Attachment C

King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Employee and Third Party Policy for Information Technology Security and Privacy Policy	ITG-P-08-03
Chief Information Officer Approval / Date: 12/15/08	**Effective Date:** 12/15/08

1.0 PURPOSE:

This policy establishes the information security and privacy practices related to hiring, user access to and confidentiality of King County Information Technology Assets, training, management oversight and reporting, performance reviews, discipline up to and including separation, and procurement contracts. These practices begin before employment or contract commencement, personnel guidelines and contract language that articulate expectations for information security and privacy, and continue until separation from employment or contract termination. The intent of this policy is to reduce risks to King County from errors, theft, fraud or misuse by employees and third parties.

2.0 APPLICABILITY:

King County Workforce Members (as defined in the Acceptable Use Policy) who are using King County Information Technology Assets or Resources.

3.0 REFERENCES:

3.1 Enterprise Information Security Policy.

3.2 RCW 42.56 (Washington Public Records Act).

3.3 Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines.

3.4 Acceptable Use of Information Technology Assets Policy.

3.5 King County's Security Incident Response Plan.

4.0 DEFINITIONS:

4.1 **Acknowledgement of Information Technology Security Responsibilities and Confidentiality (AISRC):** This is a combination of a non-disclosure document and an acknowledgement of employee responsibilities relative to Information Technology Security and privacy.

4.2 **Computer-Related Position Of Trust:** This is a position that has elevated network and/or system privileges, including but not be limited to LAN administrators, systems

engineers, network engineers, database administrators, PC support technicians, and help desk technicians.

4.3 **Elevated Network And/Or System Privileges:** Network and/or system rights and/or responsibilities that are greater than those of a standard data user. Functions performed by individuals having these privileges may include but are not limited to:

- Creating, deleting or modifying network, e-mail, or database user accounts;
- Resetting passwords on any system;
- Performing routine network (LAN/WAN), database, or PC maintenance and support;
- Having discretion and ability to grant rights to any system or information asset higher than the user's default rights.

4.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization and that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

4.5 **Business Owner:** The entity, in this case King County, that is responsible for protecting an Information Technology Asset, maintaining accuracy and integrity of the Information Technology Asset, determining the appropriate data sensitivity or classification level for the Information Technology Asset and regularly reviewing its level for appropriateness, and ensuring that the Information Technology Asset adheres to policy.

4.6 **Information System:** Software, hardware and interface components that work together to perform a set of business functions.

4.7 **Least Privilege:** Granting a user only those access rights required to perform official job duties.

4.8 **Non-Disclosure Agreement (NDA):** A legally binding document that protects the confidentiality of ideas, designs, plans, concepts, proprietary commercial material, vital government information, or personal information. Every NDA is subject to the provisions of the Washington Public Disclosure Act (RCW 42.17).

4.9 **Organization:** Every county office, every officer, every institution, and every department, division, board and commission.

4.10 **Separation Of Duties:** The practice of purposefully dividing roles and responsibilities, so a single individual cannot subvert a process.

4.11 **Third Party:** Any person, group of persons or organization that has a business relationship with the county.

4.12 **User:** Any individual performing work for King County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker. Each term is used in the general sense and is not

intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

4.13 **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, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

5.0 POLICIES:

5.1 **Employee Acknowledgement of Information Technology Security Responsibilities and Confidentiality (AISRC).**

5.1.1 **Employee AISRC:** An employee whose job function requires access to proprietary, secure or confidential information shall be required to sign a AISRC as a condition of employment. Organizations shall maintain on file the signed AISRC.

5.2 **User Access:** Organizations must have formal documented procedures in compliance with this policy for authorizing appropriate access to Information Technology Assets that includes granting different levels of access to Information Technology Assets, tracking and logging authorization of access to Information Technology Assets, and regularly reviewing and revising, as necessary, authorization of access to Information Technology Assets.

5.2.1 **Granting Access:** The Business Owner shall explicitly grant access to Information Technology Assets based on Least Privilege to an employee or Third Party and shall not allow access by default.

5.2.2 **Gaining Access:** Employees or Third Parties shall not attempt to gain access to Information Technology Assets for which they have not been given proper access authorization.

5.2.3 **Removing Access:** Organizations shall remove access to all Information Technology Assets and remove network and resource privileges at the time an employee or Third Party is separated from King County or when an employee or Third Party no longer needs to access them.

5.3 **Management Oversight:**

5.3.1 **Oversight:** Organizations shall provide oversight for employees and Third Parties who have access to proprietary, secure or confidential information, or are working in restricted areas that may include specific supervision.

5.3.2 **Contracts:** Organizations shall include the following provision in King County procurement contracts involving proprietary, secure or confidential Information Technology Assets:

"Contractor warrants and represents that each and every Contractor employee working on this contract can meet the following requirements:

- No convictions within the past ten (10) years for crimes involving computers, moral turpitude, including fraud, perjury, or dishonesty;
- No adverse employment actions within the past ten (10) years regarding dishonesty or the use or misuse of computers;
- Contractor shall, on an annual basis, confirm that it meets the requirements of this section."

5.3.3 **Vendor NDA:** Organization shall require vendors to sign a non-disclosure agreement when the work requires the vendor to have access to proprietary, secure or confidential information.

