Document Code No.: ITG-P-21-08
Title: King County Incident Response Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Security Incident Response
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 establish requirements for response to information security incidents by workforce members through the establishment of an information security incident response plan. 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

This policy applies to all information security incidents that may impact the confidentiality, availability, and integrity of technology assets, including but not limited to attempted network intrusion, denial of service attack, detection of malicious software, unauthorized access to data, and violation of policies.

A. Users

This policy applies to all persons working for, or on behalf of King County, including workforce members, third parties, volunteers, and contractors accessing technology assets owned and operated by King County. These requirements apply whether the workforce member is working at a King County facility or connecting remotely.

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

A. Reporting of Potential Information Security Events or Issues

1. All workforce members are required to immediately report information security incidents or information security vulnerabilities to the Department of Information Technology (KCIT) by opening a ticket with the helpdesk.
2. Information Security Awareness Training provided by the Department of Information Technology (KCIT) shall include content on identifying and reporting potential information security events.
3. The Chief Information Security and Privacy Officer will provide additional and required training to workforce members who are responsible for information security incident response at least annually in accordance with the Security and Awareness Training Policy.
4. The Chief Information Security and Privacy Officer will ensure that regulatory notification requirements regarding information security incidents are followed (e.g. notification to the Washington State Patrol for incidents covered by the CJIS Security Policy).

B. Information Security Incident Response Plan

The Chief Information Security and Privacy Officer is responsible for establishing an information security incident response plan that includes:

1. Procedures for responding to suspected or known information security incidents including escalation to the Department of Information Technology (KCIT) Major Incident Management process and the King County Office of Emergency Management where necessary.
2. Reporting procedures to regulatory or third parties where required
3. Documentation procedures for incidents
4. Roles and responsibilities during an information security incident
5. Communication and notification requirements and procedures when an information security incident is confirmed and how to conduct communications during an information security incident including when normal communication channels are unavailable
6. Availability requirements by King County workforce members responsible for information security incident response
7. Authorities to make decisions during response activities
8. Consistency with the King County Comprehensive Emergency Management Plan and Emergency Support Function 2 as defined by the Federal Emergency Management Agency’s National Response Framework.

9. The definition of a data breach and the requirements and procedures to manage a data breach
10. Incident closeout procedures that include a review for improvement opportunities

C. Incident Information Sharing

1. Any public release of information concerning an information security incident requires notification to the Chief Information Security and Privacy Officer prior to release.
2. Information about information security incidents must not be shared by workforce members who are responsible for or participate in information security incident response unless otherwise described by the Incident Response Plan or approved by the Chief Information Security and Privacy Officer.

D. Information Security Incident Metrics

Procedures shall be established by the Chief Information Security and Privacy Officer to report on information security incidents including types, frequency of occurrence, and costs of information security incidents. This information must be reviewed at least annually by the Technology Management Board and Business Management Council.

E. Documentation

Workforce members responsible for responding to information security events and incidents are required to document confirmed information security incidents. Information security incidents managed by automated security tools or processes must generate the same documentation which must be reviewed on at least an annual basis for opportunities to reduce or prevent recurrence. Documentation must include at a minimum the following information:

1. Name of person(s) and organization(s) or system(s) conducting or participating in the response
2. Description of the technology assets affected by the incident
3. Time and date of the incident discovery
4. Time and date of earliest known event causing the incident
5. Impact to the technology assets
6. The suspected cause of the incident
7. The actions taken to mitigate the incident and restore the technology asset to a trusted and healthy operating status
8. Recommendations for further actions to prevent the recurrence of a similar incident

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

- Incident Response Plan
- Security and Awareness Training Policy
- King County Comprehensive Emergency Management Plan
- Federal Emergency Management Agency's National Response Framework
- 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)(6)	Security Incident Procedures
CJIS Policy v5.9	5.3	Incident Response

PCI DSS v3.2.1	11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.
	12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
	12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.
NIST CSF	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
NIST 800-53r5	IR	Incident Response
CIS Controls v7.1	19	Incident Response and Management