

**Purpose:**

- 1 To establish standards to:
  - (1) protect the integrity of The City's information technology (IT) systems, services, and networks;
  - (2) protect the integrity of personal information in the custody of The City; and
  - (3) promote acceptable use of The City's information technology systems.
- 2 To inform authorized users of The City's information technology (IT) systems of the consequences for inappropriate and/or fraudulent use.

**Policy Statement(s):**

- 1 Employees adhere to all related policies and procedures when using The City's IT Infrastructure.
- 2 All devices need to be approved and configured by Information Technology Services (ITS) before connecting to the Corporate network.
- 3 The City disconnects devices or disables services without notification for the sake of maintaining the integrity of The City's IT infrastructure.

**4 Expectations of Use**

- (1) Users do not:
  - (a) use the provided technology in any way that advances personal financial gain;
  - (b) use the provided technology for deliberately interfering or disrupting other users through electronic distribution of unsolicited advertising;
  - (c) visit web sites, download, upload, save, send, or knowingly receive material that includes sexually explicit or pornographic content, or other material using sexist, racist, threatening, violent, or defamatory language;
  - (d) conduct gambling or illegal activities; or
  - (e) share confidential information outside of appropriate channels.
- (2) Additional usage is permitted as required by the user's role or as approved by Management in extenuating circumstances.
- (3) Users may use provided information technology for a limited amount of non-City-related purposes, providing such use:
  - (a) does not cause additional expense to The City;
  - (b) is performed on the employee's personal time; and
  - (c) is done in accordance with this Policy.
- (4) Network Use and Access:
  - (a) Users complete The City's Network Basic Training course. Users must read, understand, and agree to the conditions of use in order to access the City's network.
  - (b) ITS personnel notify users of any scheduled maintenance which may impact the user's access of the network.

- (c) Users are assigned a “My Documents” area that is secured to the individual user with limited drive space imposed.
  - (d) Departments are assigned a network folder that allows for the storing and sharing of business information among group members.
  - (e) Authorized City staff have access to The City’s Electronic Records Management Systems (ERMS).
  - (f) Network drives, application systems data, and the ERMS are used for business purposes and are backed up for business resumption purposes only.
  - (g) Local hard drives are not for permanent business storage and are not backed up.
  - (h) Users who generate, create, alter, or handle sensitive data take reasonable measures to safeguard and maintain the accuracy of the data.
- (5) Wireless and Wireless Networks:
- (a) All networks within city facilities and property require ITS approval.
- (6) Internet and E-mail Services:
- (a) Corporate emails are subject to search and retrieval as required in accordance with a FOIP request.
  - (b) Users do not use personal email (third party email services) to send corporate email messages.
  - (c) All forms of electronic communication through The City’s Internet service are monitored and controlled by ITS.
- (7) Social Media/Social Networking:
- (a) The City monitors social media for contributions or comments relating to The City, its staff, its operation, and its reputation.
  - (b) When using and posting on City moderated social media sites and/or profiles, employees:
    - (i) adhere to ethical and professional standards;
    - (ii) only make comments on behalf of The City if/when authorised to do so;
    - (iii) do not post confidential or proprietary information about The City, its operations, and/or its staff; and
    - (iv) conduct themselves in accordance with this Policy, other applicable policies and procedures, and legislation.
  - (c) When posting about The City on personal social media sites and/or profiles, employees:
    - (i) speak about The City, in an accurate, respectful, and professional manner;
    - (ii) do not make statements on behalf of The City;
    - (iii) identify when comments are of a personal opinion, and not The City’s official position;
    - (iv) do not post confidential or proprietary information about The City, its operations, and/or its staff; and
    - (v) do not misrepresent or risk the reputation of The City in any way.
  - (d) Any inappropriate personal social media activity by employees, brought to the attention of The City, is subject to the “Failure to Meet Expectations of Use” section below.
- (8) Corporate Networked Devices:
- (a) Connecting unauthorized equipment to devices and/or network is prohibited.
  - (b) Only approved software, which is licensed or owned by The City, is installed on these devices. Unauthorized software is removed.

- (c) All software installations and device troubleshooting is done by authorized ITS personnel. ITS personnel clearly identify themselves and provide proper identification before accessing the user's device.
  - (d) ITS determines which device configurations can be modified by the user.
  - (9) Corporate Non-Networked Devices:
    - (a) ITS determines the access rights the user has to the device.
    - (b) Where ITS has granted administrative rights to the user of the device:
      - (i) users may install software and apps and it is the user's responsibility to ensure all software is properly licensed;
      - (ii) the user is responsible for the backup, restore and security of the software they install; and
      - (iii) the device may be utilized for personal use (including the installation of application software (apps)) in accordance with this Policy.
  - (10) Personal Devices:
    - (a) Department Head and ITS approval is required to allow a personal device to replace a City supplied device; a personal device cannot replace a Corporate Networked Device.
    - (b) Devices used to replace City owned equipment are presented to ITS for configuration before they are allowed access to City resources.
    - (c) The City does not reimburse employees for the purchase of their personal device.
    - (d) Reimbursement of a portion of the ongoing service fees of Personal Devices is given only with prior department Manager approval.
    - (e) ITS determines what operating systems are supported.
    - (f) Connectivity issues are supported by ITS on a best effort basis.
      - (i) Users contact the device manufacturer or service provider for operating system or hardware related issues.
    - (g) Users assume all liability for the partial or complete loss of personal or City data, that impacts the usability of their personal device, due to technical issues.
  - (11) Remote Access:
    - (a) Remote access to the City's network must be authorized, and conducted on a City supplied device or device supported and approved by ITS.
  - (12) Monitoring:
    - (a) ITS monitors the use of City networks for capacity and resource usage.
    - (b) In the event of unintentional discovery of violations of expected use, ITS alerts the appropriate supervisor.
    - (c) ITS may block access to certain Internet sites when they affect system performance, threaten integrity, and/or are considered inappropriate.
    - (d) The Director of Communications and Strategic Planning monitors compliance with requirements for social media use and informs supervisors of non-compliance.
- 5 Failure to Meet Expectations of Use:
- (1) Failure to meet the expectations of use in this Policy may result in:
    - (a) denied access to The City's information technology systems;
    - (b) progressive disciplinary action up to and including dismissal; and

