Information Technology Executive Council (ITEC)

NOTICE OF PUBLIC MEETING

REGULAR MEETING OF ITEC
Tuesday, October 15, 2024 – 1:30pm – 2:30pm

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

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 J.R. Claeys, Senate Representative
Senator Jeff Pittman, Senate Representative
Representative Emil Bergquist, House Representative
Representative Pam Curtis, House Representative

Tom Day, Interim Legislative Branch CITO
Anne Johnson, Interim Judicial Branch CITO
Alex Wong, 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

September 3, 2024

Introduction of PMM Graduates

ACTION ITEM STATUS

Action Item Review

Alex Wong, CITA

SENATE BILL 291 – CONSULTATION SERVICES

Statement of Work Discussion

Jeff Maxon, E-CITO

POLICY AND PROCEDURES DISCUSSION

John Godfrey, E-CISO

Final Action on Security Policies

- Access Control Policy
- Remote Access Security Policy
- Critical Vulnerability Patching Policy
- Domain Name Policy
- IT Enterprise Security Policy

Security Policy Discussion

- Telework Security Policy
- Cloud Security Policy
- Configuration Management Policy
- Identification and Authentication Management Policy
- IT Asset Management Policy
- Media Protection Policy
- Mobile Device Policy
- Software Usage Restrictions Policy

Introduction of 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

Alex Wong, CITA

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
1	Provide Statement of work (SOW) for RFP of IT consolidation plan for ITEC review	8/13/2024	Alex Wong	This action is completed as the SOW will be discussed in the October ITEC meeting.

Upcoming Meetings

ITEC:

November 12, 2024

December 17, 2024

January 21, 2025

Kansas Information Technology Executive Council

Information Technology Executive Council
Regular Meeting of the ITEC Board

MINUTES

September 3, 2024

The Regular Meeting of the ITEC Board was held on September 3, 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 [Absent]
Adrian Guerrero, Non-Cabinet Agency Head #1
Lynn Retz, Non-Cabinet Agency Head #2

Vacant, KCJIS [Absent]
Greg Gann, County Representative
Mike Mayta, City Representative
Murray McGee, Information Network of Kansas
Steve Funk, Board of Regents
John Berghuis, Private Sector Representative [Absent]

Non-Voting Members:
Present unless otherwise noted

Senator J.R. Claeys, 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
Anne Johnson, Interim Judicial Branch CITO
Alex Wong, Chief Information Technology Architect

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

Public attendees, that signed in.

Abraham, Mark [OITS]
Atwood, Charlene [OITS]
Burns, Hope [OITS]
Denning, Allie [OITS]
Finney, Vince [OITS]
Godfrey, John [OITS]
Hildebrandt, Jason [OITS]
Ramirez, Celena [OITS]
Reiter, Brian (OITS)
Robison, Cole [OITS]
Spinks, Sara [OITS]

WELCOME / CHAIRMAN COMMENTS

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

APPROVAL OF Agenda

Jeff Maxon introduced a motion to approve the agenda. Secretary Proffitt moved to approve the agenda. Steve Funk seconded the motion. The motion passed.

APPROVAL OF MINUTES

Jeff Maxon introduced the August 13, 2024, meeting minutes for discussion. Steve Funk, moved to approve the minutes. Ken Harmon seconded the motion. The motion passed.

ACTION ITEM STATUS

Alex Wong, CITA, reported that we do have action item from last meeting. Which is to provide the statement of work for the IT consolidation plan RFP for ITEC reviews by the next ITEC meeting.

POLICY AND PROCEDURES DISCUSSION

John Godfrey, CISO, presented the following policies for discussion:

- Access Control Policy
- Remote Access Security Policy
- Critical Vulnerability Patching Policy
- Domain Name Policy
- Telework Security Policy
- IT Enterprise Security Policy

The first policy discussed was the access control policy, which underwent some formatting changes and language clarifications. Feedback was received regarding emergency and temporary accounts, and it was decided to extend the time for disabling or removing these accounts to 24 hours after the conclusion of the emergency or temporary need. There was also discussion about accounts that have been inactive for 90 days or more, with concerns raised about faculty members who may only teach for one semester or year. It was suggested to have an exception process for such cases.

Next, the telework policy was reviewed. Changes were made to clarify that personal devices should not be connected to the entity's IT infrastructure without prior approval, and if approved, they must comply with security configurations. Concerns were raised about the feasibility of monitoring the security of personal devices, especially for adjunct faculty members who use their own devices. It was suggested to John Godfrey to revise the language to specify the use of protected networks and to address the issue in other policies.

The remote access security policy was discussed, with changes made to clarify the monitoring and logging of remote access sessions. There was also discussion about the requirement for devices to be up to date with software patches, and concerns were raised about the practicality of enforcing this requirement. It was suggested to address this issue in other policies or to ensure that there is a good program in place to keep devices updated.

