


Document Code No.: ITG-P-21-02
Title: King County Access Management Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Access Management
Sponsoring Agency: Department of Information Technology (KCIT)



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

I. Purpose:

The purpose of this policy is to ensure King County provides secure and appropriate access to technology assets (e.g., hardware, software, data, and authentication information). 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 King County workforce members responsible for technology asset ownership and support.

B. Technology Assets

This policy applies to all King County technology assets. 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

King County shall provide each user, service, and device the minimum access to technology assets necessary to fulfill assigned duties or tasks. This is referred to as the principle of least privilege. Technology asset owners are responsible for ensuring that users of their assets have the appropriate levels of access.

A. Deny All by Default

All technology assets shall be configured to deny access by default. Access must be explicitly granted to users, groups, roles, or technology systems, devices or services through a validation and approval process. This includes scenarios where the public or

countywide workforce members are intended to have some level of access. The access should be configured with the minimum necessary privileges (e.g., Read Only, other privileges validated and explicitly granted).

B. System Use Notification

Technology asset owners are responsible for ensuring that technology assets display a system use notification approved by the Chief Information Security and Privacy Officer before granting access to the system wherever technically possible. Lack of notification does not imply an exception to this policy. The notification shall at a minimum:

1. Inform the user they are accessing a restricted system
2. State that use of the system may be monitored, recorded, and is subject to audit
3. State that unauthorized use is prohibited and may subject the user to employment, civil, and criminal penalties
4. State that use of the system indicates consent and acknowledgement of the notification

C. Access Approval Requirements

1. The Department of Information Technology (KCIT) is responsible for providing an enterprise access request and approval workflow process and tool (not the act of approving) such as a ticketing system or similar mechanism. This includes retention of access approval documentation for auditing and ongoing access management purposes which must be easily accessible to internal and external auditors (e.g., Chief Information Security and Privacy Officer, King County Auditor, federal or state regulatory body, third party auditor).
2. Technology asset owners must approve access requests to their assets. Technology asset owners may delegate approval authority to an individual, role, or group but must document the delegation in the asset management system of record as defined in the Asset Management Policy and Asset Management Standard. Access approval may only be exercised by employees of King County who have completed an identity verification process by authorized King County employees responsible for human resources functions.
3. Technology asset owners must ensure access levels are approved consistent with the principle of least privilege necessary for a workforce member to complete their work.
4. Technology assets must be configured to require multi-factor authentication prior to managing or modifying access privileges where possible.
5. Access can be requested by and granted to individual users, groups, or roles in accordance with the least privilege principle. Technology asset owners are highly encouraged to utilize groups and roles to reduce the administrative overhead of access management.

6. Prior to granting access to technology assets technology asset owners must:
 - a. Determine whether a criminal background check is required to comply with local, state, or federal law (e.g., CJIS Security Policy). The technology asset owner is responsible for ensuring a criminal background check is conducted both initially and ongoing as required by applicable regulations.
 - b. Determine whether specific security awareness training is required for the technology assets being accessed. The Department of Information Technology (KCIT) is responsible for providing a security awareness training platform capable of enabling technology asset owners and workforce members to meet these requirements however alternate training platforms may be used where necessary.
 - c. Determine whether any contractual or other legal requirements have been established for the technology asset which may require acknowledging those set of requirements by those being provided access (e.g., data sharing agreements, acknowledgement of security or privacy requirements, etc.)
7. Accounts created for use by a machine (e.g., servers, workstations, cloud infrastructure) and not a human user (i.e., service accounts used for automation, management, or scheduled tasks):
 - a. Must utilize the same access approval process as a human user as defined in this policy
 - b. Machine accounts may be a member of a group or role
 - c. Technology support owners are responsible for maintaining an inventory of machine accounts and their purpose in accordance with the Asset Management Policy
 - d. The same account may not be used repeatedly for unrelated systems, services, or machines (i.e., these accounts should be generated to serve a specific purpose and not be used for any other purpose)
 - e. Machine accounts may not be used by human users in place of non-administrator or administrator accounts assigned to the user
 - f. An annual audit of machine accounts must be completed by the Chief Information Security and Privacy Officer in coordination with the technology support owners

D. Access Audit Requirements

1. Access to King County technology assets must be logged as required by the Audit Logging and Monitoring Policy.

2. Accounts with access to technology assets classified as category 3 or higher in the Information Classification Policy must be reviewed twice annually by the technology asset owner to determine whether access is still authorized in accordance with this policy. The review process requires the asset owner to affirm the access list in its entirety for technology assets with less than 250 users. For technology assets with more than 250 users a review of the processes used for authorization management can be performed instead and must include a review of a sample of recent changes to access authorizations in order to confirm processes are working as expected. Affirmation that access authorization is accurate or working as expected must be retained for auditing purposes.
3. The technology support owner is responsible for defining and managing the review process which must use a system-generated access list from the technology asset containing:
 - a. Technology asset name
 - b. User's full name or system or service account name
 - c. Unique account identifier or username
 - d. Account status (e.g., active, disabled, etc.)
 - e. Date of last login
 - f. User Access level(s) (e.g., full access, create, read, update, delete, etc.)
 - g. Group and/or role name
 - h. Group Access level(s) (e.g., full access, create, read, update, delete, etc.)
 - i. Group Membership by individual account including nested groups

