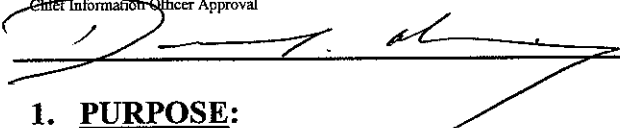




Information Technology Governance Policies & Standards

Title REMOTE ACCESS POLICY	Document Code No. ITG-P-07-04
Chief Information Officer Approval 	Date 10/3/07 Effective Date.

1. PURPOSE:

This policy is designed to minimize the potential exposure to King County from damages that may result from authorized or unauthorized use of King County resources. These damages include the exposure of privileged and protected information, loss of sensitive or confidential county data, intellectual property, harm to public image, and damage to critical King County internal Systems, etc.

The **Remote Access Policy** outlines approved methods for accessing King County's Enterprise Network resources from a remote host. This document establishes policies governing the procedures and limitations by which Workforce Members gain or lose Remote Access and by which processes Remote Access privileges are extended or narrowed.

2. APPLICABILITY:

This policy applies to all King County Organizations and Workforce Members.

3. REFERENCES:

- 3.1. *Concerned Ratepayers Association v. Public Utility District No. 1*, 138 Wn.2d 950, 958, 983, P.2d 635 (1999) (PAO Memorandum of 1 August 2007)
- 3.2. King County Administrative Policies and Procedures; Executive Orders, Policies and Procedures
- 3.3. King County Enterprise Information Security Policy
- 3.4. King County Password Management Policy
- 3.5. National Security Association (NSA) Security Configuration Guide
- 3.6. King County External Network and Systems Connectivity Policy
- 3.7. King County External Network and Systems Connectivity Standard
- 3.8. Information Technology Policy and Standards Exception Request Process

4. **DEFINITIONS:**

- 4.1. **Agreement:** Any document detailing the specifics of a relationship between parties. Examples include, but are not limited to, contracts, memorandums of understanding (MOU), and memorandums of agreement (MOA) or service level agreements (SLA).
- 4.2. **Anti-Virus Software:** Software that searches for known viruses, worms, Trojan horses and other malicious software.
- 4.3. **Asymmetric Cryptosystem:** A suite of algorithms needed to implement a particular form of encryption and decryption. In asymmetric operations it takes longer to compress and encrypt data than to decompress and decrypt it.
- 4.4. **Business Partner:** Outside businesses associated or “partnered” with a Vendor doing business with King County.
- 4.5. **County Enterprise Network:** The Network used to conduct county business that provides transport of data within and between county facilities and other agencies of county government. This definition also refers to the Network used to transport data between the county, other government agencies and the Internet. It does not refer to Networks built for the sole purpose of meeting special operations needs of county business units, including process control and supervisory control Networks. Nor does it refer to the King County Institutional Network (I-Net), which is required to meet contractual obligations with I-Net customers and the local cable television utility.
- 4.6. **Digital Subscriber Line (DSL):** Public Network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site.
- 4.7. **Due Care:** The care that a reasonable person would exercise under the circumstances; the standard for determining legal duty.
- 4.8. **Firewall:** Router or access server, or several routers or access servers, designated as a buffer between any connected public Networks and a private Network. A firewall router uses access lists and other methods to ensure the security of the private Network.
- 4.9. **Idle:** Describes a computing circumstance in which there is no keyboard activity, no applications are running and nothing is being uploaded or downloaded.
- 4.10. **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 and regularly reviewing its level for appropriateness, and ensuring the Information Asset adheres to policy. The Information Owner is one or both of the following:
 - 4.10.1. The creator of the information or the manager of the creator of the information

