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:**	July 22, 2020
Approval Authority: Administration		**Policy Owner:** DCM, Corporate Services & CFO	

POLICY STATEMENT

The computing, digital technology, and digital information resources at the City of Vaughan support the following organization's service excellence objective: To ensure citizens receive the best experience in person, by telephone and electronically, the City will provide exceptional end-to-end citizen-centred services, enhance access and streamline services with the use of technology. Usage of these resources is a privilege that is extended to employees, elected officials, volunteers, consultants and contractors. As users of these services and facilities, they 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 this policy is to establish specific requirements to support efficient, cost-effective and secure use of major information technology (IT) infrastructure and resources.

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

SCOPE

This policy applies to all City of Vaughan 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. **Authentication Token:** A physical device that an authorized user is given to ease authentication or to provide multi-factor authentication.

2. **Business Record:** Any recorded information, whether in printed form, on film, by electronic means or otherwise, created or received by the City of Vaughan in the conduct of business, including electronic messaging applications capable of producing a record.

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. **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.

5. **Computing and Telecommunications Facilities:** Any device owned by the City that is used to access, store, process or transmit information, including but not limited to personal computers, intelligent terminals, kiosks, network, servers, applications, telephones, cellular phones, pagers, radios, smartphones, geographic positioning devices, or other similar devices.

6. **Corporate Computing Devices:** Any computing device that was procured, configured or is being managed by OCIO.

7. **Information:** Any electronically stored content, including but not limited to data, records, documents, files, logs, images, audio and video.

8. **Mobile Device:** A portable computing device such as a smartphone, tablet computer or laptop.

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

10. **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.

11. **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.

12. **Personal Computing Devices:** Any electronic equipment controlled by a CPU, including desktop and laptop computers, smartphones and tablets.

13. **User:** Any individual who uses City computing and telecommunications facilities, including but not limited to City elected officials, employees, volunteers, contractors, consultants and the public.

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

POLICY

1. Computing and Telecommunications Facilities

1.1. Acceptable Use

1.1.1. Users shall not copy, destroy or alter any data, documentation, or other information that belongs to the City of Vaughan or any other business entity without authorization.

1.1.2. Users shall not allow any unauthorized third parties to access the City of Vaughan's network and resources.

1.1.3. Users will take all reasonable steps to protect and keep secure physical, intellectual and information assets accessed through City computing and telecommunications facilities.

1.1.4. The user will utilize City computing and telecommunications facilities for the conduct of the City's business activities and as required by their specific job functions or compliant personal use.

1.1.5. The users must not use or install any personal software or software for which the user has not been granted the appropriate license.

1.1.6. The user 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 pursuant to this policy.

1.1.7. Upon retirement, layoff, resignation or termination of employment contract the users must promptly return (without duplicating or summarizing), any and all electronic records pertaining to the City of Vaughan's business as well as all electronic devices issued by or paid for by the City of Vaughan, including but not limited to laptops, smartphones, portable hard-drives, memory sticks, etc.

1.1.8. Devices that require user authentication, such as PCs, laptops, smartphones, etc. must not be left in the unlocked state unattended.

1.1.9. Users shall ensure that all their actions are in compliance with all applicable laws, regulations, policies and by-laws.

1.1.10. Users shall not establish remote connections to City of Vaughan's network from systems without a functioning, up-to-date antivirus and operating system.

1.1.11. All City business records, if located, created or received outside of the Corporate systems shall be transferred to the appropriate Corporate system as soon as possible after creation or receipt (please note that documents received during the course of business from external sources are also considered official City business records).

1.1.12. The City of Vaughan will not provide extracts of user's personal data stored on any of the corporate computing and telecommunication facilities upon the termination of the employment relationship. Users are solely responsible for backup and maintenance of all personal, non-business-related records.

1.1.13. Users should avoid saving business critical data to local drives on their personal computer as this data will not be automatically backed up and might be lost due to hardware or software failure. File storage that includes automatic backups are personal or corporate shared drives (H:\ and O:\) and internal corporate SharePoint website.

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

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

1.1.16. 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.

1.1.17. 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.

1.2. Enforcement and Monitoring

1.2.1. 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.

