King County

1200 King County Courthouse
516 Third Avenue
Seattle, WA 98104

# KING COUNTY

## Signature Report

**December 13, 2010**

**Motion 13397**

**Proposed No.** 2010-0575.2 **Sponsors** Lambert

A MOTION approving written identity theft prevention programs for the department of natural resources and parks and the Seattle-King County department of public health in compliance with sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, and the Red Flags Rule adopted by the Federal Trade Commission; and the enterprise, employee and third party information security, and information privacy policies promulgated by the office of information resource management.

WHEREAS, Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, required the Federal Trade Commission ("FTC") to adopt rules to prevent identity theft from information gathered and maintained by financial institutions, utilities and other creditors, and

WHEREAS, the FTC adopted a new rule on identity theft, known as the "Red Flags Rule," that require financial institutions, utilities and other creditors to set up a program aimed at preventing identity theft, and

WHEREAS, the King County wastewater treatment division ("WTD") provides regional sewer services to thirty-four local sewer utilities and those local sewer utilities

bill customers directly for local sewer charges and the King County wholesale sewer rate, and

WHEREAS, WTD is authorized under RCW 35.58.570 and 36.94.140 to impose a capacity charge for new connections to its system, and

WHEREAS, pursuant to K.C.C. 28.84.050, WTD's capacity charge is billed for a fifteen-year period with the customer receiving a discount for paying the full amount earlier, and

WHEREAS, the Red Flags Rule defines a "covered account" as either:

1. A consumer account that allows multiple payments or transactions; or

2. Any other account that presents a reasonably foreseeable risk from identity theft, and

WHEREAS, WTD currently maintains over eighty thousand continuing accounts for customers paying the county's capacity charge which may involve multiple payments or transactions, and

WHEREAS, the Red Flags Rule requires those utilities and other creditors having "covered accounts" to develop and implement a written Identity Theft Prevention Program, attached to this motion as Attachment A and incorporated in this motion by this reference, for the detection, prevention and mitigation of identity theft in connection with certain accounts, and

WHEREAS, the Seattle-King County department of public health manages transactional systems and processes with identifying information subject to the Red Flags Rule, and

WHEREAS, the Red Flags Rule requires agencies having "covered accounts" to develop and implement a written program, attached to this motion as Attachment B and incorporated in this motion by this reference, for the detection, prevention and mitigation of identity theft, and

WHEREAS, the office of information resource management has promulgated the following policies: Employee and Third Party Policy for Information Technology Security and Privacy Policy; and the Enterprise Information Security Policy, and

WHEREAS, these policies were adopted by the county's information technology governance committees, and

WHEREAS, these policies apply to all county agencies and workforce members, and support the intent of the Red Flags Rule, and

WHEREAS, the King County council finds the department of natural resources and parks and the Seattle-King County department of public health Programs are sufficient to comply with the Red Flags Rule, and

WHEREAS, the King County council also finds the Employee and Third Party Policy for Information Technology Security and Privacy Policy and the Enterprise Information Security Policy promulgated by the office of information resource management comply with the intent of the Red Flags Rule;

NOW, THEREFORE, BE IT MOVED by the Council of King County:

The identity theft prevention programs developed for the department of natural resources and parks and the Seattle-King County department of public health, which are Attachments A and B to this motion, respectively, and the information security policies promulgated by the office of information resource management, which are Attachments

C and D to this motion, are hereby approved. The council intends to consider for adoption an information privacy policy during 2011.

Motion 13397 was introduced on 12/6/2010 and passed by the Metropolitan King County Council on 12/13/2010, by the following vote:

Yes: 9 - Mr. Phillips, Mr. von Reichbauer, Mr. Gossett, Ms. Hague, Ms. Patterson, Ms. Lambert, Mr. Ferguson, Mr. Dunn and Mr. McDermott
No: 0
Excused: 0

KING COUNTY COUNCIL
KING COUNTY, WASHINGTON

Robert W. Ferguson, Chair

ATTEST:

