THE CORPORATION OF THE CITY OF VAUGHAN

CORPORATE POLICY

POLICY TITLE: **ACCEPTABLE USE OF INFORMATION TECHNOLOGY**

POLICY NO.: **14.A.01**

Section:	Information Technology		
Effective Date:	March 15, 2018	**Date of Last Review:**	December 18, 2024
Approval Authority: Administration		**Policy Owner:** DCM, Corporate Services, Chief Financial Officer & City Treasurer	

POLICY STATEMENT

Usage of the City of Vaughan's (the "City") Information Technology (IT) resources is a privilege that is extended to City staff, elected officials, volunteers, consultants and contractors. Users of these services and facilities have access to valuable organizational resources, to sensitive and critical data, and to internal and external networks. Consequently, it is important for all Users to act in a responsible, ethical, and legal manner.

PURPOSE

The purpose of the Acceptable Use of Information Technology (the "Policy") is to establish specific requirements to support efficient, cost-effective, and secure use of major IT infrastructure and resources.

In general, acceptable use shall be taken to mean respecting the rights of other digital Users, maintaining the integrity of physical and digital assets, complying with pertinent license and contractual agreements, and where applicable, maintaining compliance with legal and regulatory requirements.

SCOPE

This Policy applies to all City staff, elected officials, volunteers, consultants and contractors.

It does not apply to the members of the public using publicly available Wi-Fi or internet access.

LEGISLATIVE REQUIREMENTS

The protection of personal privacy is one of the key principles of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). The personal privacy requirements, set out in Part II (MFIPPA), deal with privacy protection in the day-to-day operations of institutions.

As an entity engaged in electronic payment processing, the City is also contractually obligated to protect all Cardholder Data in its possession.

DEFINITIONS

1. **Artificial Intelligence (AI):** The theory and development of computer systems capable of performing tasks that typically require human intelligence. AI systems leverage machine learning, deep learning, and other advanced algorithms to simulate human cognitive functions.

2. **Authentication Token:** A physical device that an authorized user is given to ease authentication or to provide multi-factor authentication.

3. **Cardholder Data:** At a minimum, cardholder data consists of the full Primary Account Number (PAN), it may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

4. **City Record:** Any documented Information, regardless of form, that has been created or received as evidence and/or Information by the City in support of legal obligations and/or in the transaction or continuation of City business.

5. **Cloud Storage:** A cloud computing model in which data is stored on remote servers and is made available over the Internet. It is maintained, operated and managed by a cloud storage service provider.

6. **Corporate Computing and Telecommunications Devices:** Any device owned by the City that is used to access, store, process or transmit corporate Information.

7. **Generative Artificial Intelligence (Gen AI):** Artificial intelligence capable of creating content, such as text, images, videos, or software code, in response to a user's prompt or request.

8. **Information:** Information is produced by all processes and it is the values of characteristics in the processes' output that are Information.

9. **Multi-Factor Authentication (MFA):** A security method that requires Users to provide more than one type of identification to verify their identity. This could be

something the user knows (like a Password or PIN), something the user has (like a security token or card), or something the user is (like a fingerprint or other biometric method).

10. **OCIO:** The Office of the Chief Information Officer.

11. **Password:** The individual personal password or security code assigned to the User's user ID, which may be updated by the user from time to time.

12. **Removable Electronic Media:** Any device that can store data in electronic format and can be attached to various electronic devices, examples of removable electronic media include optical discs (Blu-ray discs, DVDs, CDs), memory cards (CompactFlash card, memory stick), zip disks, floppy disks, magnetic tapes, etc.

13. **Shortened URL:** A compact representation of a longer URL (Uniform Resource Locator), which is the web address of a particular webpage or file on the internet.

14. **Teleconference:** Any audio, visual or web conferencing product that are synchronous in nature and support interactions between participants in a meeting or presentation format. Such conferencing consists of real-time content delivery and can include screen and application sharing, text chat, and group document markup with electronic whiteboarding, augmented by audio, data and video.

