using IT Resources for illegal or unlawful purposes, including but not limited to copyright infringement, personal gain, libel, slander, fraud, defamation, forgery, impersonation, and spreading malware.

7.5 Ensure Organizational Users maintain the security and confidentiality of information, safeguarding login credentials, and securing Restricted-Use Information per ITEC security policies. Unauthorized access, sharing, or disclosure of Restricted-Use Information is prohibited.

7.6 Inform Organizational Users that there is no expectation of privacy when using State-issued IT Resources. All usage, including emails, messaging, internet activity, and data storage, may be monitored to ensure policy compliance and security operations.

7.7 Ensure Organizational Users return all IT Assets and associated data upon separation from employment or contract termination.

7.8 Prohibit Organizational Users from using State-owned licensing keys on personal devices without approval from the CITO or delegate.

7.9 Prohibit Organizational Users from storing Entity data on non-State cloud platforms or non-State data storage locations.

7.10 Ensure Organizational Users do not use personal devices to access IT Resources unless authorized and secured in compliance with State IT policies.

7.11 Inform that violations of this policy by contractors or third-party service providers must result in termination of contracts and/or legal action.

7.12 Ensure Organizational Users do not use State IT Resources to engage in personal social media activity. Official communication via social media must comply with applicable policies.

7.13 Ensure Organizational Users immediately report any event that threatens the availability, integrity, or confidentiality of IT Resources or data, violates policies, or contravenes applicable laws, to the Kansas Information Security Office (KISO) or Entity Information Security Officer (ISO).

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 Violations must be documented and reported to KISO.

9.3 Repeated or serious breaches may result in suspension of IT access or further legal action.

9.4 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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: IT Maintenance Security Policy

2.0 PURPOSE: The purpose of this policy is to ensure IT Assets are properly maintained to minimize risks from emerging information security threats and prevent the potential loss of confidentiality, integrity, or availability due to system failures.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers who manage or maintain IT Assets on behalf of the State of Kansas. It covers all maintenance-related activities to ensure the proper function and security of IT Assets.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 NIST SP 800-53 R5

5.2 NIST CSF 2.0

6.0 DEFINITIONS:

6.1 IT Assets: Hardware, software, data, and other technology components that make up the IT infrastructure of an Entity.

6.2 Nonlocal Maintenance: Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

7.0 POLICY: This policy governs maintenance activities for IT Assets by all Entities. Entities may implement supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

Controlled Maintenance

7.1 Schedule, document, and review records of maintenance, repair, and replacement on system components according to manufacturer or vendor specifications and/or Entity requirements.

7.2 Approve and monitor all maintenance activities, whether performed on-site or remotely, and whether the system or components are serviced on-site or removed to another location.

7.3 Explicitly approve the removal of systems or system components from Entity facilities for off-site maintenance, repair, or replacement.

7.4 Sanitize equipment to remove Restricted-Use Information from associated media before removal from Entity facilities for off-site maintenance, repair, or replacement.

7.5 Verify that all potentially impacted controls are functioning properly following maintenance, repair, or replacement activities.

7.6 Include the following information in maintenance records:

7.6.1 Date and time of maintenance.

7.6.2 Description of maintenance performed.

7.6.3 Names of individuals or groups performing maintenance.

7.6.4 Name of escort.

7.6.5 System components or equipment that is removed or replaced.

7.7 Ensure all maintenance activities must be logged and audited regularly to verify compliance with this policy.

7.8 Maintenance logs must be reviewed periodically by designated personnel to identify unauthorized activities or inconsistencies.

7.9 Ensure maintenance activities must be coordinated with the Entity's risk management and/or change management processes to identify, assess, and mitigate potential risks to system integrity and security.

7.10 Establish communication protocols for reporting incidents or issues that arise during or following maintenance activities.

