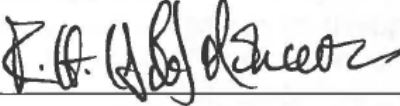
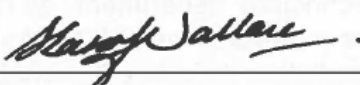


**Acceptable Use of City of Burnaby's Computing  
Technology and Network Resources  
Statement of Policy and Procedure**

Department:	City Manager's Office	Division:	Information Technology
Policy area:	User Responsibilities		
Policy No.:	IT 13.0		
Subject:	Acceptable Use of City of Burnaby's Computing Technology and Network Resources		
Issued to:	All City Staff		
Issued date:	2015 September 30	Effective date:	2015 October 23
Approved by:			
	City Manager – Bob Moncur	Chief Information Officer – Shari Wallace	

## 1 PURPOSE

The Information Technology department, on behalf of the City of Burnaby, supplies staff with a range of technology (e.g., business software applications and desktop and mobile devices) to support the delivery of services to other City departments and to citizens and customers of the City. The purpose of this policy is to ensure that all staff are informed of the expectations regarding the professional use of City supplied technology and to:

- (a) Protect the City's name, reputation and image
- (b) Prevent unauthorized or inadvertent disclosure of sensitive information
- (c) Safeguard the City's information technology assets

## 2 SCOPE

This policy applies to all authorized users of City of Burnaby owned computing devices and software applications that connect to the City's secure network and information systems, and also covers appropriate use of City resources for storing, accessing and transmitting sensitive or private data.

Personal use of City devices to access the Internet during lunch and rest breaks, or outside of normal business hours is permitted as long as usage is kept to a minimum and draws minimal network bandwidth. Usage may be monitored by a supervisor.

## 3 POLICY

- 3.01 All users must restrict their use of City of Burnaby (City) applications, systems, network and equipment to those activities broadly defined as appropriate for City business. Exceptions are made for limited personal use of the Internet as

outlined in Section 2 of this policy.

- 3.02 All data entered and maintained on City systems by employees in the course of performing their job is owned by the City.
- 3.03 The IT Infrastructure division monitors network and system usage on a regular basis as part of their role in managing the City's systems and network. Any incidental discovery of inappropriate use of the City's network or systems in the course of this work will be brought to the attention of the employee's supervisor and the Human Resources department.
- 3.04 Employees are not to download or install software on City owned computer equipment that has not been acquired or authorized by the Information Technology department. All requests to purchase or install software (including free software) are to be forwarded to the IT Helpdesk for evaluation and installation ([helpdesk@burnaby.ca](mailto:helpdesk@burnaby.ca) or 604-294-7939).
- 3.05 Users must report computer or network incidents to the IT Helpdesk promptly and not attempt to remedy the problem themselves without the knowledge or guidance of IT Helpdesk (e.g., by troubleshooting, installing, un-installing or re-configuring software, or disassembling hardware). IT Helpdesk will ensure that the incident is recorded, and correlated to any other similar incidents ([helpdesk@burnaby.ca](mailto:helpdesk@burnaby.ca) or 604-294-7939).
- 3.06 Suspected security computer incidents involving private, confidential or sensitive data must be reported immediately to the IT Helpdesk according to the affected department's internal procedures. IT will invoke the IT Security Incident Response Plan (SIRP) to begin an investigation.
- 3.07 If any City owned portable computer (laptop, tablet, etc.), mobile device, or personal storage device (PSD) is lost or stolen, it must be reported immediately to IT Helpdesk (copying Risk Management) who will disable the device as appropriate.
- 3.08 Users having a justifiable business reason for transporting a portable computing device or removable media such as PSDs with City data offsite must be authorized by a supervisor. This excludes staff who are issued City computing devices for use off City premises as part of their regular job duties (e.g., sanitation workers, licence and permit inspectors, etc.)
- 3.09 All removable media that may connect to City equipment or networks must be purchased by the City.
- 3.10 Users who require remote access to the City network and business applications must have management approval. A System Access Form must be submitted to IT Helpdesk. New employees will not be granted remote access capability by default.

Users must follow the security guidance supplied by IT Infrastructure regarding the configuration of their remote connection software and all applicable security procedures specific to the information asset they are authorized to access.

Policies and procedures apply regardless of technology used to access the City's secure network and systems.

- 3.11 Users may access data to which they are authorized, but must do so using City-authorized applications, programs, interfaces and regular business procedures.
- 3.12 The City's secure wireless network shall be used by employees, contractors, and consultants for City-related communications only.