- (c) potential legal prosecution.
  - (2) A supervisor, suspecting an employee of violations of expected use, follows Corporate Procedure 5203-CP ITS Security Incident Plan to respond to the situation.
- 6 Information Technology Security:
- (1) General:
    - (a) Access to applications, systems, and data are protected by an authentication mechanism.
    - (b) ITS employs endpoint protection on all Corporate Networked Devices and Corporate Non-Networked Devices.
    - (c) Networked devices conform to ITS approved network security requirements.
    - (d) Employee access to City data/resources is limited based on their security level, as defined by ITS and their department Manager.
    - (e) Passwords conform to ITS criteria based on current industry standards.
    - (f) Users ensure all downloads are scanned for viruses before using them.
  - (2) Users:
    - (a) are provided with valid login credentials to access the network;
    - (b) are accountable for all actions performed with their login credentials;
    - (c) are required to change their password at regular intervals as determined by ITS;
    - (d) lock workstations when unattended;
    - (e) follow procedures set out in Corporate Procedure 5203-CP ITS Security Incident Plan in the event of an Information Security incident;
    - (f) do not share network or application specific login credentials, or allow unauthorized users access to The City's information technology; and
    - (g) upon termination of employment, return all City information technology property.
  - (3) Termination of Login Credentials:
    - (a) Inactive accounts are disabled.
    - (b) Supervisors follow City termination processes to notify ITS of a user's termination.
  - (4) Information Management:
    - (a) Users do not use third-party information technology services without ITS approval.
    - (b) Users refer to Corporate Procedure 5211-CP Cloud Computing Decision Making when cloud services are required.
    - (c) Users do not access data or information systems without proper authorization.
  - (5) Mobile Device Management:
    - (a) ITS determines the requirement of mobile device management on a per device basis.
    - (b) ITS confirms mobile device configuration complies with this Policy.
    - (c) Where possible, mobile devices have current (and ITS approved) mobile device management, endpoint protection, encryption, and security related software installed on them.
    - (d) Mobile devices are:
      - (i) subject to valid ITS approved compliance rules;
      - (ii) kept physically secure;
      - (iii) password protected;

- (iv) set to automatically lock after being idle for five minutes;
  - (v) set to automatically wipe all resident data after five unsuccessful attempts to unlock a device; and
  - (vi) configured to encrypt data where capable.
- (6) Personal Devices:
- (a) On Personal Devices, employees are responsible to:
    - (i) back up personal data;
      - (A) The City is not responsible for lost data in the event of a personal device being wiped in accordance with this Policy.
    - (ii) ensure all manufacturer updates and patches are installed on a regular basis; and
    - (iii) ensure confidential data on devices is secure.
  - (b) Personal Devices are not granted access to the The City's corporate network Employees immediately report the loss or theft of a device storing corporate data to ITS and ITS remotely wipes all data from the device
- (7) Removal and Protection of City data:
- (a) ITS reserves the right to wipe all data from all devices as defined in this Policy:
    - (i) if the device is found to be non-compliant with this Policy;
    - (ii) if device inspection is not granted in accordance with this Policy;
    - (iii) upon termination of employment;
    - (iv) at the end of the life of the device; and
    - (v) if ITS detects the device poses a threat to the security of The City's data or technological infrastructure.
  - (8) Tracking IT Assets:
    - (a) ITS tracks all Corporate Networked and Non-Networked Devices.
    - (b) Users are required to contact ITS to reassign, relocate, or dispose of any device (including printers) to ensure the protection of City assets and data.

### Definitions:

- 7 "**Corporate Networked Devices**" means laptops, tablets, and desktops, that are owned by The City, and a member of The City's corporate network.
- 8 "**Corporate Non-Networked Devices**" means smart phones, laptops, tablets, and desktops, that are owned by The City, that send, receive, or store City information using any connection other than a City corporate network connection.
- 9 "**Mobile Device**" means a portable device, which can include Corporate Networked Devices, Corporate Non-Networked Devices, and Personal Devices, that send or receive City data to a City network, or store City Information.
- 10 "**Personal Devices**" means smart phones, laptops, tablets, and desktops that are not owned by The City and not a member of The City's corporate network that send, receive, and store City information.

**References/Links:**

- 1 *Freedom of Information and Protection of Privacy Act*
- 2 2024-CA Respectful Workplace
- 3 2024-CP Respectful Workplace
- 4 2025-CA Ethical Standards
- 5 2212-CA Corporate Security
- 6 5007-CP Records Management
- 7 5203-CP ITS Security Incident Plan
- 8 5210-CA Records Management

**Scope/Application:**

- 1 This Policy applies to all employees, and anyone granted access to The City's information technology, systems, services, and networks.

**Authority/Responsibility to Implement:**

- 1 Information Technology Services Manager is responsible for reviewing this Policy and monitoring for compliance.

**Inquiries/Contact Person:**

- 1 ITS Service Desk

**Policy Monitoring and Evaluation:**

- 1 The ITS Manager will evaluate this Policy one year from the approval date and every three years after that, with revisions made as required.

**Document History:**

<b>Date:</b>	<b>Approved/Reviewed By:</b>	<b>Title:</b>
May 4, 2018	"Craig Curtis"	City Manager