

RESOLUTION 2014 - B



**A RESOLUTION OF THE CITY COUNCIL OF THE  
CITY OF SUNNYSIDE, WASHINGTON, APPROVING  
A COMPUTER AND INFORMATION TECHNOLOGY POLICY**

**WHEREAS**, the City of Sunnyside, as part of its business practice, provides computers and associated internet connectivity for its employees; and

**WHEREAS**, the City of Sunnyside is aware of the risk cyber-attacks, viruses, and malware associated with IT systems; and

**WHEREAS**, the City of Sunnyside is determined to take every reasonable action to protect its resources and assets from such risk; and

**WHEREAS**, the City Council finds and determines that a comprehensive policy on the use of Information Technology and computer use is in the best interest of the city.

**NOW, THEREFORE, IT IS HEREBY RESOLVED BY THE CITY COUNCIL OF THE CITY OF SUNNYSIDE, WASHINGTON**, as follows:

**SECTION 1.** That the City Sunnyside Computer and Information Technology Policy, a copy of which is attached hereto as Exhibit "A" and incorporated herein by this reference, is hereby approved; and the City Manager is hereby authorized to execute and administer such policy for and on behalf of the City of Sunnyside.

**SECTION 2.** This Resolution shall be effective upon passage, approval and signatures hereon in accordance with law.

**PASSED** this 27<sup>th</sup> day of October, 2014.

  
\_\_\_\_\_  
JAMES A. RESTUCCI, MAYOR

**ATTEST:**

  
\_\_\_\_\_  
DELILAH SAENZ, CMC, CITY CLERK

**APPROVED AS TO FORM:**

A handwritten signature in black ink, appearing to be "Kerr", written over a horizontal line.

KERR LAW GROUP, PLLC  
Attorneys for the City of Sunnyside



## **COMPUTER AND INFORMATION TECHNOLOGY POLICIES**

It is the policy of the City of Sunnyside to maximize the cost-effective use of computer systems as a means of improving productivity for employees. The City provides communication resources for electronic mail (email), internet access, telephone and voicemail, facsimile machines, cellular telephones, and other electronic communication devices (collectively referred to as the City's Technology Resources) to employees to assist in and facilitate City business and communications.

This policy does not address all required, allowed, or prohibited behaviors by employees, but merely covers common examples. In general, the City relies on the good judgment of its employees to ensure that City Technology Resources are used in the public's best interest.

### No Expectation of Privacy:

By using the City's Technology Resources users understands that they have no expectation of privacy or confidentiality in their use of these systems or in any data that they create, store, or transmit over the systems, including any data created, stored or transmitted during an employee's incidental personal use of the Technology Resources as permitted under this policy. Also, understand that any data, they create, store or transmit from/to or within city systems to include electronic and physical is the sole property of the City and not individuals. Users further understand that they are aware of, understand and will comply with the provisions of this policy, and that their use of the Technology Resources can and will be monitored and any data that they create, store or transmit on or over City systems may be inspected by City management at any time. Employees should understand that certain email messages, other electronic communications, and documents created on City computer systems may be considered a public record subject to disclosure and/or subject to discovery in the event of litigation.

### Standardized Software and Hardware

The City has established software and hardware standards for commonly used applications. The use of unauthorized, non-standard software or hardware, including personally owned software or hardware, on city computer systems without written approval by IT staff and authorized by the City Manager, is prohibited.

### Installation of Software and Hardware

All software and hardware is to be installed by the IT Division. Specialized software and hardware technologies exclusive to individual departments may be managed within the appropriate department, in coordination with and approval of the IT Division. Any moving, relocating, or rearranging of computer software or hardware will also be coordinated and scheduled with the IT Division using the current defined process or

appropriate form.

#### Ownership and Confidentiality

All software, programs, applications, data, data files and web pages residing on City systems or storage media, developed on City computer systems are property of the City. The City retains the right to access, copy, modify, destroy or delete this property. Data files containing confidential or sensitive data should be treated accordingly and should not be removed from the workplace without proper authorization. This includes, but is not limited to:

- Certain employee records including those relating to or containing financial, medical or personal information;
- Legal documents including but not limited to those relating to property transactions, litigation or claims against the City;
- Banking and financial information including but not limited to transactions, credit cards, customer passwords, etc.

#### Incidental, De Minimus Personal Use

Incidental, de minimus personal use may be permitted where, in the judgment of the employee's supervisor or department director, such use does not interfere with employee or department productivity, nor distract or take time away from the worker or co-workers assigned work. Generally speaking, incidental, de minimus personal use means:

- It is done on an employee's personal time, such as on a lunch break;
- It does not interfere with job responsibilities;
- It does not result in any expense to the City;
- It does not solicit for or promote commercial ventures;
- It does not utilize excessive network resources;
- It does not constitute any prohibited use, as discussed below.