E. Removal/Modification Requirements

1. In the event of workforce member termination (e.g., retirement, voluntary separation, involuntary separation) or job transfer within King County, the workforce member's current supervisor or manager must open a ticket with the helpdesk so that access may be modified accordingly.
2. All instances of a terminated workforce member's access must be disabled within 24 hours. If a terminated workforce member will subsequently volunteer or perform a new role with King County this should be considered a job transfer and access should be updated in accordance with the new role that will be performed.
3. Strictly limited access to payroll and benefits information may be granted to a terminated workforce member so long as that access cannot be used for any other King County technology assets.

4. Processes that create, modify, or remove identities or account credentials must comply with the Asset Management Policy and the Identification and Authentication Policy.

F. Multi-Factor Authentication

Multi-factor authentication must be used when accessing King County's technology assets in compliance with the Identification and Authentication Policy.

G. Separation of Duties

1. Technology asset owners approving access to technology assets classified as Category 3 or higher in the Information Classification Policy must review whether separation of duties requirements are necessary and take due care to avoid and control for potential conflicts of interest when approving access to technology assets, when making changes to a user's access levels and during the twice annual review process. This can be accomplished by:
 - a. Establishing a joint review and approval process with two or more approvers
 - b. Establishing access such that the approver has no access to the technology assets for which they are an approver and is not a peer, subordinate, manager or supervisor of the requestor
 - c. Separating tasks where conflicts exist and assigning to multiple individuals with additional independent reviews of those tasks
 - d. If conflicts of interest or clear risk of potential harm to access management approvals such as insider threats cannot be resolved then mitigating controls must be designed and implemented by the asset owner
2. Technology asset owners approving access must not have the ability to modify audit logs of the approval process or logs generated by the technology asset as defined in the Audit Logging and Monitoring Policy.
3. Administrative and privileged accounts used for the administration of technology assets must be separate from accounts used for normal duties and only used for those administrative tasks.
4. Technology asset and support owners will limit access authorization to administer technology assets between technology skill domains (e.g., network administration, server administration, cloud infrastructure administration, application administration, database administration, identity administration) where possible to reduce the ability for a single workforce member or team to

cause significant impacts to the confidentiality, integrity, or availability of King County technology assets.

H. Session Control and Lockout

1. Sessions generated when connecting to King County technology assets (e.g., logging into a Windows desktop, logging in to a web or cloud application, logging into a records management system) must be configured to timeout or lock after a period of inactivity of 30 minutes or less except when regulated by the Payment Card Industry Data Security Standard (PCI DSS), in which case sessions must timeout after 15 minutes. Re-authenticating to the system after a timeout or lock is required.
2. Technology assets used for kiosk or display purposes may be configured to allow sessions of inactivity longer than 30 minutes if:
 - a. Configured as a display only system for purposes of visualizing information within a secured area controlled by King County such as a utility or emergency operations environment
 - b. Configured as a kiosk (i.e., completely limits interactions with the technology asset to a specific set of interactions and prevents administration or changes to configuration of any kind to non-administrators)
 - c. Required by use cases covered by the Americans with Disabilities Act
3. Identities and accounts used to access King County technology assets must be immediately and if possible automatically prevented from any further access (e.g., account lockout or disable, application specific account lockout mechanisms, token revocation):
 - a. After five unsuccessful attempts to authenticate within a 30 minute time period
 - b. If a potential security incident is suspected to be in progress due to security incident detection and response systems and tools, conditional access policies or security incidents reported by users
4. Technology assets may be configured to automatically allow or re-enable access after a period of one hour from the last event or condition(s) that caused the prevention of access to occur. If a security incident has been detected or reported the Department of Information Technology (KCIT) or technology support owner will require a password reset and re-establishment of any sessions to technology assets.

I. Physical Access Control

Physical access to King County technology assets must be limited to authorized workforce members. Technology assets classified as category 2 or higher by the

Information Classification Policy may require specific physical access controls. Please consult with the Chief Information Security and Privacy Officer on physical access controls for technology assets by opening a ticket with the helpdesk.

J. Account Expiration and Inactive Accounts

1. Identities and accounts created as part of working for or on behalf of King County must be automatically disabled through the use of an expiration date if an expiration date is known and technically possible (e.g. STT, TLT, volunteers, other time limited employment or vendor contracts).
2. Identities and accounts created as part of working for or on behalf of King County with access to King County technology assets must be reviewed and automatically or manually disabled (i.e., prevented from being used but may still be retained) if not used for more than 90 days.
 - a. Identities and accounts created and used for emergency operations only when an emergency or incident is declared or for associated emergency training exercises may be configured to remain enabled even if not used within 90 days 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).

