FORTFRANCES
BOUNDLESS

INFORMATION TECHNOLOGY RESOURCES

HUMAN RESOURCES 3.20

POLICY

Created:	2022-10-11
Revised:	
Authorized:	Resolution X on 2022-10-11
Superseded:	Resolution 150 on 2007-04
	Resolution 300 on 2009-10

1. PURPOSE

(1) This policy establishes controls governing the use of Data and IT Resources provided to Users from the Town by:

(a) Identifying the responsibilities of Users;

(b) Identifying prohibited User actions and ensuring the primary use of Data and IT Resources is for the Town's business activities;

(c) Protecting the confidentiality, integrity, and security of the Town's Data and IT Resources; and

(d) Informing Users about electronic monitoring.

2. APPLICATION

(1) This policy applies to all Users who:

(a) Create, distribute, access, or manage Data owned by the Town; and

(b) Access or manage IT Resources owned or operated by the Town, excluding:

(i) Members of the general public interacting with publicly accessible Town services.

3. PRIVACY

(1) The ***Employment Standards Act, 2000*** does not:

(a) Establish a right for employees not to be electronically monitored by their employer; or

(b) Create any new privacy rights for employees.

(2) IT Resources are Town property.

(3) IT Resources are provided to Users only so they can effectively conduct the responsibilities of their role with the Town.

(4) Users shall not expect privacy with respect to their use of IT Resources. Any use of IT Resources may be reviewed by the Town for the purposes outlined in Section 4.5 of this policy.

(5) Data stored on or created using IT Resources is Town property.

(6) The use of Credentials shall not create a reasonable expectation of privacy or confidentiality of Data.

(7) Access to Data may be granted to other Users through succession activities.

(8) Data is subject to relevant legislation and may be accessed by requests through ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

4. ELECTRONIC MONITORING

(1) The ***Employment Standards Act, 2000*** requires the Town to have a written policy on whether the Town electronically monitors employees, including:

(a) A description of how and in what circumstances the Town may electronically monitor employees; and

(b) The purposes for which information obtained through electronic monitoring may be used by the Town.

(2) The Town electronically monitors Users.

(3) Electronic monitoring Data may be captured using live telemetry and historical logs of:

(a) Software events, including but not limited to:

(i) Any event generated by any operating system or application installed on a Town device; and

(ii) Any event generated by any cloud application licensed or operated by the Town;

(Examples: launching Diamond from a Town workstation, making changes to an inventory record on CityWide from a personal smartphone, etc.)

(b) Network activity, including but not limited to:

(i) Attempts to access any Town network, device, or network location;

(ii) Information transmitted between any Town device and any network location (including the Internet); and

(iii) Information transmitted between any device connected to a Town network and any network location (including the Internet);

(Examples: signing into FMW from a Town workstation, uploading an EFT payment to a banking website from a Town workstation, watching YouTube from a personal smartphone connected to the Town's guest network, etc.)

(c) Communications, including but not limited to:

(i) Content and Metadata of emails and other messages sent or received by any Town device;

(ii) Metadata of emails and other messages sent or received by any device connected to a Town network;

(iii) Content and Metadata of emails and other messages sent or received by any cloud application licensed or operated by the Town; and

(iv) Content and Metadata of telephone calls sent, received, or forwarded by any Town telephone connected to a Town telephone system;

(v) Metadata of telephone calls sent, received, or forwarded by any Town Mobile Device;

(Examples: chatting through Teams from a Town workstation, sending email from a personal smartphone connected to the Town's guest network, receiving messages through When I Work, receiving voicemail from a desk phone at a Town workstation, timestamped logs of telephone numbers called from a Town smartphone, etc.)

(d) Physical movement, including but not limited to:

(i) GPS locations of Town vehicles and Town Mobile Devices; and

(ii) Attempts to access any secured Town facility or secured area in a Town facility;

(Examples: performing snow removal using a monitored Town vehicle, entering the Fire Hall outside of normal business hours, etc.)

(e) Video surveillance, including but not limited to:

(i) Images recorded by cameras at Town facilities; and

(ii) Images recorded by Town cameras in public spaces; and

(Examples: parking a vehicle at the Memorial Sports Centre, walking through the Rainy Lake Square, etc.)

(f) Use of input and output devices, including but not limited to:

(i) Cameras;

(ii) Scanners; and

(iii) Printers.

(Examples: accessing the Town's video surveillance infrastructure, scanning documents from a Town copier to a personal email, printing documents from a Town workstation, etc.)

(4) Electronic monitoring Data may be captured at any time.