15. **User(s):** Any individual who uses City Computing and Telecommunications Devices, including but not limited to City elected officials, employees, volunteers, contractors, consultants, and the public.

16. **User ID:** The individual user identification name or code assigned by OCIO.

17. **VPN (Virtual Private Network):** A technology that creates a safe and encrypted connection over a less secure network, such as the internet. It enables remote Users to access corporate resources securely, ensuring that all data transmitted between the user and the network is secure and private.

POLICY

1) CORPORATE COMPUTING AND TELECOMMUNICATIONS DEVICES

a) Acceptable Use

i) Users will ensure that all their actions comply with all applicable laws, regulations, policies and by-laws.

ii) Users will not allow any unauthorized third parties to access the City's network and resources.

iii) Users will take all reasonable steps to protect and keep secure physical, intellectual and Information assets accessed through City Computing and Telecommunications Devices.

iv) Devices that require user authentication, such as PCs, laptops, smartphones, etc. must not be left unlocked or unattended.

v) Users will utilize Computing and Telecommunications Devices for the conduct of the City's business activities and as required by their specific job functions or compliant personal use.

vi) Users will not use or install any software for which they have not been granted the appropriate license or authorization.

vii) Users will not establish remote connections to the City's network from systems without a functioning, up-to-date endpoint protection and operating system.

viii)Users must not use remote access and/or screen-sharing tools not explicitly authorized by OCIO, such as TeamViewer, VNC, etc.

ix) Users must not connect personal devices to any of the City's corporate networks, except for the public Wi-Fi network.

x) Users will not attempt to enter restricted areas of Computing and Telecommunications Facilities, or the computer system(s) of any entity related to or affiliated with the City or perform functions which the User is not authorized to perform.

xi) Port scanning, security scanning, network mapping and network packet capture activities are all expressly prohibited, unless pre-authorized by OCIO.

xii) Users will not copy, destroy, or alter any data, documentation or Information belonging to the City or any other business entity without authorization.

xiii)All City Records should be created, received or stored on a Corporate Computing Device. If a personal device is used, the User must ensure that the requirements specified in this Policy are met.

xiv) Cardholder Data must not be stored on portable storage media, mobile devices, smartphones, shared drives, corporate websites, OneDrive for business or any other storage system.

xv) Users must not save City Records outside of corporate standard storage locations that have not been configured for automated backups. OCIO can be contacted to validate the presence of automated backup for a particular storage location.

xvi) Any changes in ownership of personal computing devices and monitors assigned to Users by OCIO must be immediately reported to IT Service Desk. When no longer required, all personal computing devices and monitors must be returned to OCIO.

xvii) All procured solutions shall be architected, deployed, and configured according to corporate IT security standards.

xviii) All corporate solutions shall be operated according to the IT Systems Security Classification and Protection Standards (PRC.50).

xix) User accounts assigned to specific individuals including accounts with administrative privileges shall not be used for automation, scripting, or any other method of programmatically accessing IT systems. A service account must be created.

xx) Upon retirement, layoff, resignation, or termination of employment contract the User must promptly return (without duplicating or summarizing), all City Records, as well as all electronic devices issued by or paid for by the City, including but not limited to laptops, smartphones, portable hard-drives, memory sticks, etc.

xxi) The City will not provide extracts of user’s personal data stored on any of the Corporate Computing and Telecommunication Devices upon the termination of the employment relationship. Users are solely responsible for backup and maintenance of all personal, non-business-related records.

b) Enforcement and Monitoring

i) OCIO may monitor, audit and report on User activity to ensure compliance to corporate policies as well as in the event of an authorized audit or investigation.

ii) To enforce the Acceptable Use of Information Technology Policy and to protect corporate Information assets, OCIO may deny network access to any device upon detection of unauthorized activity.

iii) Access to various City IT resources will be limited outside of Canada and the United States. A temporary exception can be made upon request to the IT Service Desk, with approval from the employee's functional manager.

iv) Any content stored on the corporate infrastructure or devices found to be in violation of licensing agreements or copyright laws will be removed.

v) The Integrity Commissioner can, at any point and without additional authorization, request any electronic Information processing records, reports, files or property belonging to or used by the City that the Integrity Commissioner believes to be necessary for an inquiry. Information recovery would be managed as per the "Information Recovery" process documented in the "IT Security Operations Manual".

