


CITY OF BREMERTON		REMOTE ACCESS	
INDEX Information Management 2-20-12	EFFECTIVE DATE: February 1, 2008	 APPROVED <hr/> CARY BOZEMAN, Mayor	

1.0 Purpose

The purpose of this policy is to define standards for remotely connecting to the City of Bremerton's network from any host. These standards are designed to minimize the potential exposure to the City of Bremerton from damages which may result from unauthorized use of City of Bremerton resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical City of Bremerton internal systems, etc.

2.0 Definitions

Term	Definition
-------------	-------------------

<i>Dial-in Modem</i>	A peripheral device that connects computers to each other for sending communications via the 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.
----------------------	--

<i>Dual Homing</i>	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a City of Bremerton-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. The configuration of an ISDN router to dial into City of Bremerton and an ISP, depending on packet destination.
--------------------	---

<i>IPSec</i>	Internet Protocol Security
--------------	----------------------------

<i>Remote Access</i>	Any access to City of Bremerton's corporate network through a non-City of Bremerton controlled network, device, or medium.
----------------------	--

<i>Split-tunneling</i>	Simultaneous direct access to a non-City of Bremerton network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into City of Bremerton's network via a VPN tunnel.
------------------------	--

<i>VPN</i>	A Virtual Private Network (VPN) is a secure connection between two networks over an non-trusted network (such as the internet). VPN's are very useful when sensitive information must be transmitted or received over the Internet. The VPN
------------	---

prevents third parties from reading or modifying the information in transit. The connection is controlled and secured by the software installed at the connection end-points. This software implements authentication, key exchange, and data encryption according to the IPSec standard.

VPN Tunnel is a method for accessing a remote network via "tunneling" through the Internet.

3.0 Scope

This policy applies to all City of Bremerton employees, contractors, vendors and agents with a City of Bremerton-owned or personally-owned computer, workstation or device used to connect to the City of Bremerton network. This policy applies to remote access connections used to do work on behalf of the City of Bremerton, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

4.0 Policy

4.1 General

- Approved City of Bremerton employees and authorized third parties may be granted remote access to the City of Bremerton's corporate network
- It is the responsibility of City of Bremerton employees, contractors, vendors and agents with remote access privileges to the City of Bremerton's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to City of Bremerton network
- General access to the Internet for recreational use by immediate household members through the City of Bremerton Network on personal computers or devices is not permitted. The City of Bremerton employee bears responsibility for the consequences should access be misused.
- At no time should any user covered under this policy provide their login or email password to anyone, not even family members.

4.2 Requirements

- Authorized users with remote access privileges must ensure that their City of Bremerton-owned or personal computer, workstation or device is not connected to any other network at the same time, with the exception of personal/corporate networks that are under the complete control of the user.
- Authorized users with remote access privileges must ensure that any wireless technology on the user's home/corporate network used to establish a remote connection to the City of Bremerton's network conforms to the standards contained in the City of Bremerton's Wireless Security Policy.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

- Authorized users with remote access privileges to City of Bremerton's network must not use non-City of Bremerton email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct City of Bremerton business.
- All hosts that are connected to City of Bremerton internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers
- Personal equipment that is used to connect to City of Bremerton's networks must meet the requirements contained in the City of Bremerton's Minimum Baseline Configuration rules that can be confirmed by Information Technology.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the City of Bremerton production network must obtain prior approval from Information Technology.

4.2 Connection Methods

Authorized users with remote access privileges may not use any remote access methods not specifically described herein:

4.2.1 Dial-in

- City of Bremerton employees and authorized third parties (customers, vendors, etc.) can use dial-in modem connections to gain access to the City network. Dial-in access is strictly controlled, using one-time password authentication. Coordinate account activations and passwords via the Information Technology Help Desk.
- It is the responsibility of users with dial-in access privileges to ensure a dial-in connection to the City of Bremerton is not used by non-authorized users to gain access to City information systems resources. A user who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the City of Bremerton are literal extensions of the City of Bremerton's network, and that they provide a potential path to the City's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect the City of Bremerton's assets.
- Only GSM standard digital cellular phones are considered secure enough for connection to the City of Bremerton's network. Analog and non-GSM digital cellular phones cannot be used to connect to the City of Bremerton's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals
- Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of three months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4.2.2 VPN

- City of Bremerton employees and authorized third parties (customers, vendors, etc.) can use SSL VPNs to access the City of Bremerton network. This policy applies to implementations of SSL VPN's that are directed through the City of Bremerton's SSL VPN Concentrator.
- Authorized users may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.
- By using VPN technology with personally owned equipment, users must understand that their machines are a de facto extension of City of Bremerton's network, and as such are subject to the same rules and regulations that apply to City of Bremerton-owned equipment, i.e., their machines must be configured to comply with Information Technology security rules.
- When actively connected to the network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- VPN gateways will be set up and managed by City of Bremerton Information Technology
- VPN users will be automatically disconnected from City of Bremerton's network after thirty minutes of inactivity. The user must then log-in again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Only Information Services approved VPN clients may be used.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.