Attachment G

King County

Addendum D

Office of Information
Resource Management

## Information Technology Governance Policies, Standards and Guidelines

| Title | Document Code No. |
|---|---|
| **Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines** | |
| Chief Information Officer Approval / Date | Effective Date. |

### 1.0 PURPOSE:

This guideline provides King County Organizations information relative to when an agreement should be signed by persons in a Computer-Related Position of Trust who have access to proprietary, secure or confidential information. Included in these guidelines is a model agreement that acknowledges the individual's responsibility.

### 2.0 REFERENCES:

2.1 Employee and Third Party Policy for Information Technology Security and Privacy.

### 3.0 DEFINITIONS:

3.1 **Acknowledgement of Information Security Responsibilities and Confidentiality:** This is a combination of a non-disclosure agreement and a general acknowledgement of responsibilities relative to Information Security and privacy.

3.2 **Computer-Related Position Of Trust:** This is a position with elevated network and/or system privileges, including but not limited to LAN administrators, systems engineers, network engineers, database administrators, PC support technicians, and help desk technicians.

3.3 **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.

3.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization 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.

3.5 **Information Owner:** The person who is responsible for protecting an Information Asset, maintaining accuracy and integrity of the Information Asset, determining the appropriate data sensitivity or classification level for the Information Asset and regularly reviewing its level for appropriateness, and ensuring that the Information Asset adheres to policy. The information owner is one or both of the following:

- The creator of the information or the manager of the creator of the information;
- The receiver of external information or the manager of the receiver of the external information.

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

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

## 4.0 GUIDELINES:

4.1 Organizations should have each person in a Computer-Related Position of Trust sign an Acknowledgement of Information Security Responsibilities and Confidentiality, including third parties as appropriate to their contract or agreement with King County.

4.2 The Acknowledgement of Information Security Responsibilities and Confidentiality should be signed by both the person in a Computer-Related Position of Trust and acknowledged by the supervisor or manager for this position. This should be signed prior to the person's first day working in a Computer-Related Position of Trust and annually thereafter.

4.3 Organizations shall request that other workforce members with access to proprietary, secure or confidential King County information sign the Acknowledgement of Information Security Responsibilities and Confidentiality.

4.4 After the Acknowledgement of Information Security Responsibilities and Confidentiality is signed a copy should be given to the employee, contractor, consultant, etc. and the original filed in either the departmental personnel file (in the case of employees) or maintained with the official contract file (in the case of contractors, consultants, etc.).

## 5.0 APPENDICES:

## Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines

5.1 Model: Acknowledgement of Information Security Responsibilities and Confidentiality (see next page).