BRAMPTON

ADMINISTRATIVE DIRECTIVE

Category: Information and Technology

Use of Information Technology Resources

Policy Number: ITS-100
Approved by: CAO/CLT – August 1, 2024
Administered by: Information Technology
Effective Date: August 1, 2024

1. Background

The Corporation of the City of Brampton is committed to promoting appropriate and responsible use of technology in order to enable a productive working environment for all City Information Technology (IT) Users. Inappropriate use exposes the City to increased legal risk, risk of Malware, and other threats that may compromise City business systems.

2. Purpose

The purpose of this Administrative Directive is to provide governance and awareness for the acceptable use of IT Resources at the City which includes, but is not limited to, computers, printers, mobile devices (including smartphones, tablets), software, network resources (including Internet, Messaging, and Social Media), and telephones (including voicemail).

3. Application and Scope

3.1 This Administrative Directive applies to:

3.1.1 Any Employee, Member of Council, Contractor, Consultant, Vendor or Volunteer doing business with the City that has access to or makes use of the City's IT Resources in any form (collectively referred to as "Users").

3.1.2 City-owned or leased equipment and any permitted personal or third-party devices that connect and access the IT Environment.

3.1.3 IT data accessed and stored on City systems regardless of access on-site or remotely.

3.2 Exceptions

3.2.1 Members of the public who are interacting with the City's public websites and services, including public Wi-Fi, which are subject to other terms and conditions.

4. Outcomes

The intended outcomes of this Administrative Directive are to:

4.1 Identify acceptable use and restrictions for Users

4.2 Ensure the primary use of IT Resources is for City business purposes

4.3 Protect the confidentiality and integrity of data and information to ensure only authorized Users have access

4.4 Ensure security and protection of IT Resources from cyber and other threats

5. Mandatory Requirements

5.1 Access and Use of City Resources

5.1.1 The use of IT Resources is reserved for the purpose of conducting City business and is not to be used for any unlawful or prohibited purposes.

5.1.2 Occasional or incidental Personal Use of IT Resources is permitted within reasonable limits, provided it does not:

a) Negatively impact work performance.

b) Interfere with work activities of others.

c) Breach this or any other policy or directive.

d) Consume significant IT resources.

e) Result in degradation of IT services.

f) Transmit or store excessive personal content.

Users should consult guidelines and training resources for clarity on what constitutes reasonable limits of Personal Use.

5.1.3 Users will be issued an account with a unique username and password for access to IT Resources. Users must:

a) Be responsible for all activities performed under their account.

b) Not divulge their username or password to any other person.

c) Immediately change their password if they think it has been compromised and notify the IT Service Desk.

5.1.4 Multi-factor Authentication is required to be set up on User accounts to enable access to systems while remote from a City facility.

5.1.5 Users are prohibited from using another User's account or sharing credentials or systems access with others.

5.1.6 Users are prohibited from accessing systems or information they have not been authorized to use as part of their duties.

5.1.7 Devices are not to be left unattended in a position where unauthorized access could occur or the device could be stolen. The password protected screensaver (press ⊞ + L) on computers and passcode enforced screen lock for mobile devices shall be activated whenever device is not in active use.

5.1.8 The City reserves the right to delete, intercept, or block any traffic on its networks to prevent spam, pornography, hate-related material, or

illegal use of City property and violation of City policies and procedures.

5.2 Unacceptable Use of IT Resources

5.2.1 Users are prohibited from using IT Resources for:

a) Soliciting or conducting non-City work.

b) Non-City business.

c) Personal gain or profit.

5.2.2 IT services and equipment are not to be used to access inappropriate content including, but not limited to:

a) Pornography, substances, alcohol, tobacco, dating, and gambling.

b) Copyrighted material without the owner's express permission.

c) Sources used to advance or endorse views or ideas which are likely to promote discrimination, contempt, or hatred for any person.