Maintenance Tools

7.11 Approve, control, and monitor the use of system maintenance tools.

7.12 Review previously approved system maintenance tools at least annually.

7.13 Inspect maintenance tools used by personnel for unauthorized modifications and ensure the latest software updates and patches are installed.

7.14 Check media containing diagnostic and test programs for malicious code before use in systems.

7.15 Prevent the removal of maintenance equipment containing Entity information by:

7.15.1 Verifying no Restricted-Use Information is contained on the equipment.

7.15.2 Sanitizing or destroying the equipment.

7.15.3 Retaining the equipment within the facility.

7.15.4 Obtaining a documented exemption from the Kansas Information Security Office (KISO) or Entity Information Security Officer (ISO), authorizing removal of the equipment.

Nonlocal Maintenance

7.16 Approve and monitor Nonlocal Maintenance and diagnostic activities.

7.17 Allow the use of Nonlocal Maintenance and diagnostic tools only when consistent with ITEC policy and documented in the system security plan.

7.18 Employ strong authentication for establishing Nonlocal Maintenance and diagnostic sessions.

7.18.1 Require strong authenticators resistant to replay attacks and employing multi-factor authentication, such as PKI certificates stored on a token protected by a password, passphrase, or biometric.

7.19 Maintain records for Nonlocal Maintenance and diagnostic activities.

7.20 Terminate sessions and network connections when Nonlocal Maintenance is completed.

Maintenance Personnel

7.21 Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance personnel or organizations.

7.22 Verify that non-escorted personnel performing maintenance possess required access authorizations.

7.23 Designate Entity personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel without the required authorizations.

Timely Maintenance

7.24 Obtain maintenance support and/or spare parts for Mission Critical Systems and system components consistent with Entity defined Recovery Time Objectives (RTOs).

Field Maintenance

7.25 Restrict or prohibit field maintenance on IT Assets that have been deployed to remote locations.

7.26 Maintain records for Field Maintenance and diagnostic activities.

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Personnel Security Policy

2.0 PURPOSE: The purpose of this policy is to ensure that Executive Branch personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers involved in managing or accessing Information Systems on behalf of the State of Kansas. It ensures that personnel security standards are followed at all levels of the organization.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 K.S.A. 75-3707e

5.2 K.S.A. 75-7240(b)(2)

5.3 K.S.A. 75-7241

5.4 K.S.A. 75-2949(f)

5.5 NIST CSF 2.0

5.6 NIST SP 800-53 R5

6.0 DEFINITIONS:

6.1 Information Systems: Systems used to process, transmit, or store data and information, including hardware, software, networks, and cloud services.

6.2 Organizational Users: As defined in the ITEC Security and Privacy Awareness Training Policy.

7.0 POLICY: This policy governs personnel security standards for all Entities. While Entities may establish supplemental restrictions through their specific policies, these must not contradict the provisions outlined in this policy.

Entities must:

Position Designations

7.1 Assign risk designations to all positions based on an evaluation of the duties and responsibilities and the potential impact on information security.

7.2 Establish screening criteria for Organizational Users based on position risk.

7.3 Review and update position risk designations when recruitment actions occur or when position descriptions are updated.

Personnel Screen

7.4 Screen Organizational Users before granting initial access to Information Systems.

7.5 Rescreen Organizational Users in accordance with position risk designations or when roles or designations change, or when rescreening is required.

Personnel Termination

7.6 Upon termination of Organizational User employment:

7.6.1 Disable login credentials on the same day the Organizational User ends employment.

7.6.2 Terminate or revoke all authenticators and credentials associated with the individual.

7.6.3 Conduct exit interviews that include a discussion of the confidentiality of Restricted-Use Information.

7.6.4 Retrieve all security-related property, including authentication tokens, system manuals, keys, passwords, and identification cards.

7.6.5 Retain access to Entity information and systems previously controlled by the terminated individual.

7.6.6 Monitor for unauthorized access attempts by terminated personnel for a period of 30 days following termination to detect any potential security breaches.

