

**Please read through this policy.**

## **TECHNOLOGY RESOURCE USAGE POLICY AND WORK RULES**

### **Summary**

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Bellevue. The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points to remember are:

1. The City provides computing and network resources ('technology') to carry out legitimate City business.
2. There is no right to privacy in the use of City technology resources.
3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, City Council, City Manager or media should be avoided.
4. Users granted access to critical data are responsible for its protection.
5. Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule.
6. Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

## Scope

The following policies define appropriate use of the City of Bellevue network, computers, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City of Bellevue authorizes the use of computing and network resources by City staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business such as sale of cosmetics or consulting.

## Ownership of Data

The City owns all data stored on its network and systems (including e-mail, voicemail and Internet usage logs) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose and with or without notice to the employee. The City may conduct random and requested audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the City. Internet and e-mail communications may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage is subject to monitoring at any time with or without notice to the employee. There is no right to privacy in the use of City technology resources.

## Personal Use

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the city to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City technology resources. This document provides policies and general rules for appropriate use of resources. Staff use of technology resources in violation of this policy or otherwise inappropriate technology resource usage is subject to disciplinary actions up to and including termination as provided in 5.4 below.

(Technology definitions provided in section 6)

## **1 Internet/Intranet Usage**

- 1.1 This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet.

- 1.2 Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be actively used by the City to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.). Attempts to alter or bypass filtering mechanisms are prohibited.
- 1.3 Except for City business related purposes, visiting or otherwise accessing the following sites is prohibited:
  - a. "adult" or sexually-oriented web sites,
  - b. sites associated with hate crimes, or violence
  - c. sites that would create discomfort in a reasonable person in the workplace
  - d. Internet chat rooms, blogs and interactive website communication
  - e. personal dating sites
  - f. gambling
- 1.4 . Activities on Internet chat rooms, blogs and interactive website communication sites are electronically associated with City network addresses and accounts that can be easily traced back to the City of Bellevue. Comments made during the course of business use shall be reflective of City policy.
- 1.5 Staff violating this policy or otherwise engaging in inappropriate use of the Internet is subject to disciplinary actions up to and including termination from employment.

## 2 E-Mail Usage

- 2.1 E-mail content must comport with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.
- 2.2 Users must manage their e-mail in accordance with record retention policies and procedures as defined and identified by the City Clerk's office.
- 2.3 E-mail accounts must be managed within assigned capacities. Messages must be stored to alternative locations (like your F drive or back-up disk) on a regular basis and deleted from the e-mail system. Retention of personal email should be minimized, and no restores or IT resources will be engaged to recover personal email "lost" in City systems.
- 2.4 Use of the "Everyone\_COB" distribution list is restricted to the City Manager's Office, Department Directors and their specific designees. Under no circumstances should an employee "Reply to All" to an Everyone\_COB message.
- 2.5 The City provides staff access to and support of the Exchange/Outlook messaging (e-mail) system. Access or usage of any other messaging systems is not allowed unless it is web based. Subject to the personal use limitations explained above, staff may access web-based personal email but *should not download personal documents or attachments from these sites*. Staff may not install client based software for internet service on city equipment. Examples: AOL, Instant Messaging

- 2.6 Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact the support desk.
- 2.7 The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having not legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.
- 2.8 The incidental personal use of e-mail from a City account to express opinions or views other than those reflective of City policy must contain the following disclaimer: "The contents of this electronic mail message do not necessarily reflect the official views of the elected officials or citizens of the City of Bellevue."
- 2.9 Staff e-mail usage in violation of this policy or otherwise inappropriate e-mail usage is subject to disciplinary actions up to and including termination.

### 3 Security

- 3.1 ITD must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a password that meets City requirements. <http://cobnet/it/Security/SecurityPWInfo.htm> The use of another person's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended - <http://cobnet/it/Training/Troubleshoot/Computer/TrainingWhatsTheDifference.htm>. If you discover unauthorized use of your account, immediately follow the reporting procedures in section 5.1.
- 3.2 The City of Bellevue will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the City financially; put staff at risk; put facilities at risk; or could cause legal liability. Examples of critical data include: employee health information, social security numbers, credit card holder information, banking information, and police crime investigation information.
- 3.3 Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: encrypting data any time it is electronically transported outside the City network; ensuring that inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.
- 3.4 The City will restrict access to critical information only to staff who have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.

- 3.5 Staff will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.
- 3.6 Staff shall not share their password with any other person.

#### **4 Network Access and Usage**

The Information Technology Department (ITD) must approve connecting devices to the City's network. This includes PCs, network hubs and switches, printers, handhelds, scanners, remote connections, and wireless or wired devices.

- 4.1 Personal software or devices may not be loaded or attached to any City-owned equipment without written authorization by a designated department manager and by ITD. The use of personal routers and wireless access points on the city network is not allowed.
- 4.2 Exploiting or attempting to exploit into any vulnerability in any application or network security is prohibited. Sharing of internal information to others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, denial of service attack, or virus onto the City network or computers. If you encounter or observe vulnerability in any application or network security, report it to [support@bellevuewa.gov](mailto:support@bellevuewa.gov) immediately.
- 4.3 Obey the privacy and rules governing the use of any information accessible through the network, even if that information is not securely protected.
- 4.4 Non-COB staff (e.g. vendors, contractors) are required to have their PC scanned by ITD for virus detection prior to connecting to the COB network. Representatives of the contracting departments are responsible for assisting their contractors to engage ITD to perform these services by contacting support at [support@bellevuewa.gov](mailto:support@bellevuewa.gov) or calling x2886.
- 4.5 Disabling, altering, over-riding, turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden.
- 4.6 Because of band-width limitations inherent in any network system, use of the City network to download non-business related information is prohibited. Examples include streaming video of baseball games, streaming audio of radio programs, MP3 files, and on-line games.
- 4.7 Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Bellevue.
- 4.8 Users must manage their electronic documents in accordance with record retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files.
- 4.9 Access to the City's network via VPN requires approval from ITD. VPN accounts will be audited on a monthly basis, and accounts inactive for 30 days will be deactivated unless an exception is granted by ITD. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request.