(5) Electronic monitoring Data shall be used only for purposes that support the enforcement of this policy, including but not limited to:

(a) Protecting Data and IT Resources by investigating any security breaches, network anomalies, or violations of this policy as required;

(b) Preventing and responding to inappropriate or illegal activities;

(c) Administering Data and IT Resources, evaluating utilization, and planning for future use;

(d) Evaluating employee performance and supporting productive work environments; and

(e) Fulfilling freedom of information requests through ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

5. INCIDENT RESPONSE

(1) The IT Department shall always maintain unrestricted physical access to all physical IT Resources, excluding:

(a) Mobile Devices deployed to Users;

(b) Physical Credentials deployed to Users; and

(c) Physical IT Resources deployed within secured Water and Wastewater facilities.

(2) As necessitated by IT Department procedures, the Town may:

(a) Analyze electronic monitoring Data and share that Data with contracted third-party cybersecurity organizations;

(b) Limit any use of Data or IT Resources; or

(c) Recall, lock, or factory reset Mobile Devices at any time.

6. USER RESPONSIBILITIES

6.1. COMPLIANCE

(1) Users shall comply with all Town policies, procedures, and standards while using Data and IT Resources, including but not limited to:

(a) The ***Code of Conduct*** (By-Law No. 04/19);

(b) The ***Media Communication Policy*** (1.1);

(c) The ***Use of Corporate Resources in Election Periods Policy*** (1.17);

(d) The ***Employee Conduct Policy*** (3.7);

(e) The ***Social Media Conduct Policy*** (3.27);

(f) The ***Council / Staff Relations Policy*** (3.32);

(g) The ***Workplace Harassment Policy*** (5.34.1); and

(h) ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

(2) Users shall complete any security and compliance training prescribed by IT Department procedures.

(3) Users shall immediately report to the IT Department:

(a) Any inappropriate use of Data or IT Resources;

(b) Any lost, stolen, compromised, or damaged IT Resources; and

(c) Any loss, theft, or unauthorized disclosure of Data.

(4) Users shall comply with any investigation by the Town surrounding their use of Data or IT Resources.

(5) Users who violate this policy may be subject to appropriate actions, including but not limited to:

(a) Restriction, suspension, or revocation of access to Data or IT Resources;

(b) Disciplinary measures, up to and including termination of employment;

(c) Legal action, including damages, indemnification, or cost recovery; or

(d) Prosecution by local, provincial, or federal authorities.

6.2. LEGAL OBLIGATIONS

(1) Users shall comply with the laws and regulations of all applicable jurisdictions while using Data and IT Resources, including but not limited to:

(a) ***The Criminal Code of Canada***;

(b) ***The Copyright Act of Canada***; and

(c) ***The Municipal Freedom of Information and Protection of Privacy Act of Ontario***.

(2) Users shall adhere to all copyrights, patents, and licensing agreements for intellectual property licensed by the Town.

6.3. SECURING CREDENTIALS

(1) Users shall take every precaution reasonable to ensure their Credentials are always secure.

6.4. SECURING DATA

(1) Users shall utilize Data only for the purposes intended by the Town.

(2) Users shall take every precaution reasonable to ensure the Data they access is always secure.

(3) Users shall store and delete Data subject to the ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

6.5. SECURING DEVICES

(1) Users shall secure unattended devices in a manner that restricts access to them using only authorized Credentials.

(2) Upon the termination of their role with the Town, Users shall immediately return to the IT Department all physical IT Resources and physical Credentials issued to them by the Town.

6.6. SECURING MOBILE DEVICES

(1) Users may be assigned Mobile Devices to perform their role with the Town as determined by their supervisor in consultation with the IT Department.

(2) Users shall always maintain the enrollment of Mobile Devices in the Town's Mobile Device Management platform.

(3) Users shall always maintain the compliance of Mobile Devices with the configuration prescribed by the Town's Mobile Device management platform.

(4) Users shall take every reasonable precaution, with consideration given to their work environment and assigned tasks, to ensure Mobile Devices are always secure and protected from physical damage.

(5) Users may be invoiced by the Town for any Mobile Device costs the Town determines to be the result of personal use, including but not limited to:

(a) Enhanced device specifications;

(b) Usage overages; and

(c) Damage.

7. PROHIBITED ACTIONS

7.1. INAPPROPRIATE ACTIVITIES

(1) Users shall not use Data or IT Resources for purposes unrelated to the Town's business activities, including but not limited to:

(a) Commercial activities;

(b) Activities prohibited by Town policies or procedures; or

(c) Unauthorized charitable or not-for-profit activities.