Anne Noris, Clerk of the Council

**Attachments:** A. Identity Theft Prevention Program--Department of Natural Resources and Parks--Effective Date June 1, 2010, B. Identity Theft Prevention Program--Public Health-Seattle & King County--Effective Date October 30, 2009, C. Employee and Third Party Policy for Information Technology Security and Privacy Policy--Effective Date 12/15/08, D. Enterprise Information Security Policy--Effective Date 9/9/09

13397

Attachment A

King County
King County **Department Policies and Procedures**

General Department
Policies & Procedures

| Title Policy: | Document Code No. |
|---|---|
| Identity Theft Prevention Program | DP-FIN-062010 |
| Department/Issuing Agency: Department of Natural Resources and Parks | Effective Date: June 1, 2010 |

Approved
Bob Burns

1.0 SUBJECT TITLE: Identity Theft Prevention Program

1.1 Effective Date: June 1, 2010

1.2 Type of Action: New

1.3 Key Words: Fraud, Identity Theft, Red Flag, Service Provider.

2.0 PURPOSE:

To establish a policy within the Department of Natural Resources and Parks (DNRP) outlining protocols, standards, schedule, responsibilities and associated actions aimed meet the requirements set forth in the Federal Trade Commission's (FTC) Red Flags Rules mandated by 16 CFR § 681.1.

3.0 ORGANIZATIONS AFFECTED: Applicable to the Department of Natural Resources and Parks (DNRP).

4.0 REFERENCES:

4.1 Fair and Accurate Credit Transactions Act of 2003 (FACTA)

4.2 16 CFR § 681.1- Federal Trade Commission Identity Theft Rules

4.3 KC DNRP Wastewater Treatment Division Identity Theft Prevention Program (Appendix)

5.0 DEFINITIONS:

5.1 "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.

5.2 "Covered Account" means:

a) any account DNRP business units offer or maintain primarily for personal, family or household purposes, that involves multiple payments or transactions (currently only the Capacity Charge Program associated with our Wastewater Treatment Division utility meets this definition); and

b) any other account the Department offers or maintains for which there is a foreseeably reasonable risk to customers or to the safety and soundness of the Department from Identity Theft.

5.3 "Fraud" means an intentional deception made for personal gain or to damage another individual.

5.4 "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

5.5 "Mitigation" means activities designed to lessen the severity or intensity of damage created by identity theft.

5.6 "Red Flags" means potential patterns, practices, or specific activities indicating the possibility of identity theft.

6.0 POLICIES:

6.1 DNRP will maintain and administer an Identity Theft Prevention Program in order to detect, prevent, and mitigate financial identity theft.

6.2 The Chief Financial Officer (CFO) is the chief official for this policy and is responsible for the administration and maintenance of the policy.

6.3 Administration of this policy shall include an annual review of DNRP's business units to determine whether any additional units have accounts covered by Section 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. At the outset of this program's development we found only one business unit that has a covered account: the Capacity Charge Program in our Wastewater Treatment Division (see Appendix A: Identify Theft Prevention Program for Wastewater Treatment Division).

6.4 Maintenance of this policy shall include annual review of the policy language and procedures to ensure that it is kept current and relevant.

7.0 PROCEDURES

Action By: Chief Financial Officer

Action:

7.1 Annually, the CFO shall initiate a review process to identify any additional DNRP business units that may have covered accounts.

Action By: Division Finance Managers

Action:

7.2 Where covered accounts are identified within their divisions, Division Finance Managers shall develop division level compliance procedures consistent with this policy and its purpose. Division-level procedures will be incorporated as appendices to this policy as part of the annual policy review process.

7.3 Either assume or designate responsibility to serve as the Program Administrator for the Division-level Identity Theft Prevention Program.

Action By: Chief Financial Officer

Action:

7.4 Where indicated by the development of new or revised division level procedure documents (which are appended to this policy document), the CFO shall make necessary updates to this Department Policy to incorporate appropriate language revision and the addition of or revision to appendices.

8.0 RESPONSIBILITIES:

8.1 CFO is responsible for initiating and conducting an annual review of accounts to determine whether there are additional covered accounts.

8.2 Division Financial Officer is responsible for developing division level compliance procedures for covered accounts and for serving as or assigning a Program Administrator to implement the compliance procedures for the division.

