

**Document Code No.:** ITG-P-21-11

**Title:** King County Security Awareness Training Policy

**Affected Agencies:** Countywide


**Authorities:** King County Code Title 2A.380

**Keywords:** Security Awareness Training

**Sponsoring Agency:** Department of Information Technology (KCIT)

**Chief Information Officer Signature:**

2/16/2021

DocuSigned by:  
  
920AF9FCB611460...

**Date signed and effective:**



## I. Purpose:

The purpose of this policy is to ensure workforce members are informed about information security policies and standards, regulatory requirements and modern cyber threats to King County technology assets and services. 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 who access King County's systems, applications, and data.

### B. Technology Assets

Intentionally left blank.

### 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

All workforce members with access to King County technology assets are required to complete Security Awareness Training in compliance with this policy. Security Awareness Training must be completed within 180 days of hire, and at least annually thereafter.

### A. Security Awareness Training System

1. The Department of Information Technology (KCIT) is required to provide an enterprise countywide training system that:
  - a. Enables King County workforce members to meet the requirements of this policy
  - b. Enables progress reporting for purposes of compliance with this policy

- c. Provides a feedback form at the end of each training module for workforce members to provide feedback
2. The Chief Information Security and Privacy Officer must review and report on the Security Awareness Training System and associated feedback at least once per biennium to Department and Agency directors and Presiding Judges to determine:
  - a. Where improvements can be made
  - b. If regulatory or business requirements have changed
  - c. If roles and responsibilities or organizational requirements have changed

## **B. Information Security Awareness Training**

Department and Agency directors and Presiding Judges are required to ensure that workforce members complete security awareness training on information security topics as determined by the Chief Information Security and Privacy Officer and as required by regulatory requirements (e.g., CJIS Security Policy, HIPAA, PCI DSS). Topics may include, but are not limited to:

- Information Security and Privacy Policies and Regulations
- Password usage and management
- Implications of non-compliance
- Malicious email attachments
- Phishing and spoofed emails
- Web usage - allowed/prohibited
- Security of devices issued to or used by workforce members
- Visitor control and physical access to spaces
- Reporting unusual activity and potential security and privacy incidents

## **C. Role-Based Security Training**

Workforce members in specific jobs and roles in King County may require additional security awareness training. The Chief Information Security and Privacy Officer will work with departments and agencies to identify these roles to ensure required training is completed. These specific jobs and roles include but are not limited to:

1. Workforce members with duties covered by regulations and security standards such as HIPAA, the PCI DSS, or the FBI CJIS Security Policy
2. Workforce members who have Incident Response responsibilities
3. Workforce members participating in software development or other technology engineering and support
4. Workforce members who have Business Continuity responsibilities

**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**

- 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.

<b>Compliance Standard</b>	<b>Section No.</b>	<b>Description</b>
<b>HIPAA</b>	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	164.308(a)(5)	Security Awareness and Training
<b>CJIS Policy v5.9</b>	5.2	Security Awareness Training
	5.3.3	Incident Response Training

<b>PCI DSS v3.2.1</b>	6.5	Address common coding vulnerabilities in software-development processes as follows: - Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. - Develop applications based on secure coding guidelines.
	9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
	12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
	12.10.4	Provide appropriate training to staff with security breach response responsibilities.
<b>NIST CSF</b>	PR.AT	Awareness and Training
<b>NIST 800-53r5</b>	AT	Awareness and Training
	CP-3	Contingency Training
	IR-2	Incident Response Training
<b>CIS Controls v7.1</b>	17	Implement a Security Awareness and Training Program