K. Vendor, Third Party, and Contractors

1. Identities and accounts assigned to vendors for maintenance purposes must only be activated as needed and have an automatic expiration period not to exceed 24 hours.
2. Accounts assigned to vendors or contractors for ongoing project based work must be unique and assigned to specific individuals and have automatic expiration not to exceed 180 days. Project teams are required to review and request a re-enablement of the expired accounts to ensure they are still necessary. These credentials may not be shared by more than one individual (i.e., a single account given to a vendor and used by all of the vendor's staff).
3. Technology asset owners that have requested identities and accounts assigned to vendors must notify the Department of Information Technology (KCIT) or the technology support owner by opening a ticket at the helpdesk immediately upon contract termination so that the accounts can be disabled.
4. Vendors must notify King County when individuals who have been provided accounts have been terminated. The Department of Information Technology (KCIT) or the technology support owner must be notified immediately with this information so the account can be disabled.

5. All contractors, vendors, and third parties who will be provided access to King County technology assets must acknowledge receipt of and agree to comply with King County's Acceptable Use Policy.
6. Prior to granting access to technology assets classified as Category 3 or higher in the Information Classification Policy to contractors, vendors, and third parties technology asset owners must:
 - a. Determine whether a criminal background check is required to comply with local, state, or federal law (e.g., CJIS Security Policy). The technology asset owner is responsible for ensuring a criminal background check is conducted both initially and ongoing as required by applicable regulations
 - b. Determine whether specific security awareness training is required for the technology assets being accessed. The Department of Information Technology (KCIT) is responsible for providing a security awareness training platform capable of enabling technology asset owners and workforce members to meet these requirements however alternate training platforms may be used where necessary
 - c. Have executed a contract with King County that includes any additional security requirements or agreements required by the technology asset owner or regulations covering the technology asset prior to receiving access (e.g., CJIS Security Policy Security Addendum, Business Associate Agreements, Data Sharing Agreements, etc.)

L. Administrator and Privileged Accounts

1. The Department of Information Technology (KCIT) is responsible for defining and managing a process for administrator and privileged accounts that:
 - a. Ensures these accounts are inventoried
 - b. Confidentially validates the workforce member has met any background check requirements
 - c. Receives approval from the technology asset owner for creation, modification, removal
 - d. Generates an audit log and alert when created, modified, or deleted
 - e. Produces a quarterly membership report for audit by the Chief Information Security and Privacy Officer
2. Administrator accounts used to administer identity and authentication platforms or directories, public key infrastructure (PKI), and systems that manage secrets and keys used for authentication and/or encryption must:
 - a. Be approved by the Chief Information Security and Privacy Officer
 - b. Be used only from workstations dedicated to this purpose

- c. Require the use of Multifactor Authentication
3. Accounts used to administer information security platforms and tools (e.g., firewalls, endpoint detection and response, anti-virus, content filters, vulnerability scanners, forensics and penetration testing tools, dynamic and static code analysis, etc.) must be approved by the Chief Information Security and Privacy Officer.
4. All non-console administrative access must be encrypted end to end using approved technologies such as Secure Socket Shell (SSH) or Transport Layer Security (TLS).

M. Passwords

1. Systems must be configured to enforce strong password requirements for all accounts in accordance with the Identification and Authentication Policy.
2. Passwords must be rendered unreadable using approved encryption or hashing mechanisms as defined in the Data Encryption Standard prior to being transmitted over a network or stored.
3. Technology assets whose primary function is password storage must be classified as Category 4 in the Information Classification Policy.

N. Emergency Access, Investigations, Public Records

1. The Chief Information Security and Privacy Officer may approve access to any technology asset for emergency or investigative purposes in accordance with the Incident Response Policy. The Chief Information Officer or Chief Technology Officer may approve emergency access as part of the Department of Information Technology (KCIT) Incident Management process.
2. King County legal representatives for the technology asset owner may be provided access as part of a legal process (e.g., discovery).
3. Department or agency records officers working for or on behalf of the technology asset owner may be provided access as part of a process required by RCW 42.56.

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, 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 Control & Authentication Standard
- Identification & Authentication Policy
- Data Encryption Standard
- Chapter 42.56 RCW
- 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)(i)	Workforce Security
	164.308(a)(4)(i)	Information Access Management
	164.312(a)(1)	Access Control
CJIS Security Policy v5.9	5.5	Access Control

PCI DSS v3.2.1	7	Restrict access to cardholder data by business need to know
NIST CSF	PR.AC	Identity Management and Access Control
NIST 800-53 r5	3.1	Access Control (AC-1 through AC-25)
CIS Controls v7.1	4	Controlled Use of Administrative Privileges
	14	Controlled Access Based on the Need to Know