2) DIGITAL IDENTITY

a) Acceptable Use

i) Users designated as administrators of internet facing applications that support multi-factor authentication, must have it enabled.

ii) All Users with remote access to City computing and telecommunications devices, including City's cloud infrastructure, must have multi-factor authentication (MFA) enabled.

iii) Users must not use a User ID not assigned specifically to them by the OCIO.

iv) Users must not share their Passwords or any other Authentication Tokens assigned to them by OCIO with any other person.

v) Users must ensure all Passwords meet corporate standard complexity requirements.

vi) In the event that a User forgets or believes that their Password has become compromised, the User must inform IT Service Desk immediately.

b) Enforcement and Monitoring

i) OCIO may suspend a User's access to City computing and telecommunications devices by deactivating or deleting account(s) if unauthorized or suspicious activity is detected.

ii) OCIO may suspend or limit a User's access to City computing and telecommunications devices if multi-factor authentication (MFA) is not enabled.

3) MOBILE DEVICES

a) Acceptable Use

i) Users of a corporate mobile device are responsible for ensuring adequate physical security of the device.

ii) Confidential corporate data must not be stored in the unencrypted form on any non-corporate mobile device or smartphone.

iii) Users must not subvert any corporate device’s security controls deployed by OCIO via hacks, jailbreaks, software changes and/or security setting alterations.

iv) Users must regularly install updates deployed by OCIO, device manufacturers or software vendors.

v) Users must report lost or stolen devices immediately to the IT Service Desk.

vi) Users must not host open (non-Password-protected) Wi-Fi hotspots on corporate mobile devices.

vii) City Records should only be processed and stored on Corporate Computing Devices. If a personal device is used temporarily for City business (unless otherwise sanctioned by OCIO), the User shall ensure that the following requirements are met:

(1) Documented business need exists.

(2) Up-to-date and functioning endpoint protection is installed.

(3) Operating system is up-to-date.

(4) Storage encryption is deployed.

(5) Password protection is deployed.

viii) Users must ensure that any City Records created or modified on a non-City device are transferred to an appropriate corporate system as soon as possible and removed from personal devices.

ix) Users shall not install any smartphone applications from unauthorized sources. An up-to-date list of authorized mobile application sources will be maintained by OCIO as a part of “IT Security Standards” document.

b) Personal Use

i) Limited and reasonable personal use of corporate mobile devices is allowed and is limited to the following parameters, and shall not:

(1) Have a negative impact on User productivity or efficiency.

(2) Interfere with City business operations.

(3) Exceed reasonable time limits or duration.

(4) Cause expense in the form of storage, financial or network overhead to the City.

(5) Compromise the integrity and security of the City’s resources or assets.

(6) Violate any policies, procedures, by-laws, regulations or laws.

c) Enforcement and Monitoring

i) All corporate mobile devices will be centrally managed and controlled by OCIO via the mobile device management system.

ii) Devices found to be in violation of corporate security standards or this Policy may be remotely disabled, wiped or disconnected from various corporate services including the City’s internal network.

