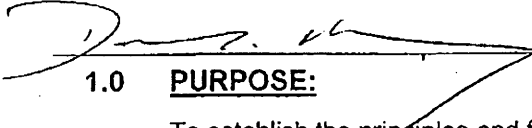




King County

Office of Information
Resource Management

Information Technology Governance Policies and Standards

Title Enterprise Information Security Policy	Document Code No. ITG-PDS-03-02
Chief Information Officer Approval 	Date Effective Date. 9/9/09

1.0 PURPOSE:

To establish the principles and foundation for King County's information security practices for development and compliance with applicable laws, regulations, contractual obligations and countywide information security policies and standards.

Information security is both a technical and a business issue and is every county Workforce Member's responsibility. Effective information security requires the active engagement of county management to assess emerging security threats to their business and provide strong information security leadership.

2.0 APPLICABILITY:

This policy is applicable to all King County Organizations and Workforce Members

3.0 REFERENCES:

- 3.1 Information Technology Policy and Standards Exception Request Process
- 3.2 Washington State "Public records act" RCW 42.56
- 3.3 King County's "Commitment to protecting privacy" KCC 2.14.030
- 3.4 ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems - Requirements
- 3.5 ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management
- 3.6 National Institute of Standards and Technology (NIST) special publication series 800
- 3.7 National Security Administration (NSA) Security Configuration Guides

4.0 DEFINITIONS:

- 4.1 **Information Asset:** A definable piece of information, information-processing equipment, or Information System, that is recognized as "valuable" to the Organization. It has one or more of the following characteristics:
 - Not easily replaced without cost, skill, time, resources, or a combination thereof.

Enterprise Information Security Policy

- Part of the Organization's identity, without which, the Organization may be threatened.
- 4.2 **Information Custodian:** The person who is responsible for defining specific control procedures, administering information Access Controls, implementing and maintaining cost-effective information control measures, and providing recovery capabilities consistent with the instructions of Information Owners.
 - 4.3 **Information Security:** The prevention of, and recovery from unauthorized or undesirable destruction, modification, disclosure or use of Information Assets whether accidental or intentional.
 - 4.4 **Information System:** Software, hardware and interface components that work together to perform a set of business functions.
 - 4.5 **Information Owner:** The person who is responsible for protecting an Information Asset, maintaining the accuracy and integrity of the Information Asset, determining the appropriate Data sensitivity or classification level for the Information Asset, reviewing its level for appropriateness, and ensuring that the Information Asset adheres to policy.
 - 4.6 **Organization:** Every county office, officer, institution, department, division, board, and commission.
 - 4.7 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full- and part-time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, volunteers, and staff from third-party entities who provide service to King County.

5.0 POLICIES:

King County is a public entity; as such the information in the possession of King County is generally available for public review. Nevertheless, King County is committed, to the extent allowable by law, to protect and secure all Information in its possession. The commitment must be balanced with the rights of public access under Chapter 42.56 RCW (Washington Public Records Act) and consistent with KCC 2.14.030 and any contractual obligation, applicable federal, state, and local statute or regulation.

King County information is a valuable asset, therefore King County's information, and information that has been entrusted to King County, must be consistently protected in a manner commensurate with its sensitivity, value, and criticality. The confidentiality, integrity and availability of King County's Information Assets shall be protected from unauthorized disclosure, modification, or destruction, and shall be safeguarded to the extent permitted by law

Enterprise Information Security Policy

- 5.1 **Security Principles** King County information security practices shall conform to the following principles:
- 5.1.1 **Risks** – Risks to information and Information Systems shall be assessed periodically and continually managed as part of a information security risk management program to address risks, vulnerabilities and threats.
 - 5.1.2 **Governance** – Information security policies, standards, guidelines and, procedures shall be developed and implemented based on industry recognized security standards and best practices. These policies, standards guidelines and procedures will be periodically reviewed and corrective actions taken to remediate identified deficiencies.
 - 5.1.3 **Policy-Driven Information Systems Security Architecture** - To assure that business goals and objectives are properly translated into information systems as well as the controls employed in these same information systems, King County shall employ a policy-driven information systems security architecture approach which is coordinated and integrated into the information security risk management process.
 - 5.1.4 **Integration** - Information security is an important element of sound business management and should be an integral part of the county's information management.
 - 5.1.5 **Accountability** - Information security accountability and responsibility shall be clearly defined as part of a security management structure and be acknowledged by staff and management.
 - 5.1.6 **Awareness** - All Workforce Members with access to King County's Information Assets must be aware of the need for information security and trained in what they can do to enhance security to support the county's business.
 - 5.1.7 **Cost Effective** - Information security controls should be cost-effective and proportionate to the risks associated with the Information Asset.
 - 5.1.8 **Equity** - Organizations should respect the rights of one another and their actions in King County's shared information environment should be ethical and not adversely affect others.
 - 5.1.9 **Timeliness** - Organizations should act in a timely, coordinated manner to prevent, detect and respond to breaches of, and threats to information security.
- 5.2 **Countywide policies** - Specific countywide information security policies, standards, guidelines and procedures shall be implemented to ensure that integrity, confidentiality, and availability of county information are not compromised.
- 5.2.1 **Policy foundation** - Countywide policies, standards and guidelines shall be based on industry recognized security standards and best practices, such as International Standards Organization (ISO) 27000 series, National Institute of

Enterprise Information Security Policy

Standards and Technology (NIST) Series 800 Special Publications, and National Security Administration (NSA) Security Configuration Guides.

