



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

SECTION 1: Purpose

The risk of disruption to City services or the City network (the Network) through the introduction of malicious code and/or exploitation of technical vulnerabilities is very high when remote and ad hoc connections by unauthorized or uncontrolled devices are allowed to connect to the Network.

The purpose of this policy is to define the types of devices allowed to connect to the Network on a remote or ad hoc basis and how their connection will be controlled and managed. Ad hoc connections refer to those that occur on an unplanned or unscheduled basis with computing devices not under direct maintenance and control of City Desktop, Server or Network Services. These devices are referred to as non-City owned.

The handling of City restricted or confidential data, that may reside on ad hoc devices, or is collected remotely, is included in this policy also. The City of Seattle's *IT Security Policy and Guidelines*, Section 7.2 provides data classification and related protective measures for data in general.

SECTION 2: Applicability

This Policy is applicable to the use of all computing and data storage devices, regardless of ownership. Any device that can be connected remotely or locally to a City wired or wireless network must adhere to these operating policies and guidelines. This policy also applies to servers that may be connected remotely or on an ad hoc basis to the Network.

This policy applies to connection access methods provided and maintained by the City for authorized business use. The connection types include wired, VPN, dialup, wireless, and Internet.

This policy applies to City employees, contractors, vendors, business partners, and other agents connecting a computing or data storage device to the Network. For the purpose of this policy, users have been defined as Authorized, Ad Hoc, and Contracted Vendor.

This policy must be explicitly referenced and included in all IT procurement activities and documents where applicable.

This policy may apply to public safety mobile computing devices or wireless connections for access to classified or emergency response applications and systems.

This policy does not apply to publicly accessible City of Seattle websites, including those sites that support business transactions and access to City data.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

This policy will be supported by connectivity management initiatives currently planned.

SECTION 3: Associated Policies

This policy augments the IT Security Policy and Guidelines (hereafter referred to as the ISSP) adopted Citywide in October of 2003. The IT Security Policy and Guidelines sections on acceptable usage, access controls, data confidentiality, etc. apply to all authorized and ad hoc users connecting to the Network.

Review the following policies for additional standards and guidelines that govern the use of City remote access methods:

- IT Security Policy and Guidelines - http://inweb/technology_security/policy.htm
- 802.11x Wireless Exception Process - http://inweb/technology_security/word/wireless_exception_process.doc
- PDA Guidelines and Policy - http://inweb/citytech/infrastructure/Distributed_Computing/pda.doc
- Policy for Computers Infected with Malicious Programs - http://inweb/citytech/infrastructure/Distributed_Computing/wormpolicy.doc
- Virtual Private Network Use Policy - http://inweb/citytech/itmanagement/ITgov_standards/VPN_5.14.htm

SECTION 4: Definitions

Acceptable Use Agreement: An agreement outlining policies, guidelines, responsibilities for Authorized Users granted remote access to the Network. The Agreement must be signed and returned to the granting department.

Ad Hoc Connectivity: Plugging an ad hoc device directly into the Network or another City owned workstation while on City premises for the purposes of accessing City applications, the Internet and/or other City data resources.

Ad Hoc Device: City or non-City owned devices that have not been connected to the Network for a designated period of time. Because they have not been connected, they are considered “untrusted”, and assumed to be non-compliant with current patching levels.

Ad Hoc User: Employees, contractors, business partners, etc., who are not Authorized Users, but have a need, on a temporary basis, to connect to the City network to conduct City business.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Cable Modem: Cable companies such as Comcast provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Computing Device: A device such as a desktop, laptop, handheld, or notebook computer, Personal Digital Assistant (PDA), or a server.

Connectivity Management: Controlled access to Network resources by allowing only computing devices that fully comply with established criteria; that is, current operating system patch levels, up-to-date virus signatures and the absence of specific worm, virus, or Trojan malware. Ad hoc devices will be denied access or will be quarantined in a holding queue. Connectivity management can be achieved through combinations of process, procedures, and hardware/software.

Contracted Vendor: A vendor who, through agreement and contract with the City, will provide technical support on City applications or software via a remote connection on the Network.

Data Storage Device: A device that may or may not have intelligence that is connected to the Network via a network port, or by insertion into a computing device port that is connected to the Network. These devices are generally used to store data.