4) REMOVABLE ELECTRONIC MEDIA AND CLOUD STORAGE

a) Acceptable Use

i) Users must consider all legislative and regulatory requirements, policies guidelines, and by-laws prior to placing corporate data on Removable Electronic Media or Cloud Storage.

ii) Users must not copy personally identifiable, sensitive or confidential data to Removable Electronic Media unless absolutely necessary. If it cannot be avoided the data must be protected with the corporate standard encryption, available to all users of corporate standard PCs and laptops. Once corporate Information is placed on a storage device it must not be used for personal data storage.

iii) All owners of Removable Electronic Media must employ reasonable physical security measures to prevent loss and theft.

iv) Users must permanently erase (simple delete does not qualify) all corporate data when the Removable Electronic Media is no longer required. Alternatively, Users can deliver the device to IT Service Desk for proper disposal.

v) Use of corporate Cloud Storage is only allowed for conducting City business activities and as required by a User’s specific job functions.

vi) Corporate Cloud Storage must only be accessed from systems that are Password protected, have an up-to-date endpoint protection and operating system (all Corporate Computing and Telecommunications Devices automatically qualify).

vii) Users shall not configure synchronization of corporate Cloud Storage to non-corporate devices.

viii)Corporate information must not be shared with the “public” or “everyone” using Cloud Storage; specific people or groups must be used.

ix) Microsoft OneDrive when accessed using corporate (@vaughan.ca) account is currently the only authorized secure Cloud Storage provider suitable for corporate Information storage. Users shall not copy corporate data to any of the other third-party Cloud Storage providers (e.g., Google Drive, Dropbox, Amazon Cloud Drive, etc.).

x) Users are responsible for managing permissions of their corporate Cloud Storage to ensure security of corporate data.

xi) Users must consider sensitivity of Information being placed on corporate Cloud Storage and, if required, protect it with encryption. An up-to-date list of corporate tools authorized for secure file encryption will be maintained by OCIO as a part of IT Security Standards.

xii) Users must only use systems authorized for secure Information exchange when sharing personally identifiable or sensitive Information with other organizations. An up-to-date list of corporate systems authorized for secure information exchange will be maintained by OCIO as a part of IT Security Standards.

xiii) All corporate Removable Electronic Media must be returned to the City upon termination of employment relationship.

b) Enforcement and Monitoring

i) OCIO may restrict the use of USB connectivity on any client PCs that it deems to be particularly sensitive. OCIO also may disable this feature on PCs used by Users in specific roles.

ii) OCIO may, through policy enforcement and any other technical means, limit the ability of Users to transfer data to and from specific resources on the corporate network.

iii) In specific situations, OCIO may establish audit trails to track the attachment and utilization of external storage devices.

iv) OCIO may monitor, audit and report on activities and Information being accessed, stored and transmitted to and from Cloud Storage to ensure compliance with corporate policies.

5) INTERNET

a) Acceptable Use

i) Users of City corporate internet may use the internet only to complete their job duties, under the purview of the City’s business objectives.

Permissible, acceptable, and appropriate internet-related work activities include:

(1) Researching, accumulating, and disseminating any Information related to the accomplishment of the User’s assigned responsibilities.

(2) Collaborating and communicating with other Users, business partners, and customers of the City, according to the Users’ assigned job duties and responsibilities.

(3) Conducting professional development activities (e.g., news groups, chat sessions, discussion groups, posting to bulletin boards,web seminars, etc.) as they relate to meeting the Users’ job requirements. In instances where the personal opinions of the User are expressed,

a disclaimer must be included asserting that such opinions are not necessarily those of the City.

ii) Users shall not download files from the internet unless their use is required for the purposes of conducting City business or compliant personal use.

iii) Users shall not engage in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.

b) Personal Use

i) Limited and reasonable personal use of internet access is defined as any personally conducted online activity or internet usage for purposes other than those listed in this Policy. Personal use is limited to the following parameters, and shall not:

(1) Have a negative impact on User productivity or efficiency.

(2) Interfere with City business operations.

(3) Exceed reasonable time limits or duration.

(4) Cause expense or network overhead to the City.

(5) Compromise the integrity and security of the City’s resources or assets.

(6) Violate any policies, procedures, by-laws, regulations or laws.

c) Enforcement and Monitoring

i) OCIO may monitor and log internet traffic for the purpose of enforcing acceptable use policies and may block access to certain websites for which access is deemed to be a contravention of corporate policies.