Lastly, the domain name policy was reviewed. Changes were made to allow regent institutions to continue using their .edu domain names for official communications and services, if they align with security requirements. It was clarified that old domain names can be retained and redirected to the new domain, and reporting of domain usage is required.

COMMENTS FROM BOARD MEMBERS

There no comments from Board Members.

CLOSING REMARKS

New Action Item Review – Alex Wong, CITA, reported that there were no new action items.

ADJOURNMENT

Adrian Guerrero introduced a motion to adjourn the meeting. Secretary Proffitt seconded the motion.

Adjourned at 2:22 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

(Vacant)
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 J.R. Claeys
Senate Representative

Senator Jeff Pittman
Senate Representative

Emil Bergquist
House Representative

Pam Curtis
House Representative

Tom Day
Legislative Branch Interim CITO

Anne Madden Johnson
Judicial Branch Interim CITO

Alex Wong
Office of Technology Services

Senate Bill 291 Consulting Services Statement of Work

Background

During the 2024 legislative session, the Kansas Legislature passed the House Substitute for Senate Bill 291 (SB 291). In SB 291 the legislature asked the Executive Branch Chief Information Technology Officer (CITO-E) to develop a plan to integrate all information technology services under one agency, the Office of Information Technology Services (OITS). Currently IT staff and resources are spread across multiple cabinet agencies and several non-cabinet agencies. OITS currently provides enterprise services such as networking, telephony, cybersecurity, centralized email, and several other services to state agencies. Many agencies have not had proper IT support and funding which exposes the state to significant risk. In addition, when agencies go in their own direction with regards to IT, it reduces economies of scale increasing IT costs to the state, limits the number of resources available to support systems and solutions, and creates disparate technology stacks. The State of Kansas (SoK) needs find ways to maximize the scarce IT resources, better secure, and leverage economies of scale to reduce costs and reduce technological debt to provide the best citizen services possible.

Purpose

The purpose of this Task Order (TO) is to solicit bids from consulting firms to assist the CITO-E and the OITS analyze the current SoK Executive Branch IT (EBIT) landscape and develop a roadmap and plan for IT integration within Executive Branch to comply with SB 291. This effort should focus on the optimization of existing resources to better provide IT capabilities in a secure uniform fashion across the executive branch agencies. The regents institutions will be excluded from this IT integration effort. However, the regents institutions will be included in a landscape assessment of cybersecurity resources across executive branch.

Response Requirements

Vendor must:

- Answer and identify how they would accomplish each of the requirements/specifications outlined below.

1. Vendor must demonstrate experience in consulting with state government organizations and their efforts in planning and consolidating IT.

2. Propose a timeline on creating deliverables for each section outlined in 3

3. Deliverables:

3.1. Current IT Landscape Assessment

3.1.1. Governance

3.1.1.1. Analysis of state statutes, rules, policies, executive branch organizations, to understand the current rules and regulations applicable to this project.

3.1.2. Organizational Structure

3.1.2.1. Assess existing IT organization structures across multiple agencies

3.1.3. Architecture

3.1.3.1. Identify the varying IT architectures across multiple agencies

3.1.4. IT Service Inventory

3.1.4.1. Conduct assessment to identify all IT services provided by OITS, Executive Branch Agencies and vendors that are providing the services on behalf of the State.

3.1.5. Financial Analysis

3.1.5.1. Identify agency IT budgeting and spending for FY 2024 and FY2025

3.2. Future IT Landscape Recommendations

3.2.1. Identify and recommend an effective IT governance structure for providing service-oriented IT for the State of Kansas.

3.2.2. Recommend the optimum IT operating model and structure for the State of Kansas executive branch based on lessons learned from other states that had went through similar process.

3.2.3. Recommend and identify best practices for future state architecture including potential standardization, integration, consolidation and modernization of IT Platforms.

3.2.4. Recommend the best financial model to support State of Kansas IT operations. Financial model should address items such as leveraging federal funding, addressing capital expenditures, and addressing innovation.

3.2.4.1. Appropriation

3.2.4.2. Chargeback

3.2.4.3. Hybrid

3.3. Gap Analysis

3.3.1. Develop roadmap for the State of Kansas to identify and address the gap between current state and future state. Provide recommendations and plans, including cost and resources, for integration of IT services identified in the project plan.

3.3.1.1. Identify IT services that should be integrated and in what order they should be integrated in.

3.3.1.2. Identify what resources might be needed to perform integration of each function.

3.3.1.3. Identify missing digital services to help further enable a digital government

3.4. Cybersecurity Landscape Analysis

3.4.1. Assess the current cybersecurity landscape across executive branch to including the regents institutions in the following areas:

3.4.1.1. IT Security Services provided including but not limited to IT security capabilities and solution sets that provide these services.

3.4.1.2. Recommendations for cybersecurity solutions, tools or technology to enhance security posture for the State as a whole.