Personnel Transfers

7.7 Review and confirm the need for current logical and physical access authorizations when individuals are reassigned or transferred within the Entity.

7.8 Initiate additional screening when required by position risk designations.

7.9 Modify access authorizations as needed to correspond with the reassignment or transfer.

7.10 Notify personnel responsible for logical and physical access administration no less than five (5) business days before the Organizational User's transfer.

Access Agreements

7.11 Develop and document access agreements for Information Systems.

7.12 Review and update access agreements annually.

7.13 Ensure individuals sign appropriate access agreements before being granted access to Information Systems, acknowledging their understanding of the system constraints.

7.14 Require re-signing of access agreements when updates are made or at least annually to maintain access.

External Personnel

7.15 Establish documented personnel security requirements, including roles and responsibilities, for external providers.

7.16 Ensure external providers comply with personnel security policies and procedures.

7.17 Ensure that external contractors or vendors complete onboarding procedures, including background checks, security training, signing access agreements, and signing non-disclosure agreements (NDAs), before gaining access to Information Systems.

7.18 Require external providers to notify Entity leadership of personnel transfers or terminations of external staff who possess organizational credentials or system privileges, within timeframes defined by ITEC policy.

7.19 Ensure that temporary access to Information Systems or facilities by external providers or contractors is limited to the duration of the specific project or need. Temporary access must be immediately revoked upon completion of the work or when no longer required.

7.20 Monitor provider compliance with personnel security requirements.

Personnel Sanctions

7.21 Implement a formal sanctions process for individuals who fail to comply with established information security and privacy requirements.

Position Descriptions

7.22 Incorporate security and privacy roles and responsibilities into position descriptions.

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Physical and Environment Security Policy

2.0 PURPOSE: This policy establishes requirements to ensure that Entities' information assets are protected by physical controls to prevent tampering, damage, theft, or unauthorized physical access.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers who manage or access IT systems and facilities on behalf of the State of Kansas.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 NIST CSF 2.0

5.2 NIST SP 800-53 R5

6.0 DEFINITIONS:

6.1 Controlled Areas: Collective term for Operations and Restricted Access Zones.

6.2 Operations Zone: A general access area where Entity business activities or support services are regularly conducted.

6.3 Restricted Access Zone: An area that requires specific authorization granted by the owner of each restricted zone, including data centers, server rooms, cable cabinets, and communication equipment rooms.

7.0 POLICY: This policy governs physical and environmental security measures for protecting information and information systems. Entities may establish supplemental restrictions, but these must not contradict this policy.

Entities must:

Physical Access Authorizations

7.1 Develop, approve, and maintain a list of individuals authorized to access Controlled Areas. When hosting is outsourced, ensure vendors maintain similar lists for Restricted Access Zones.

7.2 Annually review and approve access lists to Controlled Areas.

7.3 Remove access (including from the access list, keys, badges, and combination changes) when it is no longer required or upon termination.

7.4 Develop and implement procedures for reporting and responding to physical security breaches or incidents, which must include immediate notification to the appropriate Entity incident response teams.

7.5 Implement procedures for issuing, tracking, and auditing physical access credentials, including keys and badges.

7.5.1 Lost or stolen credentials must be reported immediately, and replacement credentials must be issued only after verification of need.

Physical Access Controls

7.6 Enforce access authorizations at entry and exit points of Controlled Areas by:

7.6.1 Verifying individual access authorizations before granting access.

7.6.2 Controlling ingress and egress to the facility using physical access control systems, devices, or guards.

7.7 Maintain visitor logs for Restricted Access Zones.

7.8 Escort visitors and monitor their activity within Restricted Access Zones.

7.9 Secure unused IT assets by moving them to designated secure areas if not in use for extended periods.

7.10 Change combinations and/or keys annually or when combinations are compromised, or personnel are transferred or terminated.