6) EMAIL

a) Acceptable Use

i) All City business email communications must be conducted through @vaughan.ca email accounts.

ii) Email communication with external organizations is not considered a secure method of Information exchange. An updated list of corporate systems currently authorized for secure Information exchange will be maintained by OCIO as part of the IT Security Standards.

iii) Users' email communications must be conducted professionally and meet all requirements set forth in the City's Employee Code of Conduct Policy (13.A.02).

iv) Users are responsible for managing their corporate mailbox permissions to ensure security of corporate data.

v) Prior to opening any attachments or links included in email, Users must inspect the email contents for the following risk indicators:

(1) Poor formatting, spelling and grammatical mistakes.

(2) [External] tag in the subject line and "CAUTION!" banner in the email body.

(3) Sender who does not typically send such emails.

(4) Generic greetings.

(5) Request for personal, confidential or sensitive Information.

(6) Marked as High Urgency.

(7) Lack of appropriate corporate branding in the email or linked webpages.

(8) Presence of Shortened URL's.

(9) URL's where the displayed text differs from the URL shown when hovered over.

vi) Emails exhibiting several risk indicators must be submitted to IT Service Desk and deleted immediately.

vii) The City will not provide extracts of Users' personal data stored in corporate email system upon termination of the employment relationship. The User is solely responsible for backup and maintenance of all personal records not related to any corporate business activities.

b) Enforcement and Monitoring

i) OCIO may monitor, audit and report on Users email activity and Information being sent or received using corporate email system to ensure compliance with corporate security and privacy obligations.

ii) OCIO may periodically conduct simulated email phishing campaigns as part of the security awareness training program. User responses including clicking links, downloading files, or providing credentials will be captured for overall security posture and risk evaluation purposes. Additionally, follow-up security awareness training may be mandated.

7) TELECONFERENCING

a) Acceptable Use

i) The corporate standard teleconferencing solution is Microsoft Teams (MS Teams). Any other system might not include industry standard security and privacy controls or possess necessary meeting controls to prevent misuse and will not be supported by OCIO.

ii) While conducting teleconferencing sessions with any corporate standard teleconferencing or other solution, Users must employ appropriate risk mitigation controls, including but not limited to:

(1) Enable Password protection for meetings when appropriate.

(2) Provide links only to specific people and avoid advertising on social media or other publicly available forums, unless absolutely necessary.

(3) Ensure screen sharing and file sharing permissions are managed to prevent any unauthorized person(s) from access or viewing content.

(4) Always use the latest version of the teleconferencing client.

(5) Only share Teleconference access details (such as PINs or meeting links) with authorized individuals.

iii) The recording of a Teleconference meeting or the use of the automated transcription function in a Teleconference meeting is generally not permitted. In certain circumstances, these functions may be permitted on a case-by-case basis, only if prior written approval is provided at the Director level.

iv) Recording or automatically transcribing a Teleconference meeting will only be approved by a Director including the following circumstances:

(1) Virtual training and/or staff information sessions.

(2) Community workshops.

(3) Townhalls.

(4) Focus group sessions.

v) The Office of the City Clerk shall be solely responsible for recording and transcribing (as deemed necessary) all meetings of Council, Committee of Council, Statutory Public Meetings, and all public meetings of Council appointed Committees (such as Task Force Meetings).

vi) A City employee who has been granted approval to record and transcribe meetings shall abide by the terms set out in this Policy and the related Teleconference Meeting Recording/Automated Transcript Terms of Use, including the requirement for Notice and Consent to those in attendance.

vii) If a User would like to record or automatically transcribe a Teleconference meeting, a request to the IT Service Desk copying the user’s Director must be submitted.

viii)A request to record or automatically transcribe a Teleconference meeting must be made at least three business days prior to the Teleconference meeting (as outlined in the Microsoft Teams Records and Transcription Terms of Use).