#### Prohibited Use of City's Technology Resources

Use of the City's Technology Resources to engage in any communication that violates federal, state, or local laws or regulations, or any City policy, is strictly prohibited at all times. In addition, the following uses of the City's Technology Resources are inappropriate and are prohibited at all times, unless specifically exempted below:

- Personal commercial use (benefitting an employee's outside employment or commercial business);
- Accessing, receiving or sending pornographic, sexually explicit or indecent materials of an unreasonably offensive nature;

- Usage for any type of unlawful harassment or discrimination, including the transmission of obscene or harassing messages to any individual or group because of their sex, race, religion, sexual orientation, national origin, age, disability or other protected status;
- Gambling;
- The loading of computer games;
- Usage that precludes or hampers City network performance such as streaming video or audio and playing MP3 files or online games, unless for City business.
- Unauthorized copying or downloading of copyrighted material;
- Usage that violates software license agreements;
- Downloading of software programs (unless specifically approved by applicable Department Director and coordinated with the IT Division);
- Usage for political purposes, including partisan campaigning;
- Sending anonymous messages and/or misrepresenting an employee's name, position, or job description;
- Deliberately propagating any virus, worm, malware, spyware, or other code or file designed to disrupt, disable, impair, or otherwise harm either the City's networks or systems, or those of any other individual or entity;
- Releasing misleading, distorted, untrue or confidential materials regarding City business, views or actions;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Use of Technology Resources in an excessive manner so as to deprive others of system use or resources, including the sending of bulk email for other than official business or forwarding "chain letter" emails of any kind;
- Connecting to the City network, or any specific software package, utilizing somebody else's security identification login information to gain alternate security permissions.

The preceding list does not address all prohibited uses, but merely covers common examples. Any employee who violates these policies could be subject to disciplinary action, up to and including termination. In addition, employees may be held personally liable for damages incurred as a result of copyright and licensing requirements. If in doubt, ask.

#### Downloading Files from the Internet or Opening Email Attachments

Downloading files from the internet or opening email attachments from sources outside the City can lead to spyware and/or virus attacks that can severely damage or degrade the City's network and/or data. The IT Division maintains anti-virus and anti-spyware software on City computers and with continuously updated signature definition files. However, that does not guarantee that all spyware is blocked, or that all viruses are caught. If you are downloading a file and receive a message that a virus or spyware has been detected, you must contact the IT Division immediately for assistance. Similarly if you receive an email with a suspicious attachment, or from

an unusual source, you should notify the IT Division before opening it. If you notice that your computer is behaving strangely or you suspect spyware or a virus, notify the IT Division.

Social Media and Social Networking:

The City does not authorize the use of social media and social networking websites, except in very limited and specifically authorized applications. I.e. as defined as City business. At no time are personal social media and social networking websites use authorized in any form or transmission during work hours.

Security

The IT Division must authorize all access to central computer systems via notification from Human Resources. Each user is responsible for establishing and maintaining a password that meets City requirements as prescribed by current SANS guidelines. Passwords must:

- Be changed every 120 days,
- Have a minimum length of 8 characters,
- Be complex. Passwords should use three of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special characters such as: !@#\$%^&\*(){}[]

Passwords should not be easy to guess, or use items on your desk, nor not contain your:

- Name,
- Username,
- Nickname,
- Family member names
- Pets names

Or other similar type of easily accessible items or names that can be cross referenced by outside individuals using social media and the data contained.

- Social Security Number,
- Birthday,
- License plate number,
- Address,
- Phone number.

All city computers which stand idle for more than 10 minutes will automatically "log off" or shift to "standby" mode. This will require the user to log back in through use of their personal password prior to regaining access to any program. This function is set up and controlled by IT personnel and shall not be overridden, except as authorized, in writing by the City Manager.

**Passwords should not be shared with** anyone either verbally or via email (except IT) or documented in a manner that is easily accessed by others or sent through email.

*The use of another person's passwords or attempt to capture other users' passwords is prohibited. In the event another employee's password is deemed necessary, as determined by the department director, a request shall be made to IT in writing to document the reason and IT staff will determine the appropriate method to assist the requesting party, in order to maintain proper security.*

#### Network Access and Usage

The IT Division 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.

Non-employees (e.g. vendors, contractors) are prohibited from connecting to the City's network without prior approval by IT Division and are required to have their PCs, laptops, etc. scanned by IT for virus detection prior to connecting. Additionally, any vendor/contractor will also have industry software supported software and operating system which is not end-of-life and maintained regularly with security updates. Failure to do so will result in non-connectivity of both physical and remote access until resolved. Representatives of the contracting departments are responsible for assisting their contractors to engage IT to perform these services.