5.2.2 **Minimum requirement** - Countywide policies and standards shall be considered minimum requirements to provide a secure environment for developing, implementing, and supporting information technology and systems.

5.3 Countywide security:

5.3.1 **Technology Management Board (TMB) Security Sub Team** - The TMB security sub team shall focus on countywide information security and membership shall consist of organization representatives.

5.4 Organization security:

5.4.1 **Organization policies** - Organizations may develop more stringent policies and standards as necessary to accommodate Organization-specific requirements.

5.4.2 **Organization procedures** - Organizations shall develop and document procedures that support the countywide information security policies, standards and guidelines.

5.5 Compliance:

5.5.1 **Annual compliance review** - At least annually, organizations shall review their information security processes, procedures and practices and any agency specific policies and standards, for compliance with countywide information security and privacy policies and standards.

5.5.2 **Verification of compliance** - Annually the executive, judiciary, council and all other elected officials shall verify in writing to the Chief Information Officer that the Organization is in compliance with countywide information security and privacy policies and standards and identify areas where compliance has not been achieved.

5.5.3 **Annual review** - Annually the CIO shall review the status of Organization adoption and compliance with countywide information security policies and standards and work with Organizations on any required compliance follow-up.

5.6 **Policy Non-Enforcement** – Non-enforcement of any requirement in this or any information security and privacy policy or standard does not constitute consent on the part of county management

5.7 **Violations of Security and Privacy Policies and Standards** – Organizations shall utilize appropriate actions or measures for violations of information security and privacy policies and standards consistent with county human resources policies. Such actions may include but are not limited to termination of access rights, reassignment, and remedial training. Under appropriate circumstances disciplinary action may be appropriate and may result in action up to and including termination and/or criminal prosecution.

Enterprise Information Security Policy

- 5.8 **Periodic Review:** - Information Security and Privacy Policies and Standards are subject to continuous, systematic review and improvement and are reviewed at least annually and updated to reflect changes in business objectives and/or the risk environment.

6.0 **EXCEPTIONS:**

Any Organization seeking an exception to this policy must follow the Information Technology Policy and Standards Exception Request Process using the Policy and Standards Request form. This form can be found on the Office of Information Resource Management policies and procedures Web page at <http://kcweb.metrokc.gov/oirm/policies.aspx>.

7.0 **RESPONSIBILITIES:**

- 7.1 **Chief Information Officer:** oversees development and adoption of countywide information security policies and standards, and the strategic direction for managing King County's information security.
- 7.2 **Chief Information Security and Privacy Officer:**
- 7.2.1 Lead the development and adoption of countywide information security and privacy policies and standards;
 - 7.2.2 Lead the review and revision of countywide information security and privacy policies and standards;
 - 7.2.3 Develop the county's information security management system;
 - 7.2.4 Report the status of information security countywide to the CIO.
- 7.3 **Technology governance:** endorses information security strategies and countywide information security policies, standards and guidelines.
- 7.4 **TMB security sub team:** develops countywide information security policies, standards and guidelines, plans and executes security initiatives, and reports on the county's information security health to the chief information officer.
- 7.5 **Organization IT Management:** is accountable for the organization's information security practices to protect the operations and assets under their control, manages the organization's information security, ensures organization compliance with information security policies and standards, implements, manages and supports information systems in compliance with information security policies, standards and procedures, and securely uses information and information systems.
- 7.6 **Information Owners:**
- 7.6.1 Providing appropriate protections to maintain the accuracy and integrity, determine the appropriate sensitivity or classification level of Information Assets
 - 7.6.2 Reviewing the aspects referenced in 7.5.1 on a regular basis for the Information Assets within their control.
 - 7.6.3 Ensuring that the Information Asset adheres to policy.

Enterprise Information Security Policy

7.7 Security Leads:

7.7.1 Assist in the identification and lead the implementation of security controls;

7.8 Information Custodians:

7.8.1 Identify specific control procedures, administering information Access Controls, implementing and maintaining cost-effective information control measures, and providing recovery capabilities consistent with the instructions of Information Owners;

7.8.2 Implementing appropriate security controls as directed by Information Owners and/or the Chief Information Security and Privacy Officer.

7.9 Workforce Members: Ensuring that information security and privacy policies and standards are adhered to in their daily activities.