7.11 Annually inventory keys used for securing Restricted-Use Information.

7.12 Conduct physical security risk assessments at least annually to identify vulnerabilities and ensure the adequacy of physical controls.

7.12.1 Risk assessments must be documented, and any identified gaps must be addressed through remediation plans.

7.13 Ensure that third-party vendors and contractors comply with physical and environmental security requirements. Contracts with external providers must include provisions for physical security compliance.

7.14 Ensure that appropriate signage is placed at all entry points to Restricted Access Zones, informing personnel and visitors of access restrictions.

7.14.1 Signage must also indicate emergency procedures, such as the location of emergency exits and emergency shutoff controls.

Access Control for Output Devices

7.15 Control physical access to output devices like printers, scanners, fax machines, and copiers to prevent unauthorized individuals from accessing output.

7.16 Control access to storage locations of output devices.

Monitoring Physical Access

7.17 Monitor physical access to public access facilities where IT assets reside to detect and respond to physical security incidents.

7.18 Review physical access logs monthly or upon the occurrence of a potential security event.

7.19 Coordinate results of reviews with the Entity incident response team.

7.20 Audit physical and environmental controls, including access control systems, power systems, fire detection and suppression systems, and other environmental protections, at least annually to ensure they are functioning as intended.

7.20.1 Audit results must be documented, and any deficiencies must be promptly addressed.

7.21 Conduct a post-incident review after any physical or environmental security incident to identify weaknesses in controls, improve security measures, and document lessons learned.

7.21.1 Post-incident review results must be shared with relevant stakeholders and Entity leadership.

Visitor Access Records

7.22 Maintain visitor access records for Controlled Areas in compliance with retention requirements. Records must include:

7.22.1 Name and organization of the visitor.

7.22.2 Visitor's signature.

7.22.3 Picture ID verification and initials of the verifying guard or person.

7.22.4 Date of access.

7.22.5 Time of entry and departure.

7.22.6 Purpose of visit.

7.22.7 Name of the person visited.

7.23 Review visitor access records monthly.

7.24 Report any anomalies in visitor access records to security personnel.

Delivery and Removal

7.25 Develop procedures for the delivery and removal of IT assets to and from Entity facilities.

7.26 Authorize, monitor, and control the shipment and removal of equipment from facilities and maintain records of those items.

Power Equipment and Cabling

7.27 Protect power equipment and cabling from damage and destruction.

Emergency Shutoff

7.28 Ensure that data centers have the ability to shut off power in emergency situations.

7.29 Protect emergency shutoff systems from unauthorized activation.

Emergency Power

7.30 Ensure emergency power systems are implemented to provide continuous power and protect against power surges.

Emergency Lighting

7.31 Maintain automatic emergency lighting that activates during power outages and covers emergency exits and evacuation routes.

Fire Protection

7.32 Ensure fire detection and suppression systems are maintained and supported by independent power sources.

Environmental Controls

7.33 Maintain temperature and humidity controls within service level agreements (SLA) in data centers.

7.34 Monitor and alert facility management and IT personnel in the event of significant temperature changes.

7.35 Ensure redundant humidity, ventilation, and air conditioning systems are implemented for continuous operation.

Water Damage Protection

7.36 Protect data centers from water damage by providing master shutoff or isolation valves that are accessible, functional, and known to key personnel.

Location of IT Assets

7.37 Position IT assets within facilities to minimize damage from physical and environmental hazards and unauthorized access.

Asset Monitoring and Tracking

7.38 Implement asset location tracking technologies to monitor the location and movement of unattended IT assets.

Facility Location

7.39 Consider physical and environmental hazards when selecting locations for storing, processing, or transferring Restricted-Use Information and Mission Critical Information Systems.

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 **TITLE:** Security Awareness Training Policy

2.0 **PURPOSE:** The purpose of this policy is to identify and reduce security and privacy risks to Entities by establishing and maintaining an information security awareness program that promotes security-conscious behavior and skills among the workforce to mitigate cybersecurity and privacy risks.