3.4.1.3. Provide an actionable roadmap to implement these recommendations.

3.5. Organizational of Change Management (OCM)

3.5.1. Change Management

3.5.1.1. Conduct change readiness assessments

3.5.1.2. Provides a plan for transition

3.5.1.3. Identify key considerations for transition

3.5.1.4. Identify staff training and retooling needs for transition

3.5.1.5. Recommend best practice model or methodology to ensure successful transition.

3.5.2. Communication Plan:

3.5.2.1. Develop a Communication Plan that addresses the lifecycle of this project including plan overview, communication objectives, approach, communication processes and stakeholder analysis.

3.5.2.2. Create a change impact assessment

3.5.2.3. This communication plan should be created and adapted to the following audience:

3.5.2.3.1. IT Staff

3.5.2.3.2. Business Stakeholders

3.5.2.3.3. Executive Branch Leadership

3.5.2.3.4. Legislators

3.5.2.4. Develop a summarize comprehensive pamphlet

3.6. Coordinating and Reporting

3.6.1. Prepare and present status updates on monthly basis to the Kansas Information Technology Executive Council throughout the project life cycle

3.6.2. Working with OITS staff, coordinating and facilitating all working group and discussions.

3.6.3. Prepare and present to legislative committees as needed

3.6.4. Develop and conduct briefings as needed

Final Action on Security Policies

Information Technology Executive Council

[DRAFT] Policy XXXX-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, as amended

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, as amended

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; and

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; and

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.

<u>Public Access and Information Posting</u>

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Critical Vulnerability Patching Policy

2.0 PURPOSE: This policy aims to reduce the organization's exposure to cyber threats by ensuring the timely application of critical patches that address issues affecting the integrity, confidentiality, and availability of information and digital assets.

3.0 SCOPE: This policy applies to all systems and devices classified as critical infrastructure designated as external facing, serving external users or entities. This includes web servers, email servers, DNS servers, VPN endpoints, load balancers, domain controllers, telephony systems, audio-visual components, land mobile radio systems, and any other systems or services accessible from the internet. The scope includes hardware, software, associated infrastructure, and third-party services integrated into the organization's external presence, as well as internal systems that support or interact with external-facing assets.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as 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 NIST Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Planning

6.0 DEFINITIONS:

6.1 Critical Infrastructure: Systems essential to the operation and security of external-facing services, whose failure or compromise would impact business continuity, data security, or public safety.

6.2 Critical Issue: A serious flaw in a system or software requiring a critical patch to mitigate risks to security, functionality, or stability.

6.3 Critical Patch: A mandatory software update released by a vendor to address critical issues that could impact the security, functionality, or stability of a system.

6.4 Critical Vulnerability: A serious weakness in a system that, if exploited, could compromise data security or functionality.

6.5 External Facing Asset: Any system or service accessible from the internet, intended for interaction with external users or entities.

6.6 Source Vendor: The company or organization that developed the resource for which the patch was released.

6.7 Patch or Update: Software applied to fix a vulnerability or coding error.

7.0 POLICY:

This policy governs critical vulnerability patching for all State of Kansas entities. Entities may impose supplemental restrictions through their specific policies, provided these do not conflict with this policy.

Entities must:

Vulnerability Identification

7.1 Continuously monitor and scan sources such as security mailing lists, vendor notifications, and KISO alerts for information on critical patches for all assets within the policy scope.

Patch Procurement

7.2 Verify the source before downloading patches and obtain patches directly from the source vendor or trusted providers whenever possible.

7.3 Scrutinize and test patches from other sources carefully before introducing them into the environment to ensure their integrity and authenticity.

Patch and Update Management

7.4 Implement an accelerated patch management process to ensure the rapid application of security patches, especially for critical and high-risk vulnerabilities.

7.5 Test patches in a controlled or limited environment before deployment.

7.6 Have a rollback plan for unsuccessful patches.

7.7 Report unsuccessful patches to the entity's change management process ~~and to the Kansas Information Security Office (KISO), as detailed in the Exceptions section~~.

7.8 Route critical patching requests through existing change control processes.

7.9 Reboot systems as soon as practically possible as required for the patch to take effect.

Vulnerability Remediation

7.10 Apply all critical patches within twenty-four (24) hours of the vendor's release to address critical issues.

7.11 Apply patches for high-risk vulnerabilities within five (5) days of the vendor's release for non-critical infrastructure that is not publicly available.

Compliance Monitoring and Reporting

7.12 Verify that patches have been applied successfully and that associated vulnerabilities have been mitigated.

7.13 Conduct regular audits or scans of external-facing assets to ensure compliance with this policy.

Exceptions

7.14 Document and report to KISO any deviations from this policy, ~~including when immediate patch deployment is not feasible due to operational constraints or compatibility issues~~.

7.15 Request exceptions in writing to the KISO office. Exceptions may only be granted by the Executive Branch CISO or their designee.