8.3 Program Administrator coordinates and has oversight for the implementation of division-level compliance procedures, which might also be known as a division-level Identity Theft Prevention Program.

9.0 APPENDICES:

9.1 KC DNRP Wastewater Treatment Division Identity Theft Prevention Program

Appendix A

**King County Department of Natural Resources and Parks**
**Wastewater Treatment Division**

**Identity Theft Prevention Program**
**Effective June 1, 2010**

## I. PROGRAM ADOPTION

The county's Wastewater Treatment Division ("Division"), Department of Natural Resources and Parks, staff developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the Division's operations and account systems, and as well as the nature and scope of its activities, this Program was developed and became an administrative policy of the Division with oversight by the Department's Chief Financial Officer ("Program Administrator").

## II. PROGRAM PURPOSE AND DEFINITIONS

### A. Fulfilling Requirements of the Red Flags Rule

Under the Rule, every financial institution and creditor is required to establish a Program tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

### B. Red Flags Rule Definitions Used in This Program

For the purposes of this Program, the following definitions apply:

1. Account. "Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.
2. Covered Account. A "covered account" means:
   a. Any account the utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
   b. Any other account the Division offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Division from Identify Theft.

3. Creditor. "Creditor" means a person or entity that arranges for the extension, renewal or continuation of credit, including the Division's Capacity Charge Program.

4. Customer. A "customer" means a person or business entity that has a covered account with the Division.

5. Financial Institution. "Financial institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a customer.

6. Identifying Information. "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number or unique electronic identification number.

7. Identity Theft. "Identity theft" means fraud committed using the identifying information of another person.

8. Red Flag. A "red flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

9. Service Provider. "Service provider" means a person or business entity that provides a service directly to the Division relating to or in connection with a covered account.

## III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Division shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. The Division identifies the following potential Red Flags, in each of the listed categories which might affect the Division's covered accounts:

### A. Notifications and Warnings from Credit Reporting Agencies

**Red Flags**

Because the Division does not obtain a customer's credit history before opening an account, the Division does not receive notifications or warnings from credit reporting agencies and, therefore, has not identified any red flags in this category.

### B. Suspicious Documents

**Red Flag**

1. Documents with information that is not consistent with existing customer information.

C. Suspicious Personal Identifying Information

Red Flags

1. Incomplete identifying information on a residential or non-residential sewer use certification form submitted by the local sewer agency; and
2. Identifying information on a residential or non-residential sewer use certification form submitted by a property owner rather than the local sewer agency.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Any attempt to use a credit card to pay an account when the name on the card is different from the customer listed on the account; and
2. Breach in the Division's computer system security.

E. Alerts from Others

Red Flag

Because the Division does not obtain a customer's credit history before opening an account for a customer, the Division does not receive notifications or warnings from credit reporting agencies and, therefore, has not identified any red flags in this category.

## IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, Division personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. Only open a new account if the residential or non-residential sewer use certification form is complete and was submitted to the Division by a local sewer agency that is in compliance with the Red Flags Rule; and
2. Verify billing information for a business entity.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, Division personnel will take the following steps to monitor transactions with an account:

Detect Red Flags

1. Require requests to change billing addresses to be in writing or verify a change of address using parcel viewer; and
2. Require certain identifying information such as name or residential or business address, as well as the security code on the credit card, before accepting a credit card payment.

## V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Division personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

### A. Prevent and Mitigate Identity Theft

1. Contact the customer with the covered account;
2. Not open a new covered account;
3. Notify the Program Administrator for determination of the appropriate step(s) to take;
4. Notify law enforcement; or
5. Determine that no response is warranted under the particular circumstances.

### B. Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Division accounts, the Division shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the Division website but provide clear notice that the website is not secure;
2. Make office computers password protected and provide that computer screens lock after a set period of time;
3. Require personnel to enter all credit card payment information directly into the computer without writing down the information;
4. Personnel accepting credit card information in order to process a payment shall be required to sign an Acknowledgement of Information Security Responsibilities and Confidentiality.
5. Maintain computer virus protection up to date; and
6. Require and keep only the kinds of customer information that are necessary for Division purposes.