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

1.2.3. To enforce the Acceptable Use of Information Technology policy and to protect corporate information assets, the OCIO may deny network access to any wireless device upon detection of unauthorized activity.

1.2.4. The Integrity Commissioner can, at any point and without additional authorization, request any electronic data processing records, reports, files or property belonging to or used by the City of Vaughan 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

2.1. Acceptable Use

2.1.1. In the event that a City of Vaughan infrastructure user forgets or believes that their password has become compromised, the user must inform Office of the Chief Information Officer (OCIO) Service Desk immediately.

2.1.2. Users must not use a user ID not assigned specifically to them by the OCIO.

2.1.3. Users must not share their passwords or any other authentication tokens assigned to them by OCIO with any other person.

2.2. Enforcement and Monitoring

2.2.1. OCIO may suspend user's access to City computing and telecommunications facilities by deactivating account(s) if unauthorized or suspicious activity is detected.

3. Mobile Devices

3.1. Acceptable Use

3.1.1. Users of a corporate mobile device is responsible for ensuring adequate physical security of the device.

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

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

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

3.1.5. Users must report lost or stolen devices immediately to the OCIO Service Desk.

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

3.1.7. Users shall ensure that the following criteria are met prior to placing any corporate data on a non-corporate personal computing device:

3.1.7.1. Business need must exist.
3.1.7.2. Up-to-date and functioning antivirus must be deployed.
3.1.7.3. Operating system must be up-to-date.
3.1.7.4. Storage encryption must be deployed.
3.1.7.5. Password protection must be deployed.

3.1.8. User 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.

3.1.9. The City of Vaughan will not provide extracts of a user's personal data stored on corporate mobile devices, including files, e-mails, contacts, notes, pictures, etc. upon termination of the employment relationship. User is solely responsible for backup and maintenance of all personal, non-business-related records.

3.2. Personal Use

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

3.2.1.1. Have a negative impact on user productivity or efficiency.
3.2.1.2. Interfere with normal business operations.
3.2.1.3. Exceed reasonable time limits or duration.
3.2.1.4. Cause expense in the form of storage, financial or network overhead to the City of Vaughan.
3.2.1.5. Compromise the integrity and security of the City of Vaughan's resources or assets.
3.2.1.6. Violate any policies, procedures, by-laws, regulations or laws.

3.3. Enforcement and Monitoring

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

3.3.2. Devices found to be in violation of corporate security standards or this acceptable use policy may be remotely disabled, wiped or disconnected from various corporate services including the City of Vaughan's internal network.

4. Removable Electronic Media and Cloud Storage

4.1. Acceptable Use

4.1.1. Users must not copy personally identifiable, sensitive or confidential data to portable electronic media unless absolutely necessary. If it cannot be avoided the data must be protected with the corporate standard Microsoft BitLocker 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.

4.1.2. All owners of removable electronic media must employ reasonable physical security measures to prevent loss and theft.

4.1.3. When removable electronic media device is no longer required users must permanently erase (simple delete does not qualify) all corporate data prior to disposal. Alternatively, users can deliver the device to OCIO Service Desk for proper disposal.

4.1.4. All corporate removable electronic media must be returned to the City of Vaughan upon termination of employment relationship.

4.1.5. Corporate cloud storage must only be accessed from systems that are password protected, have an up-to-date antivirus and operating system (all corporate assets automatically qualify).

4.1.6. Users shall not configure synchronization of corporate cloud storage to non-corporate devices.

4.1.7. Corporate information must not be shared with “public” or “everyone” using cloud storage; specific people or groups must be used.

4.1.8. 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.).

4.1.9. Use of corporate cloud storage is only allowed for conducting City business activities and as required by user’s specific job functions.

4.1.10. Users are responsible for managing permissions of their corporate cloud storage to ensure security of corporate data.

4.1.11. 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 document.

4.1.12. 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 document.

4.1.13. 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.

4.2. Enforcement and Monitoring

4.2.1. 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.

4.2.2. 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.