7.16 Ensure all exception requests include the following:

7.16.1 Justification for the exception.

7.16.2 Assessment of the risk associated with delaying the patch or update deployment.

7.16.3 Proposed mitigation measures to reduce the risk during the delay.

7.16.4 Timeline for patch implementation.

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: Domain Name Policy

2.0 PURPOSE: This policy establishes the mandatory use of ".ks.gov" or ".gov" domain names for all official online communications, publications, service delivery, online content design, and digital product development for covered entities within the State of Kansas.

3.0 SCOPE: This policy applies to all digital and online assets, communications, services, and content managed, developed, or utilized by entities within the State of Kansas, including official websites, web applications, email communications, online publications, and any digital products or services intended for public access or internal use by state agencies. This policy does not apply to domain names or digital assets not used for official state business or communication and not intended to represent or be associated with the State of Kansas in an official capacity. Regent institutions operating under the Kansas Board of Regents (KBOR) may continue to use their ".edu" domain names for all official online communications, publications, service delivery, online content design, and digital product development.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as 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 DOTGOV Online Trust in Government Act of 2020 (DOTGOV)

6.0 DEFINITIONS:

6.1 Alias: A second domain name that points to the first domain name. For example, an Alias for www.hello.com might be www.department.ks.gov.

6.2 Commercial Domain Name: Any domain name not maintained by the Office of Information Technology Services (OITS).

6.3 Domain Name: A unique name identifying an internet resource such as a website, consisting of alphanumeric words separated by periods.

6.4 Domain Name System (DNS): The international system for naming network resources and assigning alphanumeric names to numeric IP addresses, where domain names are registered.

6.5 HTTP Redirect: Occurs when a web server instructs a web browser to go to a different location for the requested web page. Redirects can be based on any part of the domain name.

6.6 ".gov": A first-level internet domain name controlled by the Cybersecurity and Infrastructure Security Agency (CISA).

6.7 ".ks.gov": A second-level internet domain name controlled by the Office of Information Technology Services (OITS).

7.0 POLICY:

This policy governs the use of ".ks.gov" or ".gov" domain names by all covered Entities. Entities may impose supplemental restrictions through their policies, provided these do not conflict with this policy.

Regent Institutions' Domain Use

7.1 Regent institutions may use their ".edu" domain names for official communications, information, and services, provided they align with the security requirements, guidelines, and operational standards established by the Executive Branch Chief Information Technology Officer (CITO) or their designee(s).

7.2 The use of ".edu" domains by regent institutions must be reviewed and reported annually in accordance with this policy to ensure compliance with applicable security requirements.

Entities must:

Domain Name Approval and Use

7.3 Prioritize the use of ".ks.gov" domain names over ".gov" domain names.

7.4 Obtain prior approval from the OITS CTO or their designee for purchasing, activating, or using any commercial domain name. Approval from the CISA registrar is required for ".gov" domain names when applicable.

7.5 Ensure all domain name requests have approval from the Entity's Chief Information Officer (CIO) or agency head. Requests must include:

7.5.1 A detailed description of the domain's intended use,

7.5.2 The intended audience for the domain name,

7.5.3 An explanation of why the specific domain name is needed, 7.5.4 A brief description of how this domain name will conform to all applicable policies and requirements, and

7.5.5 The name of any commercial domain name company/system being requested

7.6 Use government domain names (".ks.gov" or ".gov") for official communications, information, and services, except for third-party services operated by non-governmental entities on non-governmental domains for public interaction (e.g., social media).

7.7 Ensure that Entity systems hosted or operated by third parties comply with the requirements of this policy.

Reporting and Review Domains

7.8 Annually report all domain usage to the Chief Information Technology Architect (CITA). The report must include hostnames of internet-accessible information systems and the names of any commercial domain companies used.

7.9 The CITA must compile a consolidated report of all domain usage and provide it to the Chief Technology Officer (CTO) and the Chief Information Security Officer (CISO) for review and oversight.

7.10 The OITS CTO or their designee will review the use of non-".ks.gov" and non-".gov" domains and may require justification for continued use or direct cessation of non-compliant or inappropriate domains. Inappropriate domain names include, but are not limited to, those that are misleading, offensive, deceptive, or otherwise not reflective of the Entity's official purpose and responsibilities.

7.11 In domain name conflicts or instances of inappropriate domain names, the OITS CTO or designee will work with the involved Entities to resolve issues and may deny, not renew, or transfer domain ownership to another Entity to prevent conflicts, confusion, or reputational harm. The OITS CTO or designee reserves the right to suspend or terminate domain names that do not align with the State of Kansas's values, mission, or established guidelines.

Commercial Domain Names

7.12 The use of commercial domain names is discouraged and will be prohibited after January 1, 2025, unless a written exception is obtained in advance. Exceptions are issued by the Chief Information Security Officer (CISO) or their designee within Kansas Information Security Office (KISO) in consultation with the OITS CTO or their designee.

Aliases and Redirects

7.13 Ensure aliases that present a ".ks.gov" domain as a ".org," ".com," or other top-level domain will only be granted in limited circumstances with prior OITS approval.