Users wanting to connect wirelessly to the City's network resources using their personal computers, laptops, tablets or mobile phones may connect to *Burnaby Public-Wifi*.

City-supplied mobile computing devices are configured to connect to the City's secure WiFi network –*Staff*. Staff should always connect to *Staff Wi-Fi* when conducting City business.

- 3.13 For employees, failure to comply with Information Technology acceptable use policies or other associated policies, standards, guidelines and procedures may result in remedial action appropriate to the situation and may range from warning to dismissal.

For contractors or consultants, failure to comply with Information Technology acceptable use policies or other associated policies, standards, guidelines, and procedures may result in remedial action appropriate to the situation and may range from warning to termination of contracts.

## **4 RESPONSIBILITY**

- 4.01 All users who have access to the City's systems, data and secure networks are responsible for understanding and adhering to this acceptable use policy for computing technology and network resources.
- 4.02 Users of equipment configured for wireless connectivity are responsible for following IT Infrastructure's guidelines and direction to minimize security risks when their wireless devices are enabled for network connectivity.
- 4.03 IT Infrastructure is responsible for providing security and usage guidelines appropriate to the risk associated with the type of technology used to access the network and the City's data assets.
- 4.04 For employees whose jobs require them to access the City's secure network remotely, line managers are responsible for evaluating employees' offsite computing needs (whether with a City-provided computing device or with a personally-owned computer) and providing written authorization through the System Access Form (available on the connectBurnaby portal→Forms and Policies→Information Technology Forms→System Access Form).

- 4.05 The Chief Information Officer and the Director, Human Resources are responsible for interpreting this policy, as necessary, and for recommending revisions.

## 5 DEFINITIONS

- 5.01 **“Encryption”** - a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to de-crypt the information.
- 5.02 **“Information Assets”** - refers to any data or business information which has value to the business operations of the City, and/or has intrinsic value for its citizens, customers, employees, and vendors or suppliers.
- 5.03 **“Personal Storage Devices (PSDs)”** - compact devices with internal storage that can be attached to any computer such as memory sticks, removable hard drives, laptops, tablet PCs, CDs/DVDs, and smartphones and mobile music storage devices.
- 5.04 **“Sensitive Information”** - refers to information that is confidential such as personally identifiable information and credit card data, or of high value such as information pertaining to security of critical infrastructures. The disclosure of sensitive information may be a violation of the British Columbia *Freedom of Information and Protection of Privacy Act (“FIPPA”)*, interrupt the City’s ability to deliver services, lead to financial losses related to correcting the situation, legal actions, and erosion of public trust in the City.
- 5.05 **“Transport Layer Security”** - is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
- 5.06 **“Unauthorized Disclosure”** – intentional or unintentional revealing of sensitive information to individuals, inside and/or outside of the City, who do not have a legitimate need to know that information.
- 5.07 **“VPN”** – a virtual private network within a network infrastructure that is logically closed from all except intended users, which ensures secure remote access in the City network.

## 6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

IT 13.0A – Acceptable Use of the City of Burnaby’s Email Systems Policy  
IT 13.03 – IT Password Policy  
Social Media Use Policy  
IT Security Incident Response Plan  
Respectful Workplace Policy

## **7 PROCEDURES**

- 7.01 All employees and consultants who access the Internet on City-supplied computer systems and secure networks are prohibited from intentionally viewing, downloading, uploading, forwarding, printing, copying or storing digital content which may be considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit or pornographic, sexist, racist, discriminatory, embarrassing, fraudulent, or disrespectful to others.

Access to Internet websites and protocols that are deemed inappropriate for the City's business environment will be blocked.

- 7.02 Certain network behaviour consume considerable network bandwidth and can cause a disruption or delays in network and system connectivity. For this reason, downloading streaming audio, video and other files, or storing large files such as personal photos is prohibited, unless this content is used for business purposes (e.g. City's public website, City's staff portal).

- 7.03 Wireless is provided for convenience and mobility and to reduce mobile data costs, but bandwidth on wireless access points is shared. High bandwidth applications should be deferred to wired connections, where possible. Unless specifically designed and approved, permanent usage of wireless connectivity is discouraged.