#### Removable Computer Media

Personal removable computer media, i.e. USB hard drives, flash/thumb drives, CDs/DVDs, laptops, cell phones and similar devices may not be loaded or attached to any City-owned equipment without authorization by IT.

#### Electronic Document Management

Users must manage their electronic documents in accordance with record retention policies and procedures as defined and identified by RCW 40.14 - Retention Periods. <http://apps.leg.wa.gov/RCW/dispo.aspx?cite=40.14> Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files. Examples of electronic documents include, but are not limited to:

- files
- email
- web pages

#### Remote Access

Employees may access the City's hosted email system at- <http://mail.sunnyside-wa.gov>. There are a limited number of laptops projectors available for employees to check out

for business-related travel or projects. These must be returned to IT immediately upon returning, and before being connected to the City's network.

Access to the City's network for vendors and contractors via VPN (virtual private network) requires written approval from the Department Head and IT. VPN accounts will be audited, and inactive accounts will be deactivated. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request and approval by IT Division.

Remote Virtual Desktop access requires permissions to use, with certain restrictions, and work hours for remote work etc. Contact IT staff for more information.

#### City Phone System

Consistent with these guidelines, employees are not permitted to make excessive or extended personal telephone calls on City telephones.

#### City-Provided Cellular Telephones

Based on the particular duties of an employee's position, the City may determine that it is in the City's interest that an employee has a cellular telephone and/or stipend

#### Purchasing of Information Technology Hardware and Software

Purchases of technology for City use must be coordinated through the IT Division. This policy applies to all computing and network-related resources of the City of Sunnyside, whether located in the City or in remote locations or facilities. The City's technical resources include but are not necessarily limited to:

- Desktops, laptops, tablets and servers, Network Printers, scanners, and copiers.
- Software running on these devices;
- Peripheral equipment (e.g. printers, scanners, cameras, etc.);
- Cabling or connectivity-related devices;
- Audio-visual equipment such as projectors.

#### Non-Standard Office Productivity Software

Non-standard software will not be supported by the IT Division. Requests for nonstandard software must be approved by the department head and the IT Division. Before purchasing non-standard software, the purchaser must describe the source of support for the software being purchased prior to installation/activation, IT Staff will be provided sufficient time for testing and configuration management processes

If for any reason the non-standard software interferes with any regular production software configurations, operations or networking resources such as copiers, scanners or other software, this software will be deemed detrimental to City IT Resources and will be removed. The department affected can if desired, have this software loaded on a

standalone system with no outside connections or communications. At no time will IT resources be committed to correcting non-standard software which has been deemed detrimental, to properly perform and interface cleanly with any city resources that have or have not been previously affected.

#### Standard Office Productivity Software

Standards for office productivity software are defined for the City and re-evaluated periodically. Office productivity software includes such packages as

- Microsoft Office Suite, i.e. Word, Excel, Access, Outlook
- SunGard
- Adobe Acrobat Reader
- Adobe Flash Player
- Adobe Shockwave
- Java

#### Application Software:

Application software is software that fulfills a specific business purpose. Examples of application software are Adobe Professional, ArcGIS, Spillman, NetMotion, PastPerfect, WorkFlows, BlueZone, Envisionware, Overdrive, WonderWare, AutoCAD, Photoshop, InDesign, Illustrator, etc.

All application software packages must be evaluated and approved by the IT Division before purchase. Before an application software package is purchased, agreement must be reached between the vendor, purchaser and the IT Division in regard to the operating environment of and support for the application.

If application software is to be supported by the IT Division the package must fit within the City's standard operating environment. Application software will be evaluated based on:

- The nature of the application;
- It's usage base;
- The support requirements associated with the package;
- It's criticality to the mission of the department or the City of Sunnyside as a whole;
- It's fit within the City environment, i.e. operating hardware requirements, database management system, operating system requirements, and Web environment requirements.

#### Non-Standard Hardware

Non-standard hardware will not be supported by the IT Division. If a hardware component is not listed as a current standard below, it is considered to be nonstandard. Requests for non-standard hardware must be approved by the department head and IT Division. Before purchasing non-standard hardware, the purchaser must describe the source of support for the hardware being purchased.

Hardware Standards

Standards have been defined for workstation hardware, peripherals and servers. These standards are re-evaluated periodically based on common needs, vendor offerings, cost, reliability, supportability, and quality and timeliness of vendor support.

I, \_\_\_\_\_, hereby acknowledge receipt of the City of Sunnyside Computer and IT Information Technology Policies.

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

Print Name: \_\_\_\_\_