7.14 Ensure redirects from “.ks.gov” must adhere to ITEC, OITS, and KISO requirements, including security, accessibility, and content standards.

7.15 Ensure redirects must not mask or hide the final destination, such as through URL shortening services.

7.16 Maintain a list of the name of the redirect, the location to which it is being redirected, and the date the redirect was made active.

7.16.1 Review this list annually to ensure the continued need and functionality of redirects.

7.17 If a redirection occurs from a “.ks.gov” or “.gov’ website to a non-“.ks.gov” or non-“.gov” website, present an exit notification or disclaimer that includes:

7.17.1 The State of Kansas cannot attest to the accuracy of a non-State of Kansas site.

7.17.2 Linking to a non-State of Kansas website does not constitute an endorsement by the State of Kansas or any of its employees of the sponsors of the information and products presented on the website.

7.17.3 You will be subject to the destination website’s privacy policy when you follow the link.

7.17.4 The State of Kansas is not responsible for Section 508 compliance (accessibility) on other websites.

Old Domain Names

7.18 Retain the old domain name indefinitely when transitioning to a “.ks.gov” or “.gov” domain name to prevent spoofing or misuse.

7.19 Monitor retained domain names for unauthorized activity.

7.20 Not use retained domain names unless for redirects.

7.21 Communicate domain name changes, transitions, or redirects to stakeholders.

7.22 Ensure redirects are removed once the retained domain is no longer in use.

Domain Registration and Contact Information

7.23 Ensure all domain names have current administrative, billing, and technical points of contact. Entities are responsible for maintaining accurate contact information.

7.24 Ensure all domain names are renewed before their expiration date to maintain continuous ownership and prevent unauthorized registration by third parties.

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: ITEC Policy 7230 – IT Enterprise Security Policy

2.0 PURPOSE: This policy establishes the foundational requirements for developing, implementing, and enforcing enterprise information technology security policies, standards, and procedures applicable to the Executive Branch. Its aim is to ensure the protection of the confidentiality, integrity, and availability of information across all Executive Branch Entities.

3.0 SCOPE: This policy applies to all Executive Branch Entities, including all information systems, networks, applications, and data owned, operated, or managed by these Entities. It encompasses all IT security practices and standards required to protect the confidentiality, integrity, and availability of information within the State of Kansas Executive Branch.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as 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 K.S.A. 75-7238

5.2 K.S.A. 2013 Supp. 75-7203 authorizes the Kansas Information Technology Executive Council (ITEC) to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state entities.

5.3 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300R1, Information Technology Security Council Charter.

6.0 DEFINITIONS:

6.1 Security Policy: A collection of mandates, actions and required documentation governing the security protections and controls of an entity.

7.0 POLICY:

7.1 Entities must implement an Information Technology Security Policy for their organization. All Information Technology Security Policies adopted by the Entity must be at least as stringent as this policy.

7.2 Entities that do not implement their own Information Technology Security Policy must adopt this policy in accordance with the standards and procedures referenced in applicable Information Technology Executive Council (ITEC) and Executive Branch IT (EBIT) Security policies.

7.3 Entities must regularly review and update their Information Technology Security Policies to address emerging threats, technological changes, and regulatory requirements.

7.4 The provisions of all Executive Branch IT (EBIT) Security Policies, insofar as they are not explicitly covered in this policy, are incorporated by reference and made an integral part of this policy. In the event of any conflict between this policy and the EBIT Security Policies, the provisions of the EBIT Security Policies shall prevail.

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: Remote Access Security Policy

2.0 PURPOSE: This policy establishes uniform security controls for remote access across all applicable Entities.

3.0 SCOPE: This policy applies to all remote access activities involving non-public State of Kansas networks, systems, applications, and services. It governs the use of remote access technologies, including Virtual Private Networks (VPNs), secure web gateways, and other methods used to connect to the State's internal networks from external locations.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, and amendments thereto

6.0 DEFINITIONS:

6.1 Information Systems: As defined in ITEC Information Security Program Policy.

6.2 Multi-Factor Authentication (MFA): An authentication method requiring two or more different pieces of evidence to confirm a user's claimed identity, such as something the user knows, has, or is.

6.3 Organizational User: An employee or individual with employee-like status, including contractors, volunteers, interns, or individuals detailed from another Entity.

6.4 Remote Access: Access to State information by users or processes communicating through external networks, such as the Internet, to non-public Entity networks.

6.5 Virtual Private Network (VPN): A secure link that uses tunneling, security controls, and endpoint address translation, simulating a dedicated line.

7.0 POLICY:

This policy governs the security of remote access to all State of Kansas Entities. Entities may impose supplemental restrictions through their policies, provided these do not conflict with this policy.

Entities must:

Remote Access Control

7.1 Strictly control remote access to non-public State networks, systems, applications, and services.

7.2 Permit authorized Organizational Users to connect remotely to conduct State-related business only through secure, authenticated, and Entity-approved access methods, with prior Entity management approval based on business needs.