Remote Access Policy

- 4.10.2. The receiver of external information or the manager of the receiver of the external information
- 4.11. **Local Area Network (LAN):** High-speed, low-error data Network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.
- 4.12. **Login or Logon:** The process of gaining access, or signing in, to a computer System. The process (the noun) is a "logon" or "login," while the act of doing it (the verb) is to "log on" or "log in."
- 4.13. **Network:** A System that transmits any combination of voice, video, and/or data between users. The network includes the network operating System in the client and server machines, the cables connecting them and all supporting hardware in between, such as bridges, routers, and switches. In wireless Systems, antennas and towers are also part of the network.
- 4.14. **Organization:** Every county office, every officer, every institution, whether educational, correctional or other; and every department, division, board, and commission.
- 4.15. **Public Record:** A Public Record includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used or retained by an agency regardless of physical form or characteristics.
- 4.16. **Remote Access:** The ability to log on to a computer or Network within an organization from an external non-county location. Remote Access is typically accomplished by directly dialing up analog or ISDN modems or via a connection to the Internet.
- 4.17. **Remote Access Profile:** An OIRM form that describes the type of access allowed and what King County resources are available to the Workforce Member.
- 4.18. **Resources:** Assets that can be used for help or support that can be drawn on when needed.
- 4.19. **Secure Sockets Layer (SSL):** The leading security protocol on the Internet. SSL is widely used to do two things: to validate the identity of a Web site and to create an encrypted connection between devices.
- 4.20. **Symmetric Cryptosystem:** A suite of algorithms needed to implement a particular form of encryption and decryption. In symmetric operations, it takes the same time to compress and encrypt data as it does to decompress and decrypt it.
- 4.21. **System:** Software, hardware, and interface components that work together to perform a set of business functions.
- 4.22. **Vendor:** A person or entity who is a seller of products or services to a King County Organization. Vendors can also be Workforce Members.

Remote Access Policy

- 4.23. **Virtual Private Network (VPN):** Enables IP traffic to travel securely over a public TCP/IP by encrypting all traffic from one Network to another. A VPN uses “tunneling” to encrypt all information at the IP level.
- 4.24. **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 services to King County.

5. POLICIES:

5.1. Approved Remote Access Methodologies

- 5.1.1. All Workforce Members are required to use only Remote Access methodologies approved by OIRM Network Engineering and the Chief Information Privacy and Security Officer (CISPO).
- 5.1.2. Virtual Private Networks (VPN) shall follow the IP Security (IPSec) or Secure Socket Layer (SSL) standard and uses an asymmetric or symmetric cryptographic key strength.

5.2. Access

- 5.2.1. No Workforce Member shall be granted Remote Access to the County Enterprise Network Resources except in accordance with a demonstrated need and permission from the proper authorities.
 - 5.2.1.1. The proper authorities for Workforce Members are the King County Information Owners.
- 5.2.2. Remote Access Workforce Members may be provided access to the same Systems and resources they currently access non-remotely. However, Workforce Members may receive a lesser degree of access via Remote Access methods, dependant upon the clearance received when their Remote Access is granted. In no case shall Remote Access Workforce Members be granted a greater degree of access than they are allowed via their direct connection.
- 5.2.3. Selected consultants and Vendors may be granted Remote Access to the County Enterprise Network, provided they have an Agreement with King County that clearly defines the type and scope of Remote Access permitted, as well as other conditions which may be required, such as Anti-Virus protection software. Such contractual provisions must be reviewed and approved by the Office of Information Resource Management (OIRM) Chief Information Security and Privacy Officer (CISPO) before Remote Access will be permitted.
- 5.2.4. King County shall reserve the right to electronically examine all devices connecting to the County Enterprise Network prior to granting access to the Network.

Remote Access Policy

- 5.2.6. The Workforce Member's need for Remote Access privileges shall be reviewed initially at approximately six (6) months and then annually thereafter by the appropriate supervisor or contract manager with the approval of the Organization's IT Service Delivery Manager (ITSDM).
 - 5.2.7. Approved Remote Access Workforce Members shall not permit unauthorized access by others, including family members, to the county computing environment.
 - 5.2.8. Remote Access Workforce Members shall not share their Remote Access credentials with anyone.
 - 5.2.9. Remote Access for King County employees may be allowed through the use of equipment owned by or leased to King County, or through the use of the employee's personal computer System, unless otherwise restricted by the Organization or Information Owner.
 - 5.2.9.1. "If a personal computer is used for any County business, it could be subject to electronic discovery rules during a lawsuit or the Washington Public Records Act. Any work-related emails, files, data or other record residing on a personal computer is subject to the same retention requirements as records on a County computer." (From PAO Memorandum of 1 August 2007.)
 - 5.2.10. King County is not responsible for the purchase, set-up, maintenance or support of any equipment that is not owned by or leased to King County.
- 5.3. **Management: King County**
- 5.3.1. A request to make changes to a Workforce Member's Remote Access Profile shall originate with his or her manager, supervisor or LAN Administrator.
 - 5.3.2. Immediate supervisors and division managers shall set-up Remote Access agreements so they expire on a routine basis, such as every six (6) months, up to a maximum of twelve (12) months. At the expiration of a Remote Access Agreement the employee would have the option of requesting a renewal.
 - 5.3.3. When a Workforce Member leaves the employ of King County Remote Access shall be disabled immediately upon departure.