Dial-up: A method of communicating via telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device.

Examples include but are not limited to:

1. Connecting a server to two different networks using two network interface cards (NIC).
2. Connecting a computer to a City provided DSL, ISDN, or cable modem AND concurrently connecting to a public ISP, a bulletin board, or a family member's network via modem or publicly provisioned broadband.
3. Configuring an ISDN router to dial into City and an ISP, depending on packet destination.
4. Connecting a computing device to the Network and concurrently using a modem to connect to another network (whether wired or wireless).

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 1.5 Mbps downstream (to the user) and slower speeds upstream (to the Internet).



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Frame Relay: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame relay has a flat-rate billing charge instead of a per time usage. Frame relay connects via the telephone company's network.

Holding Queue: A logical network location for ad hoc devices that contains compliance remediation services. This holding queue will be separated from the Network such that non-compliant devices cannot affect or infect other computing devices or Network resources. This queue may be a single disconnected PC, that ad hoc devices can be connected to, or a VLAN with server remediation services.

Internet: The Internet is made up of computers in more than 100 countries covering commercial, academic and government endeavors. Originally developed for the US military, the Internet has become widely used for academic and commercial research. Users have access to unpublished data and journals on a huge variety of subjects. Today, the Internet has become commercialized into a worldwide information highway, providing access to information on every subject known to humankind.

ISDN: Integrated Services Digital Network. Provides for point to point data transmission at 128K bps. ISDN users must connect to a host, which is also capable of ISDN connection using an adaptor. The reliability of ISDN is not questioned, however, it is relatively expensive and is being eclipsed by the recent growth in broadband Digital Subscriber Line (DSL) technology.

ISP: An Internet Service Provider - commonly referred to as an 'ISP', is a company which provides individuals and organizations access to the Internet, plus a range of standard services such as e-mail and the hosting (running) of personal and corporate Web sites. The larger ISPs will offer a range of access methods including telephone, leased line, ISDN or the newer DSL (ADSL) circuits and will be connected to 'backbone' high speed digital circuits which form the Internet itself. ISPs usually charge a tariff for their services although income can be derived from various sources of advertising and portal activities. Occasionally an ISP are referred to as IAP - an Internet Access provider

LAN: A home or office network operated within one location. This may comprise one or more adjacent buildings, but a local network will normally be connected by fixed wires. For purposes of this policy, a router that connects multiple computing devices at home is considered a LAN.

Remote Access: Any access to the City's network through a non-city controlled network, device, or medium.

SSL VPN: A secure socket layer (SSL) VPN tunneling method that employs SSL encryption protocol.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Split Tunnel: This term has meaning only for VPN tunnels. It is the definition of how network traffic is handled by a remote end of a VPN tunnel. If using a split tunnel, then traffic bound for the City's network uses the VPN tunnel and traffic bound for anywhere else, is not sent to the city, but rather is handled as normal by the ISP. If not using split tunnel, then when the tunnel is up, any traffic from the remote computing device is sent through the tunnel and handled by the City network. The choice of using a split tunnel or not is NOT configurable by the VPN client.

System Owners: Individuals within the City who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that are associated with the City.

System Operators: Individuals within the City who are accountable for the operational decisions about the use and management of a computing system. (See also, system owners).

Untrusted Image: A file containing an operating system, applications, services etc. that is used to custom configure a computing device specific to the needs of a particular organization. An untrusted image file is one that has not been updated to current patching and virus signature levels and is therefore untrusted and should not be used.

VPN: A Virtual Private Network (VPN) tunnel is a method for accessing a remote network via "tunneling" through the Internet.

Wired: Generally refers to the physical cabling in a network. "Over the wire" means transmitting the signal onto the physical medium. Increasingly, the wire is not longer metal, but glass. In this policy, a "wired" connection is one that is connected directly to the City's backbone network without having passed through any wireless or Internet connection.

Wireless: Radio transmission via the airwaves. Various communications techniques are used to provide wireless transmission, including infrared line of sight, cellular, microwave, Bluetooth, satellite, packet radio and spread spectrum. This policy covers the use of wireless technologies based on the IEEE 802.11x standards.