7.3 Do not automatically grant access to internal networks; access must be explicitly requested by the user and approved by the system manager.

7.4 Establish and document usage restrictions, configuration requirements, and implementation guidance for each type of remote access allowed.

Monitoring and Logging

7.5 Collect and maintain logs of all remote access sessions, including session details such as time, duration, user identity, and actions performed, to support auditing and compliance reviews.

7.6 Ensure remote access is treated as a privilege and deny access to Organizational Users that pose unacceptable security or privacy risks.

Authentication and Revocation

7.7 Require MFA for all remote access to Entity Information Systems.

7.8 Revoke remote access at any time for reasons including non-compliance with security policies, request by the user's supervisor, or adverse impact on network performance due to remote connections.

7.9 Terminate remote access privileges upon an employee’s or contractor’s termination and review access upon changes in assignment or during scheduled account reviews.

7.10 Prohibit anonymous remote logins (e.g., using “guest” accounts) except on publicly accessible systems where users are anonymous.

Tunneling and Connection Controls

7.11 Implement controls to prevent split tunneling for remote devices unless necessary for Entity business and securely provisioned.

7.12 Provide remote access through technologies and methods authorized by the Executive Branch Chief Information Technology Officer (CITO) or their designee(s). Regent institutions may authorize additional methods in collaboration with CITO, provided these methods align with the security requirements, guidelines, and statewide security policies established by the Executive Branch.

7.13 Route all remote access sessions through State managed or Regent institution managed network access control points.

7.14 Implement FIPS 140-2 (or its successor) compliant encryption techniques to protect the confidentiality and integrity of remote access sessions.

Connection Criteria and Session Management

7.15 Configure remote access infrastructure to force an automatic disconnect after thirty (30) minutes of inactivity.

7.16 Configure VPN technologies to limit sessions to no more than twelve (12) consecutive hours before requiring a forced disconnect and reestablishment of the session.

7.17 Restrict remote network connections for vendors or third parties to only when needed for a valid business function and immediately deactivate access after use.

Device Security Validation

7.18 Validate the patch level and software versions of devices attempting to connect, where technically feasible.

7.19 Prevent connections until devices have the latest security patches installed, where technically feasible.

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

Kansas
Office of Information Technology Services

POLICY AND PROCEDURES MEMORANDUM
0000.00

Effective Date
Approval Date

Type of Action
New

1.0 SUBJECT: Telework Security

2.0 DISTRIBUTION: Executive Branch Information Technology Entities

3.0 FROM: John Godfrey, Chief Information Security Officer

4.0 PURPOSE:

The purpose of this policy is to define the security requirements and procedures for Organizational Users who telework to ensure the protection of the organization's information and systems.

5.0 SCOPE:

This policy applies to all Organizational Users who are authorized to telework and access the Entity's Information Systems, including but not limited to, remote access, use of personal devices, and any external connections to the Entity's networks and data. It covers all forms of data handling, system interactions, and security measures required during teleworking.

6.0 ORGANIZATIONS AFFECTED: All branches, boards, commissions, departments, divisions, and agencies of the State of Kansas, hereafter referred to as an Entity or Entities.

7.0 REFERENCES:

7.1 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, and amendments thereto

8.0 DEFINITIONS:

8.1 Information Assets: A body of information defined and managed as a single unit, so it can be understood, shared, protected, and used effectively.

8.2 IT Assets: As defined in the Executive Branch Information Technology (EBIT) IT Asset Management Policy.

8.3 Organizational User: An employee or an individual the Entity deems to have similar status of an employee, including contractors, volunteers, interns, or individuals detailed from another Entity.

8.4 Telework (telecommuting): Refers to a work arrangement where Organizational Users perform their job duties from a location other than the traditional office setting. This can include working from home, a satellite office, a coworking space, or any other location with internet access that is conducive to productivity.

9.0 POLICY:

This policy is the principal governing authority for Telework security. While individual Entities retain the right to impose supplemental restrictions through their Entity-specific policies, such policies must not contradict the provisions contained herein.

9.1 Entities must ensure authorized telework users receive security training, addressing at a minimum, the following subjects:

9.1.1 The responsibilities outlined in this policy.

9.1.2 The potential risks to the Entity's IT Assets, Information Assets, and those of other State Entities that are interconnected and/or available through the Entity's IT infrastructure.

9.1.3 Protection of authenticators, such as passwords, personal identification numbers (PINs), and hardware tokens.

9.1.4 Recognition of social engineering attack techniques and appropriate mitigation measures.

9.1.5 The consequences for disabling, altering, or circumventing the security configurations that protect State Information Assets.

9.1.6 Security incident management and breach disclosure procedures.

9.2 Authorized telework users must:

9.2.1 Adhere to all applicable information security policies, standards, and procedures regarding the use of Entity Information Assets and IT Assets, regardless of the work location.