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

4.2.4. 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

5.1. Acceptable Use

5.1.1. Users of the City of Vaughan corporate Internet may use the Internet only to complete their job duties, under the purview of the City of Vaughan's business objectives. Permissible, acceptable, and appropriate Internet-related work activities include:

5.1.1.1. Researching, accumulating, and disseminating any information related to the accomplishment of the users assigned responsibilities.

5.1.1.2. Collaborating and communicating with other users, business partners, and customers of the City of Vaughan, according to the users assigned job duties and responsibilities.

5.1.1.3. 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 of Vaughan.

5.1.2. Users shall not download files from the Internet unless their use is required for the purposes of conducting City of Vaughan business or compliant personal use.

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

5.2. Personal Use

5.2.1. 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 s.5.1. of this policy. Personal use is limited to the following parameters and shall not:

5.2.1.1. Have a negative impact on user productivity or efficiency.
5.2.1.2. Interfere with normal business operations.
5.2.1.3. Exceed reasonable time limits or duration.
5.2.1.4. Cause expense or network overhead to the City of Vaughan.
5.2.1.5. Compromise the integrity and security of the City of Vaughan's resources or assets.
5.2.1.6. Violate any policies, procedures, by-laws, regulations or laws.

5.3. Enforcement and Monitoring

5.3.1. 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. E-Mail

6.1. Acceptable Use

6.1.1. All City of Vaughan's business e-mail communication must be conducted through @vaughan.ca e-mail accounts.

6.1.2. 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 a part of IT Security Standards document.

6.1.3. Users e-mail communications must be conducted professionally and meet all requirements set forth in the City of Vaughan's Employee Code of Conduct policy (13.A.02).

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

6.1.5. The City of Vaughan will not provide extracts of users personal data stored in the corporate e-mail system upon termination of the employment relationship. User is solely responsible for backup and maintenance of all personal records not related to any corporate business activities.

6.1.6. Prior to opening any attachments or opening links included in emails, users must inspect the email contents for the following risk indicators:

- Poor formatting, spelling and grammar mistakes
- [External] mark in the subject line
- Sender who does not typically send such emails
- Generic greetings
- Requesting personal or confidential information
- High urgency
- Lack of appropriate corporate branding in the email or in linked webpages

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

6.2. Enforcement and Monitoring

6.2.1. OCIO may monitor, audit and report on users e-mail activity and information being sent or received using corporate e-mail system to ensure compliance with corporate security and privacy obligations.

6.2.2. 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

7.1. Acceptable Use

7.1.1. Corporate standard teleconferencing solutions include Microsoft Skype for Business and Microsoft 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.

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

7.1.2.1. Enable password protection for meetings when appropriate;
7.1.2.2. Provide links only to specific people and avoid advertising on social media or other publicly available forums, unless absolutely necessary;
7.1.2.3. Ensure screen sharing and file sharing permissions are managed to prevent any unauthorized person(s) from access or viewing content; and,

7.1.2.4. Always use the latest version of the teleconferencing client.

8. Working from Home

8.1. Acceptable Use

8.1.1. Users must not plug-in or connect any personal electronic devices, which were not explicitly authorized by OCIO, to corporate PCs, laptops, smartphones, networks. This includes personal printers, hard drives, USB keys, cameras, microphones, computers, etc.

8.1.2. 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 IT services such as cloud storage, productivity applications, email, etc.

8.1.3. Users must ensure that any home wireless being used is password protected and that any default wireless router passwords have been changed.

8.1.4. 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.

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

8.1.6. 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. Sanctions and Violations

9.1. Any users found to have breached this policy, may be subject to disciplinary action.

9.2. Any violation of the policy by a temporary worker, consultant or supplier may result in the termination of the contract or assignment.

9.3. Any violation of this policy will be considered a breach of the City's Code of Conduct or Code of Ethical Conduct, as applicable.

10. Exceptions Management

10.1. 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 If other, specify here	**Next Review Date:**	March 15, 2025
Related Policy(ies):	13.A.02 – Employee Code of Conduct, CL-011 – Code of Ethical Conduct for Members of Council		
Related By-Law(s):			
Procedural Document:	PRC.01 – IT Security Standards		

Revision History	
Date:	**Description:**
28-Nov-19	Administrative update
22-Jul-20	Contextual update
Click or tap to enter a date.	