(2) Users shall not use IT Resources for personal activities while on duty during working hours, including but not limited to:

(a) Activities that result in increased costs to the Town;

(b) Activities in locations that may disrupt the productivity of other Users;

(c) Social telephone calls or communications; or

(d) Playing games, watching videos, or browsing the Internet recreationally.

(3) Users shall not use personal email accounts to conduct the Town's business activities.

7.2. HARASSMENT

(1) Users shall not use Data or IT Resources to engage in harassment, including but not limited to:

(a) Cyberbullying;

(b) Fraudulent, abusive, malicious, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise inappropriate conduct; or

(c) Potentially offensive comments concerning religion, politics, or social policies.

7.3. DISRUPTION

(1) Users shall not circumvent or disclose any security measures implemented by the Town.

(2) Users shall not share or disclose any Credentials without authorization.

(3) Users shall not use Data or IT Resources for disruptive purposes, including but not limited to:

(a) Unauthorized access to IT Resources;

(b) Unauthorized impairment of IT Resources;

(c) Unauthorized deployment or removal of IT Resources; or

(d) Connecting unauthorized network or storage devices to IT Resources.

(4) Users shall not leave devices unattended in areas accessible by the public.

7.4. UNAUTHORIZED DATA USE

(1) Users shall not access nor attempt to access unauthorized Data, including but not limited to:

(a) Data not authorized for use by that User;

(b) Data protected under copyright law that is not licensed by the Town;

(c) Data that incurs usage fees that is not licensed by the Town; or

(d) Data that is obscene.

(2) Users shall not publish to any print or digital platform any unauthorized Data, including but not limited to:

(a) Images, video, or audio of individuals under the age of 18 without written consent of the parents or guardians of those individuals; or

(b) Images, video, or audio of individuals over the age of 18 without written consent of those individuals.

(3) Users shall not store Data on unauthorized devices.

(4) Users shall not attempt to nor successfully impair or exfiltrate Data.

(5) Users shall not destroy Data, except where authorized under the ***The Ontario Municipal Records Management System*** (By-Law No. 47-16).

7.5. USE OF MOBILE DEVICES

(1) Users shall not use Mobile Devices when it is unsafe to do so, including but not limited to:

(a) Non-firefighter Users operating vehicles;

(b) Firefighter Users operating vehicles while not responding to an emergency; or

(c) Connecting Mobile Devices to networks that are reasonably expected to be compromised.

(2) During offboarding procedures, Users shall not retain any telephone numbers of Mobile Devices assigned to them, excluding any telephone numbers released by Users to the Town during onboarding procedures.

8. DEFINITIONS

- **"Authorization"** means approval explicitly obtained from the IT Department, including but not limited to:
    - Configurations of permissions to IT Resources granted by the IT Department in consultation with a User's supervisor; and
    - Written requests for permissions from a User's supervisor to the IT Department.
- **"Credential"** means any method of authentication that grants access to otherwise restricted Data or IT Resources, including but not limited to:
    - Physical keys, proximity fobs, or hardware tokens;
    - Passcodes or personal identification numbers;
    - Combinations of usernames and passwords, or security questions and answers; and
    - Biometrics or gestures.
- **"Data"** means records stored on IT Resources, including but not limited to:
    - Documents;
    - Databases;
    - Media files;
    - Communications;
    - Metadata;
    - Location information; and
    - Activity logs.
- **"IT"** means Information Technology.
- **"IT Department"** means the IT Manager and any staff under the direction of the IT Manager.
- **"IT Resource"** means hardware, software, and networks, including but not limited to:

- Computing devices, such as servers, desktops, or Mobile Devices;
- Network devices, such as switches, access points, firewalls, printers, or scanners;
- Peripheral devices, such as mice, keyboards, docks, headsets, or cameras;
- Storage devices, such as hard drives, flash drives, tapes, disks, or optical media;
- Local services, such as applications, phone systems, network bandwidth, or storage; and
- Cloud services, such as Internet, email, collaboration tools, social media, or other digital assets.

- **"Metadata"** means Data that provides information about other Data, but not the content of that Data.
- **"Mobile Device"** means portable computing devices, including but not limited to:
  - Laptops;
  - Tablets; and
  - Smart Phones.
- **"Town"** means the Corporation of the Town of Fort Frances.
- **"User"** means anyone that accesses Data or IT Resources, including but not limited to:
  - All members of Council (including the Mayor);
  - Committee and board members;
  - Staff;
  - Volunteers; and
  - Contractors.