605. ACCEPTABLE USE OF TECHNOLOGY RESOURCES

SCOPE: This Policy applies to City employees, contractors, vendors and volunteers that access City IT networks and resources unless otherwise addressed by a current collective bargaining agreement or public safety Policy. Failure to comply with this Policy may result in corrective action up to, and including, termination or loss of contract (vendors/contractors).

POLICY: The City maintains computer systems, network utilities, internet and intranet access, e-mail and other technology resources to assist in conducting City business. This Policy applies to the access or use of the City's network and technology resources at any location, at any time, from any device, via wired or wireless connection. They apply to all users of City technology resources. The City authorizes the use of computing and network resources by City staff, temporary employees, contractors, vendors, volunteers and others to conduct City business. All users of City computing and network resources will work in an ethical, legal, and responsible manner. The City will conduct audits of IT resources usage to ensure compliance with this Policy. All use of technology resources must be consistent with all City policies, Operating Principles, as well as all federal, state, and local laws and regulations.

ACCEPTABLE USE AND YOUR RESPONSIBILITIES

1. **No expectation of Privacy**: These resources are for official business use and there should not be any expectation of privacy in any message, file, image, or data created, sent, viewed, retrieved, or received through City resources. In addition, information related to City business that is created on a personal computer, personal electronic communication device, or through a personal e-mail account will not be treated as private and may also be subject to public disclosure or discovery in the event of a lawsuit.

2. You are responsible for exercising good judgment regarding the reasonableness of personal use. The City, however, retains sole authority to determine whether your personal use is consistent with this Policy.

3. City Intellectual Property and Protected Information stored on electronic and computing devices whether owned or leased by City, you, or a third party remains the sole property of City.

4. You are permitted to access, use or share City Protected Information only to the extent it is authorized and necessary to fulfill your assigned job duties.

5. Passwords used to access City's network, systems and applications are to be kept strictly confidential.

6. Administration and user passwords must comply with the Password Management and Requirements Policy.

7. You must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

8. All computing devices must be secured with a password-protected screensaver that activates automatically within 15 minutes or less of inactivity. You must lock the screen or log off when the device is unattended.

9. You have a responsibility to promptly report the theft or loss a City owned computing device (laptop/phone).

10. You have a responsibility to promptly report unauthorized disclosure of City Protected Information.

11. City reserves the right to audit networks and systems to ensure compliance with this Policy.

INTERNET USE AND YOUR RESPONSIBILITIES

1. **Acceptable use of the Internet** consists of activities necessary to support the purpose, goals, and mission of the City of Vancouver and each user's authorized job functions.

   NOTE: The Internet is a network of interconnected computers over which City has no control. The user should recognize this when using the Internet and understand the user might come into contact with information, even inadvertently, that may be considered offensive, sexually explicit, or inappropriate. The users should understand this risk during use of the Internet.

2. **Prohibited use of the Internet**:

   a. Do not access online games, including games found on social websites.

   b. Do not use streaming media unless its use is business related.

   c. To access the Internet, use only IT-approved software. This software must incorporate all vendor-provided security patches required by IT.

   d. If using blogs or websites, do not discuss City business matters or publish material that shows the City in a negative light.

   e. Files downloaded from the Internet must be scanned for malware using IT-approved virus detection software.

   f. Make sure content on all City websites is business related and has been approved by the department publishing the information.

   g. Do not make offensive or harassing material available through City's websites.

   h. Do not use City Internet access for political purposes.

   i. Do not post personal commercial advertising on the City's websites.

   j. Do not use City Internet access for personal financial gain or for personal solicitations.

   k. Do not share sensitive or protected City data without ensuring that the material is secured to only those groups and individuals who are authorized to access it.

UNACCEPTABLE USE AND YOUR RESPONSIBILITIES

The following activities are, in general, prohibited. You may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., system administration staff may have a need to disable the network access of a server for repair or maintenance).

Under no circumstances is any user of City-owned IT Resources authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City-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.

Email and Communication Activities – the following activities are prohibited**:**

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 messaging, whether through language, frequency, or size of messages.

3. Sending any communication that may be viewed as defamatory, discriminatory, sexist, racist, abusive, threatening, obscene, or otherwise inappropriate.

4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5. Changing email header information to intentionally conceal your identity.

System and Network Activities – the following activities are prohibited:

1. Revealing account passwords to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

2. Connecting personal devices such as computers, flash devices (thumb drives) or hand held devices to a City computer or the City's secure internal network. Employee-owned devices may be connected via wi-fi to the City's public Internet service.

3. Using the Internet in a manner that may cause embarrassment, loss of reputation, or other harm to City.

4. 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 or the end user does not have an active license ("pirating").

5. Accessing data, a server, or an account for any purpose other than conducting City business, even if you have authorized access.

6. Introducing malicious programs (malware) into the network, a computer, or a server (e.g., viruses, worms, trojan horses, key loggers, network analyzer, protocol analyzer or packet analyzer) etc.).

7. Tampering with or otherwise attempting to circumvent computer or network security controls.

8. Executing any form of network monitoring which will intercept data not intended for your City authorized computer or device, unless this activity is a part of your normal job/duty.

9. Circumventing user authentication or security of any host, network or account.

10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or deny service to, a user's computer session, via any means, locally or via the Internet/Intranet/Extranet.

REMOTE ACCESS

Any individual or entity that remotely access City network resources will only use IT-provided access methods. These include, but are not limited to, Remote Desktop Gateway, Microsoft Outlook Web Access, VPN, etc.

MONITORING

The City reserves the express right to monitor and inspect the activities of the employee, contractor, vendor or volunteer while accessing the Internet at any time. Any use of City information technology resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed.

EXCEPTIONS

Any exception to the Policy must be submitted in writing to the Information Security Officer and approved by both the Information Security Officer and the IT Director.

NON-COMPLIANCE

Anyone found to have violated this Policy may be subject to disciplinary action, up to and including, termination or loss of contract (vendors/contractors).

RELATED STANDARDS, POLICIES AND PROCESSES

CoV IT Information Security Program Policy
CoV IT Information Security Standards
CoV Password Management and Requirements Policy

REVISION HISTORY

Date of Change	**Responsible**	**Summary of Change**
Dec 2017	Information Security Officer	Significant content update to Policy 605