Section 5: Policy

5.1 General

- 5.1.1 Departments granting remote access will ensure that authorized users and contracted vendors be given an Acceptable Use Agreement, which outlines responsibilities and guidelines for use. They will acknowledge their agreement for acceptable use by returning a signed copy of the agreement to the granting department.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

- 5.1.2 Authorized users or contracted vendors must use only authorized methods defined in Section 2, Applicability, for access to the Network and City services.
- 5.1.3 Computing devices used for City business, regardless of ownership, should be physically secured in such a way as to prevent unauthorized access, misuse, vandalism or theft.
- 5.1.4 Systems owners, operators, and data custodians must apply the same level of responsibility and oversight, as specified in the ISSP, Section 5, for City systems and data that are accessed by remote or ad hoc connections.
- 5.1.5 System owners and/or operators must terminate remote access mechanisms within one business day of notification that an authorized user or contracted vendors' privileges have been revoked.
- 5.1.6 It is the responsibility of the City to support authorized users with the configuration and troubleshooting of hardware, software, or authentication mechanisms furnished by the City to authorized users for remote access to the Network.
- 5.1.7 The City is not responsible for the integrity, maintenance, and technical support of non-City owned computing and data storage devices personal firewalls and software, etc. that may be used for connection to the Network.
- 5.1.8 General access to the Internet for recreational use through the Network is not permitted. Authorized users or contracted vendors are responsible for ensuring that family members and others with access to the connection do not violate City of Seattle policies, perform illegal activities, or use the connection to conduct business not related to the City of Seattle.
- 5.1.9 Authorized users who access City restricted or confidential data must be authenticated through access mechanisms as outlined in Section 7.3 of the ISSP.
- 5.1.10 Authorized and ad hoc users and contracted vendors are accountable for all activities while connected to the Network and may bear the consequences should the access privilege be misused.
- 5.1.11 Departments authorizing remote and ad hoc connections will establish appropriate connectivity management processes and procedures to, at a minimum, audit and monitor for anti-virus signatures and required operating system patches.
- 5.1.12 Departments authorizing remote and ad hoc connections will scan computing devices for the existence of malicious code and programs.
- 5.1.13 Data classified as restricted or confidential must be protected in accordance with Section 7.2 Data Classification and Related Protective Measures of the ISSP.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

5.1.14 Contracted vendors performing technical support on City applications via a remote connection to the Network must sign an Acceptable Use Agreement before access will be granted or, during the contract renewal process. The Acceptable Use Agreement shall be an addendum or appendix to the vendor contract.

5.1.15 Ad hoc computing devices will not be allowed to connect to the Network unless for the purpose of scanning and patching the device in a secure holding queue on the Network.

5.2 Wired Access – Ad Hoc Connectivity

This section contains policy for ad hoc connections to the Network. This type of connection would enable a computing device to connect to the Network via network jacks provided on City premises. A typical use would be for consultants, vendors, contractors, etc., who would use the connection for access to the Internet, documents and briefing materials, etc. while conducting business with or for the City.

5.2.1 Ad hoc users who request connection to the Network must not introduce viruses, vulnerabilities, or other types of malicious code that could cause harm to the Network and/or City systems and data.

5.2.2 Ad hoc users who are connected the Network must not be connected to any other network at the same time.

5.2.3 Ad hoc users who request connection to the Network using an ad hoc device must ensure that the device contains anti-virus software that is patched at the most up-to-date levels.

5.2.4 Ad hoc users who request connection to the Network using an ad hoc device must ensure that the device operating system is patched at the most up-to-date levels.

5.3 Wireless Access

Refer to the [IT Security Policy and Guidelines](#) for applicability.

