

Document Code No.: ITG-P-21-09

Title: King County Information Classification Policy

Affected Agencies: Countywide


Authorities: King County Code Title 2A.380

Keywords: Information Classification, Risk, Impact, Category

Sponsoring Agency: Department of Information Technology (KCIT)

Chief Information Officer Signature:

Date signed and effective: 2/16/2021

DocuSigned by:

920AF9FCB611460...



King County

I. Purpose:

The purpose of this policy is ensure workforce members responsible for technology asset ownership and support establish and control the level of potential risk and adverse impacts to technology assets by classifying the technology asset using a consistent countywide approach. 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.

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. Impact and Classification

Understanding the sensitivity of and potential impact to technology assets is key to managing risk and applying appropriate controls.

1. Technology assets must be managed in compliance with the Asset Management Policy which includes identifying the classification and impact of the asset. Technology asset owners are required to determine and document the impact and classification of their assets for inclusion in the asset management system(s) of record defined in the asset management standards developed by the Department of Information Technology (KCIT).

2. Technology asset and support owners are responsible for prioritizing and implementing protections and security controls using Impact and Classifications as determined by the Technology Asset Owner.
3. Impact must be determined using the following table (for purposes of determining impact, low impact includes no impact) by selecting either Low, Moderate, or High impact. Only one value should be selected overall for impacts to confidentiality, integrity, and availability. For example, if low and moderate impacts to confidentiality and integrity are possible but the possible impacts to availability are high, the Impact overall would be selected as high.

Objective	Impact		
	Low	Moderate	High
Confidentiality Preventing unauthorized information access and disclosure, including preserving privacy and proprietary information.	An unauthorized disclosure of information or data could have a negative effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.	An unauthorized disclosure of information or data could have a serious adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.	An unauthorized disclosure of information or data could have a severe or catastrophic adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.
Integrity Protecting against unauthorized modification or destruction of information and includes ensuring information non-repudiation and authenticity.	An unauthorized modification or destruction of information or data could have a negative effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.	An unauthorized modification or destruction of information or data could have a serious adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.	An unauthorized modification or destruction of information or data could have a severe or catastrophic adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.

<p>Availability Ensuring timely and reliable access to and use of information</p>	<p>A disruption of access to or use of information, data, or system could have a negative effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.</p>	<p>A disruption of access to or use of information, data, or system could have a serious adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.</p>	<p>A disruption of access to or use of information, data, or system could have a severe or catastrophic adverse effect on strategic objectives, operations, assets, finance, compliance, safety, reputation, or individuals.</p>
--	--	---	--

4. Classification must be determined using the following table:

Classification			
Category 1	Category 2	Category 3	Category 4
Public Information	Sensitive Information	Confidential Information	Confidential Information Requiring Special Handling
<p>Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but may need integrity and availability protection controls.</p>	<p>Sensitive information may not be specifically protected from disclosure by law and is for official use only (FOUO). Sensitive information is generally not released to the public unless specifically requested. Sensitive or higher classification information may have been designated by third parties (e.g.,</p>	<p>Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to personal information as defined in RCW 42.56.230 and RCW 19.255.10, information about public employees as defined in RCW 42.56.250, information about infrastructure and</p>	<p>Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations, or contractual agreements. Serious consequences</p>

	federal government) using schemes like the Traffic Light Protocol (TLP) or other designation schemes.	the security of computer and telecommunication networks as defined in RCW 42.56.420(4).	could arise from unauthorized disclosure such as threats to health and safety, or legal sanctions.
Examples: King County Code Real Property Information Recreation Program Schedules	Examples: Purchase Requests or Preliminary Budget Documentation Email Communications not covered by a disclosure exemption Non-essential non-archival day to day administrative files used by non-elected, non-executive, non-department directors	Examples: Application for Public Employment Network Infrastructure Diagram Usernames and Passwords used to access King County technology assets Personally Identifiable Information or PII	Examples: Protected Health Information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Criminal Justice Information as defined by the Criminal Justice Information Services Security Policy 911 Computer Aided Dispatch System

5. Changes to classification levels during the lifecycle of technology assets can be made by the asset owner as necessary to comply with federal, state, or local law. If you have any questions or concerns about changing classification levels or disclosing information please contact your department or agency's Public Records Officer or the King County Public Records Program.

B. Data Asset and Information Protection

Data Asset owners are responsible for ensuring data assets are protected in accordance with the Data Security Policy.

1. Data Asset Owners must develop a classification map or training document for workforce members accessing data assets classified as category 3 or higher. (See example below in Section D).
2. The Department of Information Technology (KCIT) is responsible for providing enterprise technology solutions that support labeling or specifying the information classification of electronic records (e.g., Word and PDF documents, email messages) where possible.

3. Data asset owners are responsible for labeling solutions for physical records.
4. Classification maps and labeling schemes must be approved by the Architecture Review Team in the Department of Information Technology (KCIT) and should be limited to the division level or higher within a department in order to reduce complexity and administrative overhead. Cross departmental classification schemes are acceptable where needed.
5. Classification (e.g., labels, tags in asset management database, documentation about the asset) must be applied to all information and data assets classified as category 3 or higher.
6. All King County customer information and personally identifiable information must be classified as Category 3 or higher unless otherwise determined by state or federal law, King County Code, King County Policy, or a legal opinion provided by the Prosecuting Attorney’s Office.
7. Data Asset Owners and Custodians are required to ensure that workforce members are trained to manage and protect information and data assets in accordance with its classification and impact.

C. Reclassification

Technology asset owners shall reevaluate classification and impact of assets as needed to update classification and impact procedures based on changes such as legal and contractual obligations or changes in the use of the asset.

D. Example

Example Information Classification Map



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
- Chapter 19.255.10 RCW
- Chapter 42.56.070(8) RCW
- Chapter 42.56.250 RCW
- Chapter 42.56.420(4) RCW
- Chapter 42.56.230 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)(1)(ii)(A)	Risk Analysis
	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis
CJIS Policy v5.9	5.1.1.1	Information Handling
	5.2.1	Basic Security Awareness Training
PCI DSS v3.2.1	9.6.1	Classify media so the sensitivity of the data can be determined.
NIST CSF	ID.AM(5)	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
	ID.RA	Risk Assessment
NIST 800-53r5	AC-16	Security and Privacy Attributes
	AC-21	Information Sharing
	RA-2	Security Categorization
CIS Controls v7.1	13	Data Protection