Document Code No.: ITG-P-21-06
Title: King County Data Security Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Data, Open Data, Data Security, Data Governance
Sponsoring Agency: Department of Information Technology (KCIT)

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

King County

I. Purpose:

The purpose of this policy is to ensure security controls are in place to prevent data exfiltration, mitigate the effects of exfiltrated data, and protect the confidentiality, integrity and availability of King County's data assets. 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. Data Assets

This policy applies to all King County data assets. A data asset is any data that is created, stored, processed, transmitted, used, or observed by a King County system or by a workforce member working for or on behalf of King County. Data assets include any form (electronic, printed, website, voice record, email, CD, database, etc.) or location (in King County offices, personal residences, off–site, laptop computers, cellphones, etc.). "Data" and "information" are the same for purposes of this policy. This policy also applies to the use of third party or personal devices, if used to store King County data 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. Data Owner and Custodian

1. All King County technology assets must have a designated Technology Asset Owner in compliance with the Asset Management Policy. Data Asset Owners are by default the Department or Agency Director or Presiding Judge of the department or agency where the data asset was generated, stored, processed, or transmitted as part of a workflow used to deliver their department or agency's services including data that has been shared by or with a third party through a data sharing agreement. Data asset owners manage the data asset throughout its lifecycle and are most familiar with the purpose and use of the data asset.
2. Data assets must have a data custodian identified who is accountable for the technical control of data including security and privacy, scalability, configuration management, availability, accuracy, consistency, audit trail, backup and restore, compliance with standards and business rules. Data Asset Custodians are by default the technology support owner for the Data Asset Owner.
3. Data asset ownership may be delegated or transferred but this must be recorded in the data asset management system of record as defined in the Asset Management Standard.
4. Asset ownership may only be exercised by those who have completed identity verification as defined in the Identification and Authentication Policy.
5. Data owners are responsible for:
    a. Participating in data governance activities within their departments and those activities coordinated by the Department of Information Technology (KCIT)
    b. Ensuring the accurate inventory of data assets in accordance with the Asset Management Policy
    c. Understanding the regulatory requirements associated with their data assets
    d. Ensuring data assets are classified in accordance with the Information Classification Policy
    e. Authorizing and auditing access to data assets in accordance with the Access Management Policy
    f. Developing and communicating data retention, business continuity, and disaster recovery requirements to Data Custodians and Technology Support Owners
    g. Ensuring that a rigorous justification process exists to ensure that the minimum amount of Personally Identifiable Information (PII) is collected, stored, processed, and transmitted in order to provide services in accordance with federal and state law, King County Code, and King County privacy policies

B. Authorization to Access Data Assets

The following requirements must be met prior to handling King County data assets:

1. Access must be approved in compliance with the Access Management Policy.
2. Data Asset Owners must require a non-disclosure agreement (NDA) or confidentiality agreement be signed by King County workforce members or third party agents acting on behalf of King County prior to receiving access to King County data assets or third party data assets King County has been authorized to use:
    a. If required by federal, state, or local law
    b. If required by a contractual agreement King County is a party to (e.g. Data Sharing Agreement)
    c. If required by department or agency specific policy
3. A data sharing agreement (DSA) must be considered by the Data Asset Owner prior to sharing or publishing (e.g. RFP, SOW, website, white paper, database transfer or access) with any third party (e.g., private company or individual, other government or non-profit entity). Data Owners must consult with the Department of Information Technology (KCIT) and the Prosecuting Attorney's Office to review the necessity, develop the agreements, and ensure legal compliance.
4. Security awareness training must be completed by King County workforce members in accordance with the Security Awareness Training Policy. The Department of Information Technology (KCIT) is responsible for maintaining a security awareness training platform capable of enabling workforce members, their supervisors, and Data Asset Owners to comply with this policy.

C. Data Asset Documentation and Controls

Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to King County's data assets and the services that rely on them. Data Asset Owners are responsible for working with Data Asset Custodians to ensure proper documentation and controls are in place. Please request a consult with the Chief Information Security and Privacy Officer if needed by opening a ticket with the helpdesk.

