Information Technology Executive Council (ITEC)

ITEC 7026-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 Information Systems: As defined in the Access Control Policy.

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

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

6.8 Multi-Factor Authentication (MFA): 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).

6.9 Organizational User: As defined in the Personnel Security Policy.

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

6.11 Privileged Accounts: As defined in 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 MFA for all Privileged and non-privileged Organizational User accounts as widely as possible, where supported.

Management of System Identifiers

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

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

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

7.3.3 Preventing re-use of identifiers for 10 years.

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

Management of Authenticators

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

7.4.1 Verifying identities during initial authenticator distribution.

7.4.2 Establishing initial authenticator content for Entity-issued authenticators.

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

7.4.4 Changing default authenticators after initial installation.

7.4.5 Protecting authenticator content from unauthorized disclosure and modification.

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

Password-Based Authentication Controls

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

7.5.1 Transmit passwords only over FIPS 140 validated cryptographic modules.

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

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

7.5.4 Allow users to select long passwords and passphrases, including spaces and all printable characters, wherever possible.

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

7.5.6 Enforce password composition and complexity rules as outlined in ITEC 7026-S Identification and Authentication Management Standard.

7.5.7 Passwords are not viewable in clear text.

Public Key-Based Authentication

7.6 Ensure authorized access to private keys.

7.7 Map authenticated identities to individual or group accounts.

7.8 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 Feedback

7.9 Configure Information Systems to obscure authentication information by default during the logon process to prevent unauthorized disclosure.

Re-Authentication Requirements

7.10 Configure systems to require re-authentication:

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

7.10.2 When switching from Non-Privileged to Privileged Accounts.

7.10.3 After 15 minutes of inactivity.

7.10.4 After a password reset.

Identity Proofing

7.11 Identity Proof users that require accounts for logical access to Mission Critical and Restricted-Use Information Systems.

7.11.1 Identity Proofing is based on identity assurance level requirements as specified in applicable regulatory or contractual requirements, or applicable policies and standards.

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

7.13 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.