3.0 **SCOPE:** This policy applies to all Organizational Users, contractors, and third-party service providers who access or manage IT Assets on behalf of the State of Kansas.

4.0 **ORGANIZATIONS AFFECTED:** This policy applies to all State of Kansas 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 K.S.A. 75-7240(b)

5.2 House Substitute for Senate Bill 291 (2024)

5.3 NIST CSF 2.0

5.4 NIST SP 800-53 R5

6.0 **DEFINITIONS:**

6.1 Organizational Users or Users: An employee or individual with similar status, such as interns, contractors, volunteers, or individuals from another Entity.

7.0 **POLICY:** This policy is the principal governing authority for security and privacy awareness training for all Entities. Entities may impose additional restrictions through Entity-specific policies, but these must not contradict this policy.

Entities must:

Information Security and Privacy Training

7.1 Provide onboarding security awareness training to all new Organizational Users before granting access to IT Assets. The training must include at a minimum:

7.1.1 Entity security and privacy policies, standards, and procedures.

7.1.2 Authentication credential security and management.

7.1.3 Social media acceptable use.

7.1.4 Social engineering awareness.

7.1.5 Artificial intelligence (AI) and associated threats.

7.1.6 Acceptable Use of Information Technology.

7.1.7 Physical security measures.

7.1.8 Risks and best practices associated with mobile device usage.

7.1.9 Multifactor authentication (MFA).

7.1.10 Incident response.

7.1.11 Regulatory compliance requirements.

7.2 Reassess security awareness and privacy training needs when Organizational Users change roles.

7.3 Provide annual security awareness training to all Organizational Users. The training must include at a minimum:

7.3.1 Entity security and privacy policies, standards, and procedures.

7.3.2 Authentication credential security and management.

7.3.3 Social media acceptable use.

7.3.4 Social engineering awareness.

7.3.5 Artificial intelligence (AI) and associated threats.

7.3.6 Acceptable Use of Information Technology.

7.3.7 Physical security measures.

7.3.8 Risks and best practices associated with mobile device usage.

7.3.9 Multifactor authentication (MFA).

7.3.10 Incident response.

7.3.11 Regulatory compliance requirements.

7.4 Employ techniques to enhance security and privacy awareness.

7.5 Update training and awareness content annually or more frequently as needed.

7.6 Incorporate lessons learned from internal or external security or privacy incidents into training and awareness techniques.

7.7 Provide practical exercises in training that simulate events and incidents.

7.8 Provide training on recognizing and reporting indicators of insider threat.

7.9 Provide training on recognizing and reporting instances of social engineering.

Simulations

7.10 Conduct regular phishing and/or social engineering simulations to assess Organizational Users' awareness and response to such threats.

7.10.1 The results of these simulations must be used to enhance training content and address identified weaknesses.

Role-Based Training

7.11 Provide role-based security training for all Organizational Users assigned specific information security and/or privacy roles, responsibilities, or duties.

7.12 Provide specific training for telework users before permitting telework and annually thereafter.

7.13 Update role-based training content annually or as needed, incorporating lessons learned from internal or external incidents.

7.14 Ensure that temporary workers, interns, and contract personnel receive security awareness training tailored to their role and access level.

Training Records

7.15 Document and monitor all information security and privacy training activities, including role-based training.

7.16 Retain individual training records in accordance with records retention schedules.

7.17 Third-party service providers must participate in security awareness training programs as specified by the Entity.

7.18 Vendors and contractors must provide documentation of their training compliance, which must be retained according to records retention schedules.

Training Feedback and Effectiveness

7.19 Track the effectiveness of training programs through metrics such as completion rates, simulation performance, and post-training incident rates.

7.20 Provide feedback and training results and metrics to senior Entity management and Entity Information Security Officer (ISO) quarterly.

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.