## VI. PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the Division from Identity Theft. The Program Administrator shall at least annually consider the Department's experiences with Identity Theft, changes in Identity methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Department maintains and changes in the Department's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted.

## VIII. PROGRAM ADMINISTRATION.

### A. Oversight

The Program Administrator shall be responsible for the Program administration, reviewing any staff reports regarding the detection of Red Flags, the steps for preventing and mitigating taken in particular circumstances and considering periodic changes to the Program.

### B. Staff Training and Reports

Division staff responsible for implementing the Program shall be trained either by or under the direction of the Division Finance Manager in the detection of Red Flags, and responsive steps to be taken when a Red Flag is detected.

### C. Service Provider Arrangements

In the event the Division engages a service provider to perform an activity in connection with one or more covered accounts, the Division shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to Division covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program and agree to report promptly to the Division in writing if the service provider in connection with a Division covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

### D. Customer Identifying Information and Public Disclosure

The identifying information of Division customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law.

13397

Attachment B

Public Health
Seattle & King County

Department Policies

| Title | Document Code No. |
|---|---|
| Identity Theft Prevention Program | INF 2-3 (DPH DP) |
| Department/Issuing Agency: Public Health – Seattle & King County | Effective Date: October 30, 2009 |
| Approved: DPH Director | |

1.0 SUBJECT TITLE: Identity Theft Prevention Program

1.1 EFFECTIVE DATE: October 30, 2009

1.2 TYPE OF ACTION: New

1.3 KEY WORDS: Fraud, Identity, Red Flags

2.0 PURPOSE:

To establish an identity theft prevention program that meets the requirements of the Federal Trade Commission's (FTC) Red Flags Rules mandated by 16 CFR § 681.1.

3.0 ORGANIZATIONS AFFECTED:

Applicable to the Department of Public Health Seattle-King County (PHSKC).

4.0 REFERENCES

4.1 Fair and Accurate Credit Transactions Act of 2003 (FACTA)

4.2 16 CFR § 681.1 – Federal Trade Commission, Identity Theft Rules

4.3 45 CFR Part 164 – Health Insurance Portability and Accountability Act

4.4 RCW 9.35.020 – Identity Theft

4.5 RCW 19.182 – Washington Fair Credit Reporting Act

5.0 DEFINITIONS:

5.1 "Fraud" means an intentional deception made for personal gain or to damage another individual.

5.2 "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including

5.2.1 Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, medical coupon/card, employer or taxpayer identification number, credit card number;

5.2.2 Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

5.2.3 Unique electronic identification number, address, or routing code; or

5.2.4 Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

5.3 "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

5.3.1 "Medical Identity Theft" means the use of a person's name and/or other parts of their identity without the person's knowledge or consent to obtain medical services or goods. Medical identity theft also occurs when an individual uses another person's identity to submit false claims for medical services and falsifying medical records to support those claims.

5.4 "Mitigation" means activities designed to lessen the severity or intensity of damage created by identity theft.

5.5 "Red Flags" means potential patterns, practices, or specific activities indicating the possibility of identity theft.

5.6 "Red Flags Rule" means the FTC rule that requires a written Identity Theft Prevention Program designed to detect the red flags of identity theft, take steps to prevent the crime, and to mitigate damage from identity theft.

5.7 "Safeguards" means precautionary activities to protect identifying information.

5.8 "Workforce" means employees, volunteers, trainees, and other persons in Public Health whose conduct, in the performance of work, is under the direct control of Public Health, whether or not they are paid by Public Health. Workforce includes, but is not limited to, other categories of persons including contract employees, students, and work study students/interns.

6.0 POLICIES:

6.1 PHSKC will maintain and administer an Identity Theft Prevention Program in order to detect, prevent, and mitigate financial and medical identity theft.

6.2 The Chief Financial Officer (CFO) is the chief official for this policy and is responsible for the administration and maintenance of the policy.

6.3 All managers/supervisors will assess transactional systems and processes that contain personal identifying information that may present opportunities for identity theft.