1. Data Asset Owners and Custodians must:
    a. Inventory the data asset in compliance with the Asset Management Policy
    b. Determine the data asset's classification and impact in compliance with the Information Classification Policy
    c. Complete Information Security Risk and Privacy Impact Assessments for category 3 or 4 data assets as defined in the Information Classification Policy (requests can be made to the Chief Information Security and Privacy Officer by opening a ticket with the helpdesk)
    d. Complete a review of business continuity and disaster recovery requirements
    e. Complete a review of records retention requirements

f. Implement controls at the appropriate level. This typically is not at the individual file or record level but for a collection of data records such as those in a database or a series of files and folders that together have similar relevance to a workflow, public service, division or team, project, regulations, or other commonalities that have the same business requirements. For example:
    - Structured Data Assets controlled by Management Systems or Solutions (e.g. database, data warehouse, data lake) and associated metadata
    - Unstructured or Semi-Structured Data Assets (e.g. PDF or Text Documents and files, Spreadsheets, Image Files, Video/Audio Files, XML Files, JSON Files) containing regulated data (e.g., criminal history, protected health information)
    - SharePoint Site Collection, Site, Library, or Folder
    - Network File Share Folder Hierarchy (group or dedicated to single user)
    - Source Code Repositories
    - Virtual Infrastructure Files (e.g. virtual hard disk files for virtual machines)
    - Technology Asset Configuration Files and Scripts
    - System Files critical to enterprise infrastructure (e.g. Active Directory Domain Services and Domain Controllers, DNS Zone Files, DHCP addressing databases) or critical individual system files (e.g. Windows and Linux operating system files). The process for developing security controls for System Files can be developed against a representative sample and applied to the entire represented set (i.e., a Windows Server 2019 operating system is evaluated and the developed security controls are then applied to all Windows Server 2019 systems).

g. Implement controls that include but are not limited to:
    i. Access and Authorization Controls
    ii. Encryption/Decryption for Data at Rest, In Use, and In Transit
    iii. Cryptographic Integrity Validation
    iv. Environment Separation Requirements (e.g., production, non-production) Production data (real data that isn't fake or generated for testing purposes) must not be used or accessible to development, test, or other non-production environments unless all the required controls for a production environment are in place first
    v. Backups for Business Continuity and Disaster Recovery
    vi. Audit Logging
    vii. Security Incident Monitoring and Alerting

viii. Retention and Secure Destruction

h. Develop a process for Data Asset Owners to audit access to their data assets and ensuring access to the data asset is appropriate and in compliance with the Access Management Policy.

D. Geographic Boundaries and Distances

1. Data assets must remain in geographic locations governed by United States law
2. Backups of data assets must be stored at least 50 miles from the geographic location where the primary or production data asset is located

E. Public Records and Retention Schedules

1. The King County Records Management Program provides King County departments and agencies with advice and guidance regarding RCW 40.14, the primary state statute describing the preservation and destruction requirements regarding public records. Judicial and Legislative branches of King County government may have different or additional public records requirements. Data Owners and the Department of Information Technology (KCIT) must consult with the Data Owner's department or agency Records Officer or the King County Records Management Program to determine retention requirements for data assets.
2. RCW 42.56.420(4) authorizes King County to redact or withhold certain records related to information security from disclosure to the public. Public Records Officers and Attorneys representing King County must notify the Chief Information Security and Privacy Officer prior to disclosing records defined in RCW 42.56.420(4) through a public records request or litigation discovery process. When applicable, an NDA will be required.

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

- Asset Management Policy
- Information Classification Policy
- Data Security Standard
- Data Encryption Standard
- Security and Awareness Training Policy
- Chapter 42.56 RCW
- Chapter 42.56.420 RCW
- Chapter 40.14 RCW
- King County Code Title 4A.601
- 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
	164.306(a)	General Requirements
	164.308(a)(1)(ii)(A)	Risk Analysis
	164.310(d)(2)(i)	Disposal
	164.312(a)(2)(ii)	Emergency Access Procedure

	164.312(a)(2)(ii)	Encryption and Decryption
	164.312(c)(1)	Integrity
	164.312(e)(1)	Transmission Security
	164.314(a)(1)	Business Associate Contracts or Other Arrangements
CJIS Security Policy v5.9	4	Criminal Justice Information and Personally Identifiable Information
	5.1	Information Exchange Agreements
	5.10	System and Communications Protection and Information Integrity
PCI DSS v3.2.1	3	Protect Stored Cardholder Data
	4	Encrypt Transmission of Cardholder Data Across Open, Public Networks
NIST CSF	PR.DS	Data Security
NIST 800-53r5	AC	Access Control
	PT	PII Processing and Transparency
	SC	System and Communications Protection
	SI	System and Information Integrity
CIS Controls v7.1	13	Data Protection