9.2.2 Not connect personally owned IT Assets to the State or Entity's IT infrastructure at the network level.

9.2.3 Only connect to the State or Entity's IT infrastructure through Entity authorized encrypted virtual private networks (VPNs).

9.2.4 Ensure IT Assets used to connect to the Entity's IT infrastructure are physically secured.

9.2.5 Not attempt to disable, alter, or circumvent established security controls on Entity Information Assets or IT Assets used to connect to the IT infrastructure, including but not limited to endpoint protection software (anti-virus/anti-malware), host-based firewalls, and content filtering software.

9.2.6 Refrain from printing sensitive documents at home or in unsecure locations unless explicitly authorized and provided with secure printing solutions by the Entity.

9.2.7 Use only Entity-approved and managed devices for teleworking. Personally owned devices are prohibited from being used to conduct Entity business.

9.2.8 Utilize only authorized software applications for conducting Entity business. The use of unauthorized or personal software applications is prohibited.

9.2.9 Be aware that the Entity reserves the right to monitor telework activities, including but not limited to access logs, usage patterns, and data transfers, to ensure compliance with this policy and other applicable security requirements.

10.0 RESPONSIBILITIES:

10.1 Heads of Entities are responsible for establishing procedures for their organization's compliance with the requirements of this policy.

10.2 The Executive Branch CISO is responsible for the maintenance of this policy.

11.0 ENFORCEMENT:

11.1Non-compliance with this policy may result in disciplinary action, including termination of employment for severe violations.

11.2Written approval from the KISO is required for any exceptions to this policy.

12.0 HISTORY: This PPM was originally issued #_____________, dated Approval Date.

13.0 CONTACT: Chief Information Security Officer

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).

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

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

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

7.12.13Classification 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: Configuration Management Policy

2.0 PURPOSE: This policy establishes standards to ensure baseline Configuration Settings are maintained to protect the confidentiality, integrity, and availability of State information assets.

3.0 SCOPE: This policy applies to all hardware, software, and associated infrastructure, such as network devices, security appliances, and cloud-based resources. It also covers third-party services integrated into the Entity's external presence, whether managed directly or indirectly.

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 Center for Internet Security (CIS) Benchmarks, as amended

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

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

5.4 NIST SP 800-70, as amended

5.5 NIST SP 800-128 Revision 3, as amended

6.0 DEFINITIONS:

6.1 <u>Baseline Configuration:</u> A set of specifications for a system or IT Asset within a system that has been formally reviewed and agreed upon. It serves as the basis for future builds, releases, and changes and can only be altered through change control procedures.

6.2 <u>Configuration Management Plan:</u> A comprehensive description of the roles, responsibilities, and governance documents (e.g., policies, standards, guidelines, and procedures) for managing the configuration of products and systems.

6.3 <u>Configuration Settings:</u> Parameters in hardware, software, or firmware that affect the security posture and functionality of an information system.

6.4 Information Systems or System: Combinations of IT assets used for collecting, processing, maintaining, sharing, disseminating, or disposing of information or data.

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

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:

Baseline Configurations

7.1 Develop, document, and maintain Baseline Configurations for Information Systems.

7.2 Review and update Baseline Configurations at least annually or when significant changes occur.

7.3 Use automated tools, such as Security Content Automation Protocol (SCAP) or CIS Configuration Assessment Tool (CAT), to maintain currency, completeness, accuracy, and availability of baseline configurations.

7.4 Retain at least one (1) previous version of the Baseline Configuration to support rollback.

7.5 Include the Information Security Officer or their designee as a member of the Entity's change control board or similar group.

Security Impact Analysis

7.6 Analyze system changes to determine potential security and privacy impacts before implementation.

7.7 Conduct post-implementation testing to verify that controls impacted by changes operate as intended and meet security and privacy requirements.

Access Restrictions for Change

7.8 Define, document, approve, and enforce physical and logical access restrictions for changes to hardware, software, and firmware components.

Configuration Settings

7.9 Configure IT Assets securely and consistently in accordance with CIS benchmarks, NIST-recommended configurations, or U.S. government configuration baselines.

7.10 Identify, document, and authorize deviations from mandatory security Configuration Settings.

7.11 Monitor and control changes to the Configuration Settings in accordance with this policy.

7.12 Install and maintain security tools provided by the Kansas Information Security Office (KISO) on all applicable IT Assets.

7.13 Password-protect the BIOS, UEFI, or equivalent to prevent unauthorized access to low-level settings during boot.

Least Functionality

7.14 Configure systems according to the principle of least functionality, providing only mission-essential capabilities.

7.15 Prohibit or restrict ports, protocols, software, and services that are not required for business functions.

7.16 Limit component functionality to a single function per device. (e.g., email servers or web servers, but not both).

7.17 Disable insecure, unused, or unnecessary physical and logical ports/protocols to prevent unauthorized connections or data transfers.