6.3.1 The assessment will identify potential red flags using Appendix 9.1, Indicators of Potential Identity Theft Red Flags.

6.3.2 When the red flags are identified, determine actions that can be taken to eliminate or reduce identity theft.

6.3.3 This assessment will be documented on the Red Flag Assessment Form (Appendix 9.2) and will be conducted whenever a transactional system or process is added, deleted, or modified.

6.3.3.1 If a manager/supervisor believes that a system or process is of minimal risk, not requiring red flag identification he/she shall provide the basis of this to the CFO who will make the final determination of red flag designation.

6.3.4 The results of the assessment will be provided to the CFO.

6.4 The workforce will be trained on this policy and operational procedures upon initial employment with the department and additionally as needed.

6.5 The workforce will be trained to look for red flags that may indicate the potential for identity theft. To detect red flags, the workforce should use alternative information to verify identity such as:

- Driver's license, passport, or other photo identification
- Social Security Number
- Date of birth
- Residence address and telephone number
- Insurance card (if available)
- Other identifying information (i.e. challenge questions, library card, utility bill, etc.)

6.5.1 When a workforce member discovers a red flag, he/she shall report this to their supervisor immediately.

6.6 Whenever an attempted or actual identity theft is reported, the supervisor will immediately report the incident by phone to the Compliance Office, who shall notify the CFO. The supervisor will follow up with a written incident/accident report.

6.7 When identity theft is reported, a mitigation plan that has a strong focus on helping the victims of this crime will be developed. Mitigation strategies may include:

- Monitoring for evidence of identity theft;
- Contacting the client;
- Changing any passwords, security codes, or other security devices that permit access to personal information; and
- Notifying law enforcement.

6.8 Managers/supervisors will evaluate ways to reduce potential identity theft through internal safeguards and practices. For example, limiting the use of a social security number, not photocopying documents unless necessary, ensuring that credit card and bank account numbers are appropriately safeguarded, etc.

6.9 This policy shall be reviewed at least annually.

7.0 PROCEDURES:

**Action By:** Managers/Supervisors

**Action:**

7.1 Assess all transactional systems and processes for identifying information.

7.2 Identify potential red flags of identity theft for the system or process.

7.3 Provide the results of the assessment to the CFO.

7.4 Ensure the workforce is trained on this policy and operational procedures to prevent identity theft.

**Action By:** Workforce

**Action:**

7.5 Know the red flags for potential identity theft.

7.6 Be alert for potential patterns, practices, or specific activities indicating the possibility of identity theft. Immediately report attempted or actual identity theft to the supervisor.

**Action By:** Supervisor/Division Manager

**Action:**

7.7 Immediately report any attempted or actual identity theft to the Compliance Office by phone, followed up with an incident/accident report.

**Action By:** Compliance Office

**Action:**

7.8 Notify the CFO when receiving a report of attempted or actual identity theft.

**Action By:** Chief Finance Officer

**Action:**

7.9 Review all evaluations of transactional systems and processes.

7.10 Review all reports of attempted or actual theft of identifying information and take appropriate action.

8.0 RESPONSIBILITIES:

8.1 Managers/supervisors are responsible for identifying transactional systems and processes for identifying information, determine red flags for these systems/transactions, and training the workforce on this policy and operational procedures to prevent identity theft. They will also immediately report to the Compliance Office any attempted or actual identity theft.

8.2 The workforce is responsible for being alert for red flags or suspicious activity in transactional systems and processes and reporting this to their manager/supervisor.

8.3 The CFO is responsible for reviewing all evaluations of transactional systems and processes and reviewing reports of attempted or actual identity theft and determining appropriate corrective actions to be taken.

9.0 APPENDICES:

9.1 Indicators of Potential Identity Theft

9.2 Red Flag Assessment Form

| Policy Owner | Last Review Date | Comments |
|---|---|---|
| CFO | | Established |

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.

13397

Attachment D

King County

Office of Information
Resource Management

## Information Technology Governance Policies and Standards

| Title | Document Code No. |
|---|---|
| **Enterprise Information Security Policy** | ITG-POS-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.

- 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, defect 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

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.

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.

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.