- 7.04 Users authorized to use City portable computing devices:
- (a) Must take extra care in public locations to protect the device. If a user is on the move, the portable computer should remain with the user. In circumstances when the user has to leave the device unattended, the device must be locked securely in a safe or cabinet, or with a locking device or cable, or securely with alternative means, and out of plain sight
  - (b) Must restrict data stored on the portable computer to what is necessary for the user's job responsibilities offsite. The device should contain as little sensitive data as possible even when the computer is in a secure City location
  - (c) Should encrypt sensitive data stored on a portable computer to protect against unauthorized access in the event that the computer is lost while in transit. Note that there are restrictions on data encryption for international travel. Users are advised to inform themselves of the entry requirements to foreign countries with regards to encrypted data. Please contact IT Helpdesk for any encryption and decryption requirements
  - (d) Must avoid reviewing or entering sensitive data in public areas to avoid disclosure to prying eyes
  - (e) Must not store passwords on, or keep smart cards with, a portable computer. If the computer is stolen, the loss must be restricted to the computer itself
  - (f) Must not allow a City-owned portable computer to be used by anyone other than the authorized controlling user
  - (g) Must power off, log off, or otherwise lock the portable computer with a secure password when not in use
  - (h) Must keep a direct line of sight with the portable computer while passing through security checkpoints at airports or train or bus stations to minimize

the potential of damage or theft.

7.05 VPN is the preferred method of connecting to the City's network from a remote site. Two-factor authentication must be incorporated to supplement simple password authentication (see IT Password Policy). At no time should any City user provide his or her login or email password to anyone, not even family members nor IT staff. Every employee is responsible for his/her own City account.

7.06 Users who connect remotely to the City's secure networks with non-City owned equipment must have up-to-date virus protection and security patches. Employees that require, as part of their job function(s), to connect using their personal home PCs or laptops, may obtain anti-virus software at no cost from IT.

Devices found to be infecting the City's network will be disconnected immediately. A breach in the protocols listed above may result in the loss of remote access privileges.

7.07 Users will bring forward to their supervisor or manager, on a timely basis, any instances in which they consider:

- (a) Their access to sensitive information is not required to perform their job
- (b) Their access to sensitive information being loaded onto portable media for transport or processing offsite to be excessive or unnecessary altogether, given their job duties
- (c) Their sending of sensitive information, especially through email and email attachments, is without adequate encryption and/or security measures to ensure the safe transfer of such data

7.08 For users of City authorized and issued Personal Storage Devices (PSDs):


- (a) Contractors' PSDs must be scanned for vulnerabilities prior to connecting to the City's secure networks.
- (b) Employees and contractors must take precautions to avoid theft or loss by not leaving mobile devices or PSDs unattended without appropriate security measures (see 7.03).
- (c) PSDs that contain confidential, personal, or sensitive City information assets must use encryption and password protection; the PSD should not be the only place where data maintained for work purposes is stored.

Any sensitive City information assets requiring transmittal to a destination not on the City's secure network must be transmitted using secure technology such as VPN or TLS. Users may contact the IT Helpdesk for assistance. Encryption will be the most current and secure method at the time of the request.

Users applying encryption to the transmittal of sensitive City information assets are responsible for securely communicating the decryption keys to the users receiving their encrypted data.

## 8 ATTACHMENTS

### Information Technology System Access Form

		<h2 style="text-align: center;">Information Technology System Access Form</h2>	
<p style="text-align: center;">**Please ensure IT has a minimum of one week for account set up prior to the start date**</p>			
<u>First Name (Nickname) Middle Initial Last Name</u>		<u>Name Change</u>	
<u>Contact Person to Notify When Complete</u>		<u>Contact Person's Phone Number</u>	
<u>Department</u>		<u>Phone Number</u>	
<u>Windows Account (PC &amp; Thin-Client)</u> <input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete <b>Same as:</b>		<u>Authorizing Signature</u> (sign and print)	
<u>Remote Access Token (if applicable)</u> Are you a Consultant? <input type="checkbox"/> Yes <input type="checkbox"/> No Choose one: <input type="checkbox"/> Physical token <input type="checkbox"/> Software token (Preferred method)		(Information Services use Only)	
<u>Telephone</u> <input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete <b>Note changes to Internal Phone Directory</b> <u>Extension#:</u> <u>Voicemail</u> <input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete <u>Attendant Ext#:</u> <u>Mailbox#:</u>		Additional Comments	
<u>Permits System (LPS) Account</u> <input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete <b>Account name:</b> <b>Same as:</b>		<u>System Owner Signature</u> (sign and print)	
<u>All-in-one Account (Cicero and Oberon)</u> <input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete <b>Same as:</b>		<u>System Owner Signature</u> (sign and print)	

When complete, please mail to the Helpdesk at Information Technology, OR use a Xerox Workstation's scan-to-email to yourself then forward to [helpdesk@burnaby.ca](mailto:helpdesk@burnaby.ca). Original is not required if scanned.

For Hansen access please email Andrea Robertson: [andrea.robertson@burnaby.ca](mailto:andrea.robertson@burnaby.ca)

Revised on: Aug 17, 2015