5.4. **Security:**

- 5.4.1. Employees with Remote Access privileges shall take Due Care to protect the assets of King County. Remote Access Employees are accountable to adhere to the county's information security policy, standards and guidelines. Being approved for Remote Access does not diminish the responsibility of adhering to all provisions of security policies; in fact the responsibility is greater when working remotely. If the Workforce Member is uncertain of their level of risk through using Remote Access he or she should contact the CISPO's Office.

Remote Access Policy

- 5.4.2. The Remote Access Workforce Member is responsible for ensuring his or her personal computer has Anti-Virus Software running and is current with the engine and data files for the Vendor software used. The Anti-Virus Software should be updated weekly, at a minimum, and preferably once a day. Failure to have current Anti-Virus scanning continuously on a Workforce Member's personal computer may be cause to have the Workforce Member's Remote Access privileges revoked.
- 5.4.3. For the Workforce Member's protection and that of the System, Workforce Members shall follow the **King County Password Management Policy**.
 - 5.4.3.1. If your Remote Login information is stolen, compromised or potentially compromised, inform the OIRM Service Desk immediately.
- 5.4.4. All locally installed host applications and/or services required for Remote Access shall be set up for manual start and stop. Services shall be left in a stopped status when not in use.
- 5.4.5. While using Remote Access, Workforce Members with non-permanent connections are required to disconnect from the County Enterprise Network whenever their computer Systems are Idle for greater than fifteen (15) minutes.

6. EXCEPTIONS:

- 6.1. Any agency needing an exception to this policy must follow the **Information Technology Policy and Standards Exception Request Process** using the **Policy and Standards Exception 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. RESPONSIBILITIES:

- 7.1. The Chief Information Officer (CIO) is the approval authority for the **Remote Access Policy**
- 7.2. OIRM Network, Systems, and Operations is the steward of the Network infrastructure and is responsible for providing all transport services across the KC WAN. As such, OIRM will become the owners of the Network policies and standards.
- 7.3. OIRM is responsible for the operations and maintenance of all Network Infrastructure Equipment connected to the County Enterprise Network. OIRM is not responsible for Network Infrastructure Equipment that operates solely within a department LAN **and** that OIRM has previously determined neither connects to, nor affects the operation of the County Enterprise Network.

Remote Access Policy

- 7.4. OIRM is responsible for protecting the integrity of the County Enterprise Network. To meet this responsibility OIRM shall ensure compliance with the terms detailed in the **Remote Access Policy**.
- 7.5. CISPO shall be responsible for maintaining records associated with all Remote Access/VPN authorizations. Periodic audits of these records will be conducted and adjusted to meet current business requirements.
- 7.6. King County departments or agencies are responsible for informing their employees of this policy.
- 7.7. OIRM will develop standards and guidelines pertaining to access of internal System resources from a remote connection. These standards and guidelines will include, but are not limited to:
 - 7.7.1. Determining the business need required for having a Remote Access request approved
 - 7.7.2. Vendor software and version to be used in establishing the remote connection
 - 7.7.3. Responsibilities and requirements of the end-user: i.e. security patches, antivirus software, etc.
 - 7.7.4. Documentation of acceptable use of county resources from the remote connection
 - 7.7.5. Documented standards of end-user internet connectivity hardware: i.e. brand of DSL or cable modem, router and/or Firewall, etc.
 - 7.7.6. Standard authentication to be used