Document Code No.: ITG-P-21-05
Title: King County Audit Logging and Monitoring Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Audit Logging and Monitoring, Audit Logs, Auditing
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 ensure audit logging is configured for technology assets and that these logs are monitored for possible security incidents. 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 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 a personal or third party device, 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. Audit Logging

1. All King County technology assets are required to comply with the Audit Logging Standard.
2. Technology asset and support owners must correct identified deviations with this policy and the Audit Logging Standard within 90 days of awareness of the deviation.
3. Audit logging must not be disabled or turned off on technology assets, and any change in this status must result in an alert to the technology asset and/or

technology support owner and must be corrected as soon as possible. For technology assets classified as category 3 or 4 as defined in the Information Classification Policy the technology asset and/or technology support owner must also contact the Chief Information Security and Privacy Officer to determine if further action is required.

4. Technology assets and audit logging solutions and services must be synchronized with a central time source configured with at least two backup time sources to ensure consistent and accurate correlation of audit log timestamps.
5. Logs should be generated for both successful and unsuccessful actions where possible.
6. All technology assets should generate audit logs that include the minimum following information where possible:
   a. User, system, and/or service identification causing the event (e.g., username, system account, service name, etc.)
   b. Date/Time of the event
   c. Affected system, information, data, or resource
   d. Source and destination causing or impacted by the event(s) (e.g., IP address, hostname, target of the action or command, etc.)
   e. Actions taken by privileged, generic, and default accounts must also be captured including but not limited to: administrator, users with administrator rights, privileged accounts, shared accounts, generic accounts, and vendor default accounts
   f. Actions that may indicate malicious activity, including, but not limited to port scans, failed login attempts and locked out accounts
   g. Modifications to system-level objects must generate a log entry (e.g., operating system files).
7. Information technology configuration management activity must include the minimum following information where possible:
   a. Changes made by a configuration management solution or tool (e.g., operating system policy configuration tools, infrastructure as code tools, application policy or configuration tools, or other information technology management tools)
   b. Audit policy changes
   c. Firewall configuration changes
   d. Switch and router configuration changes
   e. Time configuration changes
   f. Internet Protocol (IP) address changes

g. User or Group modifications (e.g., a new user was added, group membership has changed)

8. User and System Actions must include the minimum following information where possible:
   a. Logon/Logoff
   b. File/Folder Access
   c. Printing Events including what was printed
   d. Software Execution
   e. Process Creation
   f. Service Creation or Modification
   g. Scheduled Task Creation or Modification
   h. Security events such as malicious software or virus detection.
9. Server and network infrastructure shall also generate log events for:
   a. Universal Serial Bus (USB) storage devices that are connected to the system
   b. Disk usage thresholds
   c. Computer Processing Unit (CPU) and memory usage
   d. Failover monitoring of clusters
   e. Operating System Service status change including modifications
   f. Changes to system, critical application, and configuration files
10. Any failure of audit logging functionality or mechanisms must generate an alert to the technology asset or technology support owner. Other than for end user devices and peripherals audit logging functionality failures must be treated as a potential major incident as defined by the Department of Information Technology (KCIT) Major Incident Management Process if handling category 3 or 4 data in accordance with the Information Classification Policy.
11. Audit logging should be designed or configured to provide the minimum amount of information needed for corrective action while not revealing sensitive information that could be exploited by a malicious party.

B. Audit Logs

1. Centralized or aggregated audit log stores are a data asset as defined in the Asset Management Policy and should be classified as a category 3 data asset or higher in the Information Classification Policy and must be inventoried in compliance with the Asset Management Policy.
2. Audit logs must be encrypted in transit and at rest in accordance with the Data Encryption Standard (standard defined by King County).

3. Audit logs shall be protected from unauthorized access and modification:
    a. Read-only access to audit logs requires authorization from the technology asset or technology support owner.
    b. Access to modify or delete audit logs requires authorization from the Chief Information Security and Privacy Officer or their designee. This authorization and justification must be documented. Audit logs should be immutable (i.e., unchangeable and indisputable) if possible.
4. Centralized or aggregated audit logs must be backed up for disaster recovery purposes in compliance with the Data Backup and Recovery Standard as approved by the Architecture Review Team (ART).
5. Any administrative changes to logs or the logging configuration shall cause an alert to be sent to the technology support owner.
6. Audit logs may be subject to disclosure under Chapter 42.56 RCW. Audit logs must be searchable and retained in accordance with federal, state and local law and King County records retention policy requirements. Consideration of RCW 42.56.420(4) must be given prior to disclosure of audit log information. Please contact your department or agency's Public Records Officer, the King County Public Records Program, or the Chief Information Security and Privacy Officer with questions regarding disclosure of audit logs. In no case should logs be retained for less than one year.
7. Storage devices containing audit logs must comply with the equipment destruction standards developed by the Department of Information Technology (KCIT) when decommissioned.

C. Continuous Monitoring

1. Technology support owners and the Chief Information Security and Privacy Officer are responsible for ensuring the continuous monitoring of audit logs for events that could adversely affect the asset or King County's technology environments. The Department of Information Technology (KCIT) will develop and maintain an enterprise standard to monitor audit logs and document in the Monitoring Standard.
2. Due to the quantity of events that may be generated by technology assets the Department of Information Technology (KCIT) may define and utilize automation technology standards such as a security information and event management (SIEM) solution to automate the continuous monitoring of audit logs in place of a human monitoring approach. If monitoring automation is not possible for a specific audit log the technology asset owner or technology support owner must regularly review audit logs for potential security incidents at least weekly and in accordance with applicable federal, state, or local law.
3. The Department of Information Technology (KCIT) must develop and the Chief Information Security and Privacy Officer must approve security incident alert

thresholds that will generate an alert for human review. Alerting thresholds will be defined in the Monitoring Standard. Monitoring systems should at a minimum generate alerts when:

a. Malicious software or code is detected

b. Anomalous use of identities or accounts is detected (e.g. account lockouts, impossible travel)

c. Security solutions and tools detect a security incident

d. Technology assets become unavailable unexpectedly

e. Anomalous resource usage is detected in technology infrastructure

f. System and critical application or configuration files are modified

g. New services or scheduled tasks are created

h. Logins occur from accounts that can administer Identity and Access Management platforms or systems

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

- Chapter 42.56 RCW
- Chapter 42.56.420(4) RCW
- Asset Management Policy
- Data Encryption Standard
- Equipment Destruction Standard
- 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)(1)(ii)(D)	Information System Activity Review
	164.308(a)(5)(ii)(C)	Log-in Monitoring
	164.312(b)	Audit Controls
CJIS Policy v5.9	5.4	Auditing and Accountability
PCI DSS v3.2.1	10	Track and monitor all access to network resources and cardholder data
NIST CSF	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
NIST 800-53r5	AU	Audit and Accountability
CIS Controls v7.1	6	Maintenance, Monitoring and Analysis of Audit Logs