


| | | | |
|--|---|---|--|
| CITY OF BREMERTON | | ACCEPTABLE COMPUTER USE | |
| INDEX Information Management 2-20-10 | EFFECTIVE DATE: February 1, 2008 |  APPROVED <hr/> CARY BOZEMAN, Mayor | |

1.0 Objective

The City of Bremerton is responsible for securing its computer systems in a reasonable and economically feasible manner against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them.

The users of the City’s computer systems are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of the City’s computer systems may result in litigation against the offender by the proper authorities. If such an event should occur, the City will fully comply with the authorities to provide any information necessary for the litigation process.

Department Managers will ensure the physical security of Business Systems assigned to their department and where applicable of the information contained within these systems. While providing reasonable protection for these systems, the Manager will ensure that no unnecessary restrictions are placed on access to public information as defined in the Public Disclosure Act (RCW 42.17).

The computer systems of the City are provided for the business use by the staff of the City of Bremerton. All staff is responsible for seeing that these computer systems are used in an effective, efficient, ethical and lawful manner. Incidental personal use of computer systems during meal time or other breaks or outside of work hours is allowed provided that all other computer systems usage policies are adhered to, the use does not interfere with City operations and is at no cost to the City.

1.1 Computer Systems Defined

For purposes of this policy, computer systems include, but shall not be limited to, computers, computer software, Internet accounts, printers, network hardware, network software and electronic mail.

2.0 Purpose

The City of Bremerton's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the City's established culture of openness, trust and integrity. The City is committed to protecting their employees from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of the City of Bremerton. These systems are to be used for business purposes in serving the interests of the City, their clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every City of Bremerton employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Bremerton. These rules are in place to protect the employee and the City of Bremerton. Inappropriate use exposes the City of Bremerton to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the City of Bremerton, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of Bremerton.

4.0 Policy

4.1 General Use and Ownership

1. While the City of Bremerton desires to provide a reasonable level of privacy, users should be aware that the data they create on the City systems remains the property of the City of Bremerton and the confidentiality of information stored on any networked device belonging to the City of Bremerton cannot be guaranteed.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. The City of Bremerton recommends that any information that users consider sensitive or vulnerable be encrypted. Information Technology can provide assistance with encryption.

4. For security and network maintenance purposes, authorized individuals within the City of Bremerton may monitor equipment, systems and network traffic at any time.
5. City of Bremerton reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords shall be changed on a schedule determined by Information Technology.
2. All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the unit will be unattended.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised. Sensitive/restricted information should not be stored on the hard drive of a portable device when that device is removed from City premises.
4. Postings by employees from a City of Bremerton email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City of Bremerton, unless posting is in the course of business duties.
5. All computers/electronic devices used by employees that are connected to the City of Bremerton network, whether owned by the employee or the City of Bremerton, shall conform to the standards set by Information Technology.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City of Bremerton authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing a City of Bremerton-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Bremerton.
2. Placing or causing the installation of any personal copies of software or data on any City equipment.
3. Placing or causing the installation of any software that has not been properly purchased, licensed or otherwise legally obtained by the City of Bremerton. Such activities will not be considered "good faith performance of duties". The City will not defend employees in legal actions relating to such software and will not indemnify employees for the consequences of any legal actions. Further, the City will take steps to recover from the individuals concerned any damages suffered by the City in respect of such legal actions.
4. Placing or causing the installation of any City owned software on non-city owned equipment (i.e. Home computers) for personal or City use except upon expressed approval of the Department Head and the Information Services Manager. *Note: Where approval for this action is granted, be aware that any City business information created, retrieved or stored on the non-city equipment is subject to public disclosure requests as if it were a city owned piece of equipment.*
5. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City of Bremerton or the end user does not have an active license is strictly prohibited.
6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
9. Using a City of Bremerton computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment policies or contributes to a hostile workplace.

10. Making fraudulent offers of products, items, or services originating from any City of Bremerton account.
11. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
13. Port scanning or security scanning is expressly prohibited unless prior notification to Information Services is made.
14. Attaching any computing/peripheral device not approved or authorized by Information Services. This include personal computers, laptops or network enable communications devices.
15. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
16. Circumventing user authentication or security of any host, network or account.
17. Circumventing or bypassing configurations intended to direct Internet access away from monitoring and/or proxy services.
18. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
19. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
20. Providing information about, or lists of, City of Bremerton current or retired employees to parties outside City of Bremerton, unless doing so is a requirement of the job (e.g. response to public disclosure requests.)

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

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

6.0 Employee Signature

All employees will be required to sign the "Computer User Agreement" before access to the computer systems will be made available. Refusal to sign the form will result in the employee not receiving computer system access.

7.0 Definitions

Term Definition

Spam Unauthorized and/or unsolicited electronic mass mailings.