5.2.3 Users shall not use IT Resources to send spam or unsolicited messages.

5.2.4 Users shall not forge, misrepresent, or obscure their identity on any electronic communication to mislead the recipient.

5.2.5 Users have the right to voice their opinions on their own time and at their own risk. To avoid risk to the City's reputation and Users' employment status, Users should:

a) Avoid creating an impression that personal views represent the City.

b) Maintain the privacy and confidentiality of City information.

c) Offer constructive feedback about an issue or concern related to the City of Brampton.

d) Act in a respectful and civil manner in compliance with the City's code of conduct and other policies.

Consult City guidelines and Standard Operating Procedures (SOPs) on the Personal Use of Social Media for further clarity.

5.3 Use of Digital Assets

5.3.1 City email accounts are the property of the City. Users should not register City email accounts for personal, non-business or non-commercial services such as Social Media, cloud storage, etc. The

use of a City email address could breach non-commercial license agreements intended for Personal Use only.

5.3.2 Exceptions to this may include services and Social Media related to Professional Affiliations, Practices, or Designations which require a work email.

5.3.3 Information Assets, including City data, documentation, and digital content shall remain the Intellectual Property of the City and shall be used and stored in accordance with the City Information Management Administrative Directive, Privacy Administrative Directive, and Records Retention By-law with the relevant licenses, contractual terms, and conditions.

5.3.4 Users shall take all reasonable precautions to protect Information Assets of the City when shared with third parties through non-disclosure agreements, contractual agreements, or appropriate disclaimers indemnifying the City.

5.3.5 Information Assets authorized for release to the public are subject to terms and conditions of use and must meet the City's Information Management Policy, and Privacy Administrative Directive.

5.4 Software and Hardware

5.4.1 Users are not to acquire software or hardware without complying with the Acquisition of IT Related Applications, Solutions and Hardware SOP.

5.4.2 Only software licensed and approved by IT Services for use is to be installed on IT computers.

5.4.3 Users who download files or software without approval may be held responsible for costs incurred by Malware damage or unlicensed software.

5.4.4 No Unauthorized Device is to be connected to the internal IT network.

5.4.5 Users assigned IT equipment are expected to use good judgement, demonstrate a sense of responsibility, and provide due care, custody, and control.

5.4.6 Users must promptly notify IT Services to report any loss, theft, or damage of IT equipment within 24 hours.

5.4.7 Information Technology has a planned lifecycle to refresh IT equipment at end of life. Replacement of lost, stolen, or damaged equipment is the responsibility of the Division to which the equipment is assigned.

5.4.8 Users may be held responsible for the costs of repairs or replacement of damaged City-issued equipment in their care due to reckless or negligent actions.

5.5 Mobile Devices

5.5.1 Users who have a City-issued mobile device must comply with the City's Expenses – Personal Usage Reimbursement – City Provided Cell Phones SOP.

5.5.2 Personal mobile devices may be used to access corporate email, calendar, and contacts. However, all risks and costs associated are the responsibility of the device owner.

5.5.3 Users are permitted to install apps on their City-issued mobile devices provided they are in compliance with section 5.1.2 and 5.2 of this Administrative Directive.

6. Roles and Responsibilities

6.1 Chief Information Officer and IT Division

6.1.1 Ensure the administration, revision, and interpretation of this Administrative Directive.

6.1.2 Monitor the use of IT Resources to ensure compliance with corporate policies and procedures.

6.1.3 Establish hardware, software, video, and communications technology standards to ensure a secure and reliable information technology and communications environment.

6.1.4 Provide training opportunities on a regular basis for all standardized applications and for all User groups.

6.1.5 Operate a Service Desk support service for User inquiries on all standard applications.

6.1.6 Oversee all computer equipment installations, modifications, and relocations.

6.2 Managers and Supervisors

6.2.1 Ensure employees are aware of this Administrative Directive and all underlying procedures and reporting any contraventions of it.