5.4 Remote Access

5.4.1 Authorized users with remote access privileges must abide by the ISSP, Section 8, User Guidelines.

5.4.2 Authorized users and contracted vendors must not share their login ID or password with anyone, at any time.

5.4.3 Dual homing is an unsafe connectivity practice and is generally allowed only on an exception basis.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

- 5.4.4 Home LAN to City LAN VPN site-to-site tunnels are not allowed.
- 5.4.5 Home LAN's must run City specified personal firewalls and anti-virus protections that are maintained at the most up-to-date patch levels if remote connection to the Network is intended.
- 5.4.6 Non-City owned networks and computing devices, used to connect remotely to the Network, must not be reconfigured for the purpose of split-tunneling or dual homing at any time.
- 5.4.7 Any computing device used to connect remotely to the Network must run City specified firewall and anti-virus software, as defined in City standards, that is maintained at the most up-to-date patch levels.
- 5.4.8 Any computing device used to connect remotely to the Network must have an operating system that is maintained at the most up-to-date patch levels.
- 5.4.9 Contracted vendors must coordinate their access to the Network with granting department technical staff.
- 5.4.10 Departments granting access to contracted vendors must ensure that access is limited to only specific computing devices.

Section 6: Guidelines

These guidelines should be reviewed carefully by authorizing Departments and applied as needed.

- 6.1 Internet peer-to-peer (P2P) connections, such as KAZAA or Napster, should not be allowed on any computing device used for remote or ad hoc connection to the Network.
- 6.2 Home wireless networks should be allowed to connect to the Network via a SSL VPN connection only.
- 6.3 Authorized users and contracted vendors should be provided with all policies and guidelines governing their use of City supplied access methods in order to understand their role and responsibilities.
- 6.4 Application software residing on computing devices used to collect restricted or confidential City data should be maintained at the most up-to-date patch levels.
- 6.5 Data classified as restricted or confidential should be password protected if stored on a computing device.
- 6.6 City data classified as restricted or confidential should not reside on ad hoc devices until its' proper use and handling have been agreed upon between system owners, data custodians, and the recipient of the data.
- 6.7 Image files used to configure computing devices should also be maintained at current patching levels and should be considered "untrusted" until tested for compliance.



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Section 7: Implementation

Compliance initiatives will commence following adoption of the policy. The largest component, a comprehensive connectivity management solution, will be phased in as funding and toolsets become available.

Compliance steps in order of priority may be:

- ◆ Informational meetings with City technical teams to introduce the policy.
- ◆ Compliance to the ISSP in areas of systems, network, data classification and user authentication.
- ◆ Rigid controls for granting/revoking user access mechanisms and privileges
- ◆ Interim processes for scanning/validation of ad hoc devices
- ◆ Development of a Acceptable Use Agreement implemented Citywide.
- ◆ Development, review, and publishing of City preferred firewalls and anti-virus products.
- ◆ Deployment of connectivity management processes and tools.
- ◆ Integration of an Acceptable Use Agreement into City contracting practices required for contracted vendors.

Section 8: Enforcement

General policy enforcement as outlined in the *IT Security Policy and Guidelines*, Section 6.8 will apply to the Remote Access and Ad Hoc Connectivity Policy as well.

Exceptions to this policy will be handled by the authorizing Department, and must be documented in writing as to the exception request and outcome



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Document Control

Owning Organization: Information Technology Security Board (ITSB)

Initially Adopted: Adopted by Technology Council, August 31, 2004

Update Cycle: To be reviewed annually for possible changes by the ITSB, or considered for change at any time if requested.

Record of versions:

Version	Description	Release Date
Ver 1	Remote Access Policy Working Group	1/23/04
Ver 2	Laurie	2/6/04
Ver 3	Remote Access Policy Working Group	2/23/04
Ver 4	Remote Access Policy working Group	3/8/04
Ver 5	Remote Access Policy working Group	3/15/04
Ver 6	Initial review by ITSB	3/18/04
V7	Revisions by SCL/policy working group	4/20/04
V8	Revisions by Policy Working Group Term "ad hoc" device added. Replace bullets with outline numbers. Replaced term "database" with "data".	5/11/04
V9	Add def for connectivity management and holding queue. Change references to non-City owned to ad hoc devices.	5/13/04
V10	Reformat on approved policy template. Re-order section 7,8. to include implementation recommendations.	8/3/2004
V11	Add policy specific to contracted vendor connectivity.	8/24/2004



City of Seattle

Remote Access and Ad Hoc Connectivity Policy

Gregory J. Nickels, Mayor
Bill Schrier, Chief Technology Officer

Authorized this ____ day of _____, 2004 by:

Bill Schrier
Chief Technology Officer
City of Seattle