BRAMPTON

ADMINISTRATIVE DIRECTIVE

Category: Information Technology

Use of Information Technology Resources ITS-100

Directive Number: ITS-100
Approved by: SLT
Administered by: Digital Innovation & Information Technology
Effective Date: October 31 2019

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 viruses, 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 Information Technology resources at the City which includes but is not limited to, computers, printers, mobile devices (including smartphones and tablets), software, network resources (including Internet, messaging and social media) and telephony (including voicemail).

3. Application and Scope

This Administrative Directive applies to:

a. Any Employee, Member of Council, Contractor, Consultant, Vendor or Volunteer doing business with the City that has access to and/or make use of the City's IT resources in any form (collectively referred to as "Users");

b. City owned or leased equipment and any permitted personal or third party devices that connect and access the IT environment; and

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

3.1 Exceptions

Members of the general 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 business purposes;

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

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

5.2 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.

5.2.1. Occasional or incidental personal use of information technology 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; and

f. Transmit or store excessive personal content.

Consult guidelines and training resources for clarity on what constitutes reasonable limits of personal use.

5.2.2. All users will be issued a unique username/password for access to IT resources. Users must:

a. Be responsible for any and all activities performed under their account;

b. Not divulge their username/password to any other person;

c. Regularly change their password (enforced every 90 days); and

d. Immediately change their password if they think it has been compromised and notify IT Services.

5.2.3. Users are prohibited from using another user's account or sharing credentials and/or systems access with others.

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

5.2.5. Devices are not to be left unattended in a position where unauthorized access could occur. Password protected screensavers on computers and passcode enforced screen locks for mobile devices should be activated if leaving a device unattended.

5.2.6. 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 policy and procedure.

5.3 Unacceptable Use of IT Resources

5.3.1. Users are prohibited from using IT resources for soliciting or conducting non-City work or business for personal gain or profit using City owned technology or resources.

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

a. Copyright material without the owner's express permission;

b. Pornography, substances, alcohol & tobacco, dating, and gambling; and

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

5.3.3. Users shall not use IT resources to send SPAM or unsolicited messages.

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

5.3.5. 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 those of 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 codes of conduct and other policies; and

See City guidelines and Standard Operating Procedures (SOP) on the use of social media for further clarity.

5.4 Use of Digital Assets

5.4.1. 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.

5.4.2. Exceptions to this may include services and social media related to professional affiliations, practices and/or designations which require a work email.

5.4.3. 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 Policy, Privacy Administrative Directive and Records Retention By-law with the relevant licenses, contractual terms and conditions.

5.4.4. 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.

5.4.5. 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.

5.5 Software and Hardware

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

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

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

5.5.4. No unauthorized hardware is to be connected to the internal IT network.

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

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

5.5.7. Users may be held responsible for the costs of repairs or replacement of damaged City-issued equipment in their care as a result of reckless or negligent actions.

5.6 Mobile Devices

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

5.6.2. 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.

5.6.3. Users are permitted to install apps on their 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 Office and IT Department

- Ensure the administration, revision, and interpretation of this Administrative Directive.
- Monitor the use of IT resources to ensure compliance with corporate policies, administrative directives and procedures.
- Establish hardware, software, video and communications technology standards to ensure a secure and reliable information technology and communications environment.
- Provide training opportunities, on a regular basis, for all standardized applications for all user groups.
- Operate a help desk support service for user inquiries on all standard applications.
- All computer equipment installations, modifications, and relocations.

6.2 Managers and Supervisors

- Ensure employees are aware of this Administrative Directive and all underlying procedures, and reporting any contraventions of same.
- Investigate reported contraventions to ensure that there is compliance.
- Ensure that access rights of employees are issued or revoked when changes are required.

6.3 Users

- Read and comply with this Administrative Directive.
- Ensure confidential information is handled appropriately.
- 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 the corporate information technology 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, or illegal use of City property and violation of City policy and procedure.

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 and/or civil prosecution.

8. Definitions

8.1 “Information Assets” means any physical device, software applications, data or documentation within the IT environment.

8.2 “Information Technology resources” means computers, printers, mobile devices (including smartphones and tablets), software, network resources (including Internet, messaging and social media) and telephony (including voicemail).

8.3 “IT environment” refers to the entirety of Information Technology resources.

8.4 “Messaging” means to mobile, texting, email and other on-line texting applications.

8.5 “Personal use” is any use that is not business or work related.

8.6 “Professional affiliations, practices and/or designations” means an organization or a group a person belongs to based on expertise or involvement in a particular profession.

8.7 “Social Media” includes websites and applications that enable users to create and share content or participate in social networking. Some examples include, Facebook, Twitter, Instagram, Snapchat and LinkedIn.

8.8 “Unauthorized Device” means to electronic devices such as laptops or tablets that are not explicitly authorized for use on the City network.

8.9 “Users” means any Employee, Member of Council, Contractor, Consultant, Vendor or Volunteer that have access to and/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 publically available.

External references

- Municipal Freedom of Information and Privacy Act, 1990

References to related bylaws, Council policies, and administrative directives

- 14.18.1 Brampton Open Data
- 13.4.1 Care, Custody and Control of City Assets
- Corporate Fraud Prevention Policy GOV-110
- C006-2016 Council Code of Conduct
- 2.1.0 Employee Code of Conduct
- COM-110 Official Use of Social Media14.8.1 Information Management
- Privacy GOV-130
- Purchasing By-Law 19-2018
- Purchasing Card PUR-120
- 1.3.0 Respectful Workplace

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

- Acquisition of IT Related Applications, Solutions and Hardware
- Expenses – Personal Usage Reimbursement – City Provided Cell Phones
- Personal Use of Social Media by City of Brampton Employees SOP

10. Revision History

Date	Description
2019/10/31	Approved by SLT. To replace 2.11.0 Information Technology Use Policy upon Council resolution
2022/10/31	Next Scheduled Review.