- 4.10 Remote access to the City's applications via Citrix requires approval from the departmental ITGC representative and the application owner.
- 4.11 Periodically business owners will need to review and approve user accounts for their systems. A list will be provided by Information Technology for enterprise systems. This review should be completed on a predetermined schedule.
- 4.12 Staff network usage and access in violation of this policy or otherwise inappropriate network usage and is subject to disciplinary actions up to and including termination.

## **5 Administration, Reporting and Violations/Discipline**

- 5.1 Each Department will designate specific employees who have the authority to authorize ITD to provide accounts and access to technology resources. Suspected violations or concerns should be reported to the IT Help Desk.
- 5.2 ITD, the Departments and HR share responsibilities in enforcing these policies specifically:

### **5.2.1 ITD Responsibilities**

- ITD is responsible for recommending technology usage policy guidelines that are enforceable.
- ITD is responsible for enterprise monitoring of technology resources using security and monitoring tools. Security and monitoring information will be provided to HR as requested to support the investigation of technology usage policy infractions.
- If, in the normal course of business activities, ITD discovers violations of the Technology Usage Policy, ITD will report the activities to the staff member's supervisor, Director of HR and/or to the city Manager depending upon the severity of the infraction.

### **5.2.2 Departments Responsibilities**

- Departments assist in the development and adoption of the technology usage policy through ITGC.
- If, in the course of normal business activities, department management suspects a staff member is violating the technology usage policy they will report the suspected infractions to Human Resources.
- Departments are responsible for carrying out any disciplinary actions in response to Technology Usage Policy violations.

### **5.2.3 Human Resources Responsibilities**

- Human Resources assists in the development and adoption of the technology usage policy through ITGC.
- Human Resources is responsible for integrating the Technology Usage Policy into new hire training, orientation and ongoing training of City work rules and policies.

- Human Resources is responsible for the evaluation of reported technology usage policy infractions, and may request additional monitoring information (e.g., security logs) from ITD as part of their investigation and evaluation process.
  - Human resources is responsible for providing necessary information to Department heads to facilitate the consistent application of disciplinary action when technology usage policy infractions occur.
  - Human Resources is responsible for coordinating disciplinary actions with department staff when technology usage policy infractions occur.
- 5.3 As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from ITD.
- 5.4 Violations of the Technology Resource Usage Policy and Work Rules or otherwise inappropriate use of technology resources are subject to disciplinary action up to and including termination. Actions that demonstrate a clear disregard for these policies and requirements and that could have or have resulted in damage or serious disruption to the City's network, systems, services, or data or could have or have resulted in damage to the City's credibility or reputation with the public may result in immediate discharge.

## **6 Definitions: (Courtesy of WebOpida.com)**

- 6.1 Blog - Short for Web log, a Blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author. Blogging is when one posts to a Blog.
- 6.2 DOS Attack– Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DOS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DOS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DOS attacks are constantly being dreamed up by hackers.
- 6.3 Electronic Communications - The transmission of data from one computer to another, or from one device to another. A communications device, therefore, is any machine that assists data transmission. For example, modems, cables, and ports are all communications devices. Communications software refers to programs that make it possible to transmit data.
- 6.4 Modems – A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms. Modems can be wired or wireless.
- 6.5 Peripherals – A computer device, such as a CD-ROM drive or printer, that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external -- such as a mouse, keyboard, printer, monitor, external Zip drive or scanner -- or internal, such as a CD-ROM drive, CD-R drive or internal modem. Internal peripheral devices are often referred to as integrated peripherals.

- 6.6 Personal Devices - PDA (Personal Digital Assistant), smart phone. A handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. Unlike portable computers, most PDAs began as pen-based, using a stylus rather than a keyboard for input. This means that they also incorporated handwriting recognition features. Some PDAs can also react to voice input by using voice recognition technologies. PDAs of today are available in either a stylus or keyboard version.
- 6.7 Phishing - The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.
- 6.8 Software - Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware. The terms software and hardware are used as both nouns and adjectives. For example, you can say: "The problem lies in the software," meaning that there is a problem with the program or data, not with the computer itself. You can also say: "It's a software problem."

The distinction between software and hardware is sometimes confusing because they are so integrally linked. Clearly, when you purchase a program, you are buying software. But to buy the software, you need to buy the disk (hardware) on which the software is recorded.

Software is often divided into two categories:

*systems software* : Includes the operating system and all the utilities that enable the computer to function.

*applications software* : Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

- 6.9 Spyware - Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with Spyware. Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of Spyware is to download certain peer-to-peer file swapping products that are available today.

- 6.10 VPN – Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create

networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. VPN is used by outside computers to connect to the City of Bellevue network.