6.2.2 Investigate reported contraventions to ensure that there is compliance.

6.2.3 Ensure that access rights of employees are issued or revoked when changes are required.

6.3 Users

6.3.1 Read and comply with this Administrative Directive.

6.3.2 Ensure confidential information is handled appropriately.

6.3.3 Report any known or suspected violations to the immediate supervisor or manager.

7. Monitoring and Compliance

7.1 Usage Monitoring

7.1.1 The City respects the privacy of Users. However, the City reserves the right to monitor all City information technology to ensure proper working order, appropriate use by employees, and security of corporate IT resources and assets as per terms and conditions of employment and in compliance with City guidelines and procedures.

7.1.2 The City may delete, intercept, or block any traffic on its networks to prevent spam, pornography, hate-related material, illegal use of City property, and violation of City policies and procedures.

7.1.3 Information in the Users' care may be subject to discovery requests under the *Municipal Freedom of Information and Protection of Privacy Act, 1990*, or internal review in respect of any devices or systems they use in connection with City business. This discovery process may extend to personal data and communications stored within the IT Environment.

7.2 Consequences of Non-Compliance

7.2.1 Users in breach of this Administrative Directive will be reported to the appropriate level of management, who may take remedial action up to and including dismissal.

7.2.2 Users who violate laws when using the IT Environment may be subject to criminal or civil prosecution.

8. Definitions

8.1 **Information Assets** – Any physical device, software applications, data, or documentation within the IT Environment.

8.2 **IT Resources** – Computers, printers, mobile devices (including smartphones, tablets, and smartwatches), software, network resources (including Internet, Messaging and Social Media), and telephones (including voicemail).

8.3 **IT Environment** – The entirety of Information Technology Resources.

8.4 **Malware** – Malicious software including viruses, trojans, adware, spyware, and ransomware.

8.5 **Messaging** – Mobile, texting, email, and other online texting applications.

8.6 **Personal Use** – Any use that is not City business or work-related.

8.7 **Professional Affiliations, Practices or Designations** – An organization or a group a person belongs to based on expertise or involvement in a particular profession.

8.8 **Social Media** – Websites and applications that enable Users to create and share content or participate in social networking. Some examples include Facebook, X (formerly Twitter), Instagram, Snapchat, and LinkedIn.

8.9 **Unauthorized Device** – Electronic devices such as those described as IT Resources that are not explicitly authorized for use on the City network.

8.10 **Users** – Any employee, Member of Council, contractor, consultant, vendor, or volunteer that have access to or make use of the City's IT Resources in any form.

9. References and Resources

This Administrative Directive should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available.

9.1 External references

- Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c. M.56

9.2 References to related bylaws, Council policies, and administrative directives

- 14.18.1 Brampton Open Data
- Corporate Fraud Prevention Policy GOV-110
- Employee Code of Conduct HRM-100

- Official Use of Social Media Admin Directive COM-110
- Information Management Admin Directive GOV-210
- Privacy Administrative Directive GOV-130
- Purchasing By-Law 19-2018
- Purchasing Card PUR-120
- Records Retention By-Law 272-2014
- Respectful Workplace Policy HRM-150

9.3 References to related corporate-wide procedures, forms, and resources

- SOP on Expenses – Personal Usage Reimbursement – City Cell Phones
- SOP for Submission of Claims for Loss of Damage to City Assets
- SOP Personal Use of Social Media by City of Brampton Employees
- SOP Acquisition of IT Related Applications, Solutions and Hardware

10. Revision History

Date	Description
2019/10/31	Approved by SLT. Replaces 2.11.0 Information Technology Use Policy upon Council resolution.
2022/08/11	Hyperlinks corrected – authorized by Manager, Digital Innovation.
2024/08/01	Approved by CLT. Updated content and hyperlinks.
2026/01/09	Approved by the Chief Information Officer. No changes committed.