Information Technology Executive Council (ITEC)

ITEC 7010-P

1.0 TITLE: Access Control Policy

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

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

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

5.0 REFERENCES:

5.1 Information Technology Executive Council (ITEC) Policy 8010-P

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

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

6.0 DEFINITIONS:

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

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

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

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

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

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

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

7.0 POLICY:

This policy governs access control for all State of Kansas Entities. Individual Entities may impose supplemental restrictions through their specific policies, provided these do not conflict with this policy.

Entities must:

Account Management

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

7.1.1 Inventories of permitted account types for each Information System.

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

7.1.3 The conditions for group and role membership.

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

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

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

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

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

7.1.8.1 24 hours of accounts no longer being required.

7.1.8.2 24 hours before users are terminated or transferred.

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

7.1.9 Establish responsibility for ensuring accounts are disabled immediately:

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

7.1.9.2 Login credentials are disabled the same day that any employee ends their employment with the state.

7.1.9.3 Accounts that are no longer associated with a user.

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

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

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

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

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

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

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

Account Reviews and Access Controls

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

7.5.1 Review user accounts annually.

7.5.2 Review privileged accounts semi-annually.

7.5.3 Review group accounts or shared user IDs annually.

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

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

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

Account Creation and Registration

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

7.8.1 Ensuring user IDs are unique and not shared.

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

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

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

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

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

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

Vendor and Contractor Access

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

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

Privileged Access Management

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

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

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

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

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

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

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

7.18 Ensure all privileged access is logged and audited.

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

System Service Accounts

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

7.21 Review and approve all System Service Accounts annually.

Data Flow Control and Separation of Duties

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

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

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

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

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

Least Privilege and Login Attempt Limitations

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

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

7.28.1 An Administrator,

7.28.2 An authorized service desk member, or

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

7.29 Log all unsuccessful logon attempts and password resets.

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

System Use Notification Banners and Session Locks

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

7.31.1 Ensure the system use banner states the following:

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

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

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

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

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

7.32 Ensure that publicly accessible systems:

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

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

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

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

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

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

Public Access and Information Posting

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

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

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

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

8.0 RESPONSIBILITIES:

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

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

9.0 ENFORCEMENT:

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

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

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