5.3.4 **Policy Compliance:** Organizations shall require vendors to adhere to countywide and Organization-specific information security and privacy policies, standards, methods and procedures.

5.4 **Incident Reporting:** Employees and Third Parties shall report to management any incident affecting information security and privacy, and all observed and suspected security weaknesses in or threats to Information Technology Assets.

5.5 **Employee Performance Reviews:** Organizations shall instruct employees regarding compliance with countywide and Organization-specific information security and privacy policies, standards, methods, practices, and procedures for all employees in a Computer-Related Position of Trust and hold them accountable for following such policies. Where applicable and appropriate, adherence to these standards should be considered in employees' performance evaluations.

5.6 **Action for Breaches of Policies and Standards:** Organizations shall utilize appropriate actions or measures for breaches of information security and privacy policies and standards consistent with county 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.

5.7 **Separating Employees and Third Parties:**

5.7.1 **Separation of Employees in Computer Related Positions of Trust:** Organizations shall have formal documented procedures for removing access rights of a departing employee in a Computer-Related Position Of Trust or Third Party who has had access to Information Technology Assets.

5.7.2 **Removal of Access Rights:** Organizations shall remove all access rights to Information Technology Assets granted to the employee or Third Party who is being non-voluntarily separated.

5.7.3 **Confidential, Proprietary and Non-Public Information:** The separated employee or Third Party shall not retain, give away, or remove from county premises any county proprietary information (electronic or hardcopy) except (1) personal copies of information disseminated to the public, and (2) personal copies of correspondence directly related to the terms and conditions of employment. At the time of departure, the separated employee or Third Party

shall relinquish all other county proprietary information or Information Technology Assets in his/her custody to his/her immediate King County supervisor or designate.

5.7.4 **County Property:** At the time of separation, the employee or Third Party shall return to his/her immediate King County supervisor or designee all county property in his/her possession, including but not limited to portable computers, printers, modems, software, personal digital assistants, documentation, building keys, lock combinations, encryption keys, and magnetic access cards.

5.7.5 **Physical Access:** Organizations shall deactivate or change all physical security access codes, such as a keypad lock PIN, used to protect Information Technology Assets that are known by the separating employee or Third Party.

5.8 **Separation Of Duties:** Organizations shall structure job functions to ensure a Separation Of Duties and an audit trail of actions taken where collusion could harm King County's information security and/or privacy.

5.9 **New Employees:** Organizations shall inform new employees who access County Information Technology Assets of the countywide and Organization-specific information security and privacy policies, standards, guidelines, methods, practices and procedures.

5.10 **Existing Employees:** Organizations should provide regular updates to employees who access Information Technology Assets, including but not limited to information security and privacy awareness training, updates to Countywide and Organization-specific information security and privacy policies, standards, guidelines, methods, practices and procedures, and process for reporting information security and privacy incidents and vulnerabilities.

6.0 EXCEPTIONS:

6.1 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 **Organization staff** protects the integrity, availability and confidentiality of King County's Information Technology Assets by complying with countywide and Organization-specific information security and privacy policies, standards, method and procedures and the non-disclosure agreement.

7.2 **Third Party** protects the integrity, availability and confidentiality of King County's Information Technology Assets by complying with information security and privacy policies, standards, method and procedures and the non-disclosure agreement with King County.

7.3 **Organization IT management** ensures that access rights are granted and removed accurately and timely.

7.4 **Business Owner** provides clear direction to management and the appropriate IT organization on assignment of access rights to the Information Technology Assets for which they have responsibility.

7.5 **Organization management** ensures that:

7.5.1 Responses are appropriate as outlined in the Incident Response Guidelines (draft) to incident reports as described in section 5.4 or as outlined in agency specific policy or procedure.

7.5.2 Procedures are in place and are followed by staff to notify the appropriate IT organizations of creations, deletions and changes to user access rights and accounts.

7.5.3 Signed AISRCs are maintained on file.

7.5.4 All employees:

7.5.4.1 Receive appropriate Information Security and Privacy information;

7.5.4.2 Understand the countywide and Organization-specific policies, standards, methods and procedures, as appropriate; they must comply with and receive feedback on compliance during performance reviews;

7.5.4.3 Understand the terms and conditions of employment, contract or agreement, and job functions.

7.5.5 All Third Parties with access to county Information Technology Assets shall:

7.5.5.1 Receive necessary security and privacy information related to King County policies, standards, methods and procedures to ensure satisfactory levels of Confidentiality, Integrity and Availability;

7.5.5.2 Understand and comply with King County policies, standards, methods and procedures;

7.5.5.3 Understand the terms and conditions of the contract or agreement;

7.5.5.4 Have signed a King County nondisclosure agreement and maintain a copy as part of the contract;

7.5.5.5 Ensure that contracts are evaluated to contain the proper warranties regarding contractor staff;

7.5.5.6 Ensure that contractors maintain compliance with countywide and Organization-specific policies, standards, guidelines, methods, practices and procedures.

7.6 **County information security officer** provides countywide guidance and oversight on addressing information security concerns in the hiring and contracting process, in position descriptions, through training and employee reviews, and in managing access rights to Information Technology Assets.

7.7 **County information privacy officer** provides countywide guidance on addressing information privacy concerns through the use of nondisclosure agreements and in training.