Document Code No.: ITG-P-21-07
Title: King County Identification & Authentication Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Identification, Authentication, IAM, Passwords, MFA
Sponsoring Agency: Department of Information Technology (KCIT)

Chief Information Officer Signature: DocuSigned by: 920AF9FCB611460...
Date signed and effective: 2/16/2021

I. Purpose:

The purpose of this policy is to establish the requirements of King County's Identification and Authentication process used for accessing technology assets. This policy replaces existing countywide password policies. This policy reflects King County's pro equity and social justice commitment. Implementation of this information security policy aligns and complies, in every regard, with King County's equity and social justice policies and practices.

II. Applicability and Audience

A. Users

This policy applies to all persons working for, or on behalf of King County, including workforce members, third parties, volunteers, and contractors accessing technology assets owned and operated by King County. These requirements apply whether the user is working at a King County facility or connecting remotely.

B. Technology Assets

This policy applies to all King County technology assets including web or "cloud" based platforms, applications, and services that are owned and operated by a service provider. This policy also applies to the use of third party or personal devices, if used to access King County's technology assets in the process of working for or on behalf of King County.

C. Exceptions

Requests for exceptions to this policy must follow the Department of Information Technology (KCIT) information security policy exceptions handling process. Please open a ticket with the helpdesk to request a policy exception.

III. Definitions

All definitions are contained within the King County Information Security Policy and Standards Glossary.

IV. Policy

A. Identity and Access Management Platforms

1. The Department of Information Technology (KCIT) is responsible for identity and access management platforms, directories, and tools utilized by King County government (e.g., Active Directory, Azure AD, Active Directory Federation Services,

Application Proxies, Microsoft Identity Management, Azure AD Privileged Identity Management, etc.) and for ensuring these systems comply with the Access Management Policy and Audit Logging and Monitoring Policy.

2. King County will utilize a single centralized identity platform administered by the Department of Information Technology (KCIT) and will provide a single set of credentials to workforce members working for or on behalf of King County. Workforce members responsible for technology asset administration and support may receive a second set of credentials dedicated to those purposes.
3. The Department of Information Technology (KCIT) will ensure that technology asset and support owners are provided appropriate rights to manage identities and/or groups of identities in the centralized identity platform for which they are authorized to manage in accordance with the Access Management Policy.
4. All technology assets must utilize King County's centralized identity and access management platform in accordance with the Access Control and Authentication Standard.
5. The Department of Information Technology (KCIT) is responsible for ensuring that identity, authentication, authorization, and access platforms and associated processes are indisputable and provide high confidence (i.e., validity cannot be challenged or denied) to the degree reasonably possible.

B. Passwords, PINS, and Biometrics

1. Passwords must meet the following minimum requirements:
   a. Must have a minimum of ten (10) or more characters (using passphrases or sentence-like passwords is encouraged and are easier to remember)
   b. Must contain at least three of the following character types: upper case, lower case, numeric, or special character
   c. Must have a minimum age of 24 hours (i.e., cannot be changed more than once per day without assistance from the helpdesk)
   d. Must have a maximum age of 90 days
   e. Cannot be the same as the username or user id
   f. Cannot be the same as any of the previous 20 passwords used
   g. Cannot be a single dictionary word
   h. Cannot be a password contained in known breaches that have been made available to the public. These passwords may be automatically rejected as invalid by identity platforms through banned password lists requiring workforce members to choose a different password.

i. Must not be displayed in its entirety while being entered except briefly as each character is entered or with a brief view that masks the password immediately after

2. PINs or personal identification numbers must meet the following minimum requirements:

   a. Must have a minimum of six (6) characters

   b. Cannot have a repeating or sequential pattern (e.g., 111111 or 123456)

   c. Must have a maximum age of 365 days

   d. Cannot be the same as the username or user id

   e. Cannot be the same as any of the previous 20 PINs used

   f. Must be authenticated by and dedicated to the device where PIN is used and be protected by cryptographic controls

   j. Must not be displayed in its entirety while being entered except briefly as each character is entered or with a brief view that masks the password immediately after