7.18 Employ mechanisms to ensure only authorized software is executed and deny unauthorized programs.

Configuration Management

7.19 Develop, document, and implement Configuration Management Plans for Information Systems that:

7.19.1 Address roles, responsibilities, and configuration management processes.

7.19.2 Establish processes for identifying configuration items throughout the system lifecycle.

7.19.3 Define and manage configuration items for the system.

7.19.4 Are reviewed and approved by delegated management.

7.19.5 Protect the Configuration Management Plan from unauthorized disclosure and modification.

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: 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	15 minutes

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: IT Asset Management Policy

2.0 PURPOSE: This policy establishes a uniform approach to IT Asset management to ensure that components of the state network are accounted for and visible to software tools for monitoring the attack surface.

3.0 SCOPE: This policy applies to all IT assets owned, leased, or licensed 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 CIS Guide to Enterprise Assets and Software, as amended

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

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

5.4 NIST SP 1800-5, as amended

6.0 DEFINITIONS:

6.1 <u>Application:</u> A system for collecting, saving, processing, and presenting data by means of a computer. It can be executed as a component of software and is often synonymous with software application.

6.2 <u>Application Programming Interface (API):</u> A system access point or library function with a well-defined syntax, accessible from application programs or user code, providing specific functionality.

6.3 <u>End-User Devices:</u> Mobile and portable devices, such as laptops, smartphones, tablets, desktops, and workstations; a subset of IT Assets.

6.4 <u>Industrial Control System (ICS):</u> Encompasses control systems such as SCADA, DCS, and PLCs commonly found in industrial sectors and critical infrastructures.

6.5 Internet of Things (IoT): T A network of devices equipped with hardware, software, firmware, and actuators that connect, interact, and exchange data.

6.6 IT Asset: Information technology assets, including hardware, software, and firmware.

6.7 Software: Computer programs and associated data that may be dynamically written or modified during execution.

6.8 Utilities: Software that provides specific services to maintain, optimize, and enhance a computer system's functionality.

7.0 POLICY: This policy governs IT Asset Management for all State of Kansas Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

7.1 Maintain an accurate, detailed, and up-to-date inventory of all State-owned, leased, licensed, or managed IT Assets.

7.2 Inventory IT Assets, including software (applications, source code, system software, development tools, and Utilities), equipment (end-user devices, physical and virtual servers, network devices), non-computing/IoT devices (ICS, printers, physical security sensors, magnetic and optical media), and services (locally hosted, cloud computing, communications services, service accounts, and APIs).

7.3 Ensure inventories have sufficient granularity for tracking and reporting.

7.4 Review and update inventories annually and as part of installation removals and system updates.

7.5 Utilize automated tools, when possible, to maintain the currency, completeness, accuracy, and availability of inventories.

7.6 Identify and address unauthorized IT Assets promptly by removing them from the network, denying remote connections, or quarantining the assets.

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: 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 <u>Mobile Devices:</u> 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 <u>Mobile Device Management:</u> 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:

<u>Mobile Device Hardening</u>

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.

<u>Mobile Device Approved Application Stores</u>

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

<u>Mobile Device Approved Applications</u>

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.

<u>Mobile Device Application Management</u>

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.

<u>Mobile Device Approved Cloud Services</u>

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.

<u>Mobile Device Backup</u>

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.

Information Technology Executive Council

[DRAFT] Policy XXXX-P

1.0 TITLE: Software Usage Restrictions Policy

2.0 PURPOSE: This policy establishes software usage and non-standard software restrictions.

3.0 SCOPE: This policy applies to software installed on Entity IT Assets.

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 IT Asset: As defined in the IT Asset Management Policy

6.2 Organizational Users or Users: As defined in the Personnel Security Policy.

6.3 Non-Standard Software: Software not included in the Entity's officially approved suite of applications, including any software that has not undergone the formal approval process or does not conform to the Entity’s standard software lists.

7.0 POLICY: This policy governs software usage restrictions for all Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict the provisions outlined here.

Entities must:

Software Usage Restrictions

7.1 Inform Users of acceptable and unacceptable practices related to the installation and use of software, including open-source software, ensuring all licensing agreements and copyright laws are observed.

7.2 Implement controls to ensure Users comply with copyright laws and license agreements when using software.

7.3 Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

7.4 Control and document the use of peer-to-peer file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.

Non-Standard Software

7.5 Establish policies governing software installation by Users, identifying permitted and prohibited actions.

7.6 Permit software installations that include updates and security patches to existing software and downloads from Entity-approved app stores.

7.7 Prohibit software installations that include software with unknown or suspect origins or software deemed potentially malicious by the Entity.

7.8 Monitor compliance with this policy and, where technically feasible, implement automated controls to restrict Users from installing unauthorized software.

7.9 Ensure installed software programs are free of malicious code to the greatest extent possible.

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 Introduction

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 <u>Organizational Users or Users:</u> 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:

<u>Information Security and Privacy Training</u>

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.