ix) Most of the recordings or transcriptions created and maintained using MS Teams should be deemed Transitory Records (non-official records) that are required only for a limited period of time, in order to prepare subsequent records (i.e. Meeting minutes or training records).

x) Once a subsequent draft or final Official Record is effectively documented and approved by the responsible unit, the Transitory audio and/or video recording can be disposed of in accordance with the associated Terms of Use.

xi) Any MS Teams audio and/or video recordings that are not used to prepare a subsequent record are deemed to be the Official Record and subject to the relevant legislated and Enterprise Information

Management Policy (03.A.15) requirements.

8) ALTERNATIVE WORK ARRANGEMENTS

a) Acceptable Use

i) Users must not connect any Removable Electronic Media or computing devices to corporate PCs, laptops or smartphones, unless explicitly authorized by OCIO.

ii) Users must not use Virtual Private Network (VPN) services not explicitly authorized by OCIO, such as Express VPN, IPVanish, NordVPN, etc. while using any corporate services such as Cloud Storage, productivity applications, email, etc.

iii) Users must ensure that any home wireless being used is Password protected and that any default wireless router Passwords have been changed.

iv) Configuration that includes any personal devices will not be assessed or supported. Upon engaging IT Service Desk to troubleshoot any problems, Users will be asked to remove any personal devices that might be affecting application or service.

v) Any printing required should be done at the User's designated City building workspace. Personal peripheral device (e.g., printer) that are connected to City laptops will not be supported by OCIO.

vi) Corporate Passwords must not be used for personal accounts (i.e., banking, personal email, social media) and vice versa; personal Passwords should not be used for corporate accounts.

9) ARTIFICIAL INTELLIGENCE

a) Acceptable Use

i) Users must only utilize approved corporate standard AI tools for business purposes.

ii) Users must only utilize approved corporate standard AI tools on Corporate Computing and Telecommunications Devices.

iii) Users must be logged in with their corporate-issued User ID at all times when using approved corporate standard AI tools.

iv) Users must not paste or input sensitive, confidential or personally identifiable Information into non-corporate standard AI tools.

v) Users must appropriately screen, review, and fact check all content generated by any AI tool prior to using it for business purposes, as the AI output might contain mistakes, give inaccurate or outdated Information, or generate inappropriate or offensive content.

vi) Use of AI tools by external parties to record, transcribe, summarize, or otherwise interact with City staff during virtual or in-person meetings is generally not permitted. In certain circumstances, these functions may be permitted on a case-by-case basis, only if prior written approval is provided at the Director level.

10) SANCTIONS AND VIOLATIONS

a) Any Users found to have breached this Policy may be subject to disciplinary action.

b) Any violation of the Policy by a temporary worker, consultant or supplier may result in the termination of the contract or assignment.

c) Any violation of this Policy will be considered a breach of the City's Employee Code of Conduct (13.A.02) or Code of Ethical Conduct for Members of Council (CL-011), as applicable.

11) EXCEPTIONS MANAGEMENT

a) All exceptions must be managed as per IT policy exceptions management standards.

ADMINISTRATION

Administered by the Office of the City Clerk.

Review Schedule:	3 Years	**Next Review Date:**	December 18, 2027
Related Policy(ies):	13.A.02 – Employee Code of Conduct, CL-011 – Code of Ethical Conduct for Members of Council, 03.A.15 – Enterprise Information Management		
Related By-Law(s):	046-2017 – Records Retention By-Law		
Procedural Document:	PRC.01 – IT Security Standards, PRC.50 – IT Systems Security Classification and Protection Standards		

Revision History	
Date:	**Description:**
28-Nov-19	Administrative updates approved at Policy Committee.
30-Jul-20	Administrative updates approved at Policy Committee.
23-Jan-23	Administrative updates approved at Policy Committee.
18-Dec-24	Administrative updates approved at Policy Committee.