3. Biometric authentication must meet the following minimum requirements:

   a. Must be authenticated by and dedicated to the device where biometric authentication is being used and device must protect biometric identifiers with cryptographic controls

   b. Biometric identifiers may not be transmitted in any way from the device where biometric authentication is used

   c. Biometric authentication technology and use must comply with federal, state and local law

   d. Workforce members must be notified and provide consent prior to the establishment of biometric authentication processes

C. Human Identification and Authentication

1. Workforce members must have their identity verified by authorized King County employees responsible for human resources functions prior to receiving credentials (e.g., usernames and passwords) that can access King County technology assets.

2. Each workforce member must be issued unique credentials (e.g., usernames and passwords) which must be maintained in a confidential manner and may not be shared with others.

3. Workforce members may not store their credentials in a manner that can be easily stolen or accessed by others (e.g., sticky notes, labels on workstations, signs, etc.)

4. Credentials may not be transmitted unencrypted over a network (e.g., Telnet, HTTP) or shared in plain text through email

5. Workforce members may not utilize their King County email address as a username or email address for personal activities unrelated to working for or on behalf of King County (e.g., Professional or Social Networking Sites, Shopping Sites, Fantasy Sports Sites, etc.).
6. Workforce member passwords used to access King County technology assets must be unique and not be identical to any password used for personal activities.
7. Workforce member authentication credentials must utilize multifactor authentication as defined in the Access Control and Authentication Standard except if:
    a. Used infrequently (i.e., a few times per month or less) to access King County human resource, payroll and benefits, or other personnel management technology such as timesheet tracking software and is done so using a King County owned and operated workstation located securely in a King County facility

    b. Human Resources determines an individual is affected by a qualifying disability
8. Guest, anonymous and shared account identities or account credentials are prohibited except:
    a. As authorized by the Chief Information Security and Privacy Officer. If a guest, anonymous, or shared account identity is required please request authorization by opening a ticket with the helpdesk.

    b. Identities and accounts created and used for emergency operations only when an emergency or incident is declared or for associated emergency training exercises so long as these accounts can only access technology assets used for the same emergency operations (e.g., EOC computers dedicated to EOC operations with accounts dedicated to those EOC computers that cannot login anywhere else).

    i. Credentials for these identities and accounts must be printed in a permanent or semi-permanent fashion that can be easily inventoried and tracked (e.g., laminated, plastic card, etc.) with clear instructions that the credentials are not to leave the facility and who or where to return the credentials to.

    ii. The credentials must be inventoried and stored in a King County facility only. The credentials must be checked out and in during use in an auditable process. Loss of these credentials requires notification to the Department of Information Technology (KCIT) helpdesk and a rotation of the credentials (i.e., a password change).

    iii. Credentials for these identities and accounts must be rotated (i.e., a password change) at least annually.

D. Device Authentication

Technology asset and support owners will ensure that devices are authenticated (e.g., 802.1x, certificates) prior to receiving full access to King County owned and operated networks. Devices that are not authenticated may be subject to limited or no access to technology assets in accordance with the Network Security Policy, Device Security Policy and Access Control and Authentication Standard.

E. Service and Machine Account Authentication

1. Service and machine identities, accounts, secrets, and/or keys (i.e., logins typically created for IT automation and management purposes) are considered identity assets and must be generated in accordance with the Asset Management Policy.
2. Service and machine credentials:
    a. Are not required to utilize multi-factor authentication
    b. May utilize a maximum age of 730 days (e.g., secret rotation, password change)
    c. Must not utilize default or manufacturer provided passwords or accounts
    d. Must utilize a randomly generated and unique password that is different from all other service and machine accounts

F. Kiosk and Shared Device Identification and Authentication

Accounts may be created to enable automated logins for kiosks or shared devices. These accounts:

1. Must not have administrative or privileged access to the kiosk or shared device
2. Are not required to utilize multi-factor authentication
3. May utilize a maximum password age of 365 days
4. Must utilize strict configuration and hardening controls to limit users of the device to authorized and intended interactions with the device configuration, software, and other functions
5. May not have access to technology assets classified as Category 3 or 4 in the Information Classification Policy unless a separate process exists after accessing the kiosk or shared device to authenticate the individual human user who will access Category 3 or 4 technology assets (i.e., the kiosk allows access to an application login screen where each individual human user must authenticate to access the application and data)

G. Manufacturer Provided Accounts and Credentials

Hardware and software manufacturers sometimes create default or local accounts so that the technology asset may be used the first time or for other purposes by a purchasing customer. These include local administrator, system or root accounts, and may also include scenarios where only a password is required to access administration features and functionality.

1. Manufacturer provided accounts and credentials are considered identity assets and must be managed in accordance with the Asset Management Policy.
2. If possible, manufacturer provided accounts must only be used for initial configuration to use King County's centralized identity platform. If possible these accounts should also then be disabled.
3. All manufacturer default passwords must be changed prior to production use of the technology asset (i.e., before being delivered to a workforce member or made available for use).

H. Remote Access Authentication

Remote access to King County technology assets occurs when the user or device authenticating is not directly connected to King County owned and operated private internal networks (physical or wireless) or when credentials will be transmitted over a network.

1. Remote access by individuals requires the use of an encrypted connection (e.g., SSH, VPN, TLS, etc.). Credentials must not be transmitted in clear text (e.g., HTTP, Telnet) and may not be shared via email.
2. Remote access by devices that establish permanent connectivity between two sites must be configured in compliance with the Network Security Policy and Network Security Standard (e.g., site to site VPN).
3. Access may be denied even after successful authentication due to conditional access requirements defined in the Access Control and Authentication Standard (e.g., geolocation tools detect that source IP address is outside the United States).

V. Implementation Plan

This policy becomes effective for countywide use on the date that it is signed by Chief Information Officer. All new technology implementations and new material changes to existing technology implementations must ensure compliance with this policy as of the effective date. All other technology implementations must be brought into compliance within four years after the effective date.

VI. Maintenance

A. This policy will be maintained by the Department of Information Technology (KCIT), Office of the CIO, or its successor agency. This includes, but may not be limited to:

1. Interpretation of this policy
2. Ensuring this policy content is kept current
3. Recommending updates to this policy and related resources
4. Developing an escalation and mitigation process if an Organization is not in compliance

5. Assisting Organizations to understand how to comply with this policy
6. Monitoring annual compliance by Organizations

B. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the Office of the CIO, or its successor agency prior to the expiration date.

VII. Consequences for Noncompliance

Violations of this policy may be grounds for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges.

VIII. Appendix A: References

- Acceptable Use Policy
- Access Management Policy
- Access Control & Authentication Standard
- Audit Logging and Monitoring Policy
- Data Encryption Standard
- Device Security Policy
- Network Security Policy
- Information Security Policy and Standards Glossary

IX. Appendix B: Relevant Compliance Requirements

This section provides references to key regulations and standards that apply to King County. This section does not replace the authoritative source and is just a reference to assist with further research. Please use the Compliance Standard and Section No. to further research the entirety of the regulation, framework or standard from the authoritative source.

Compliance Standard	Section No.	Description
HIPAA	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	164.308(a)(3)	Workforce Security
	164.308(a)(4)	Information Access Management
	164.310(a)(2)(iii)	Access Control and Validation Procedures
	164.312(a)	Access Control
	164.312(d)	Person or Entity Authentication
CJIS Policy v5.9	5.5	Access Control

PCI DSS v3.2.1	7	Restrict Access to Cardholder Data by Business Need to Know
	8	Identify and Authenticate Access to System Components
NIST CSF	PR.AC	Identity Management, Authentication and Access Control
NIST 800-53r5	AC-2	Account Management
	AC-3	Access Enforcement
	AC-14	Permitted Actions Without Identification Or Authentication
	AC-17	Remote Access
	IA	Identification and Authentication
CIS Controls v7.1	4	Controlled Use of Administrative Privileges
	16	Account Monitoring and Control