Acceptable Use Policy for Cogeco's Information Technology Assets

DOCUMENT CLASSIFICATION	Internal Use
VERSION	3.0
PUBLICATION DATE	December 13, 2024
DOCUMENT OWNER	Information Security
REVIEW FREQUENCY	Annually, or as needed

Contents

Policy Summary

Purpose and Scope

This policy outlines how Cogeco's IT assets should be used by End-users (Employees, contractors and Third Parties) to protect the company's information and maintain operational integrity. It applies to all users of Cogeco's IT systems.

Key Responsibilities

Access Control and Physical Security

- Protect your devices and credentials; never share or store them insecurely.
- Use strong, unique passwords and enterprise-approved credential managers.
- Use privileged accounts only for intended purposes.
- Return all Cogeco equipment upon ending employment or agreement.
- Report lost and stolen Cogeco devices to IT Colleagues Services Team immediately.

Data Handling

- Handle sensitive data securely; use encryption for electronic transmissions.
- Do not share sensitive information externally without proper agreements.
- Personal storage devices are not authorized unless specifically approved (e.g., USB drives).
- Store and destroy sensitive physical documents securely.

Videoconferencing, Electronic Messaging & Internet Use

- Use Cogeco-provided email and messaging tools for work-related communication and videoconferencing.
- Be cautious of phishing attempts and report suspicious messages.
- Limit personal use of Cogeco devices and do not access inappropriate or illegal content.
- Obtain consent before recording a meeting and do not share Sensitive Data on the screen.

Device Usage

- Cogeco devices are for business use only. Do not share them or connect to unsecured networks.
- Enable security features like Virtual Private Network (VPN) and software updates.
- Follow guidelines for working remotely or traveling with devices.

Bring Your Own Device (BYOD)

- Secure personal devices used for work with strong passwords, encryption, and use Mobile Device Management (MDM) software for mobile devices.
- Cogeco reserves the right to access and wipe company data if needed.

Social Media and AI Tools

- Only authorized representatives may post on Cogeco's behalf.
- Use generative AI tools only if approved by Cogeco; do not share Sensitive Data.

Incident Reporting

- Report security incidents or suspicious activities to the IT Colleague Services Team immediately.
- Follow instructions from InfoSec and IT during security incidents.

Compliance

- Adhere to legal requirements, Cogeco policies, and ethical standards.
- Do not use unlicensed software, pirated content, or unauthorized cloud services.

Monitoring and Enforcement

- Cogeco may monitor the use of IT systems to ensure compliance. Non-compliance can cause disciplinary actions, including termination.

For full details, read the complete Acceptable Use Policy below.

---

1. Introduction

Cogeco takes the subject of information security very seriously. The purpose of this document is to outline the acceptable use of information technology assets at Cogeco and give guidance to End Users, including Employees and Third Parties, regarding the appropriate usage of hardware, software and applications. We have a duty to protect and maintain the integrity of the information that we collect and use for the benefit of the organization and its customers.

2. Scope

This policy applies to all End-users of Cogeco's systems and processes that constitute the organization's information systems.

3. General

Please refer to key definitions in the Glossary section.

End-users are expected to become familiar and follow Cogeco's security policies and standards relating to your work.

If some actions are not referred to in this policy, it does not make them permitted by default. If there is any uncertainty, End-users should consult their reporting manager, IT or the InfoSec Governance, Risk and Compliance (GRC) team.

Cogeco proprietary information stored on Computing Devices, whether owned or leased by Cogeco, an End-user or a Third Party, remains the sole property of Cogeco.

4. Access control

End-users are responsible for the following:

- Protect their own user credentials (user account and password, access token or other items you may be provided with) by taking the following actions:
    - Do not share your user credentials with others and do not store them in cleartext on any device including any Cogeco Device.
    - Use enterprise approved credential management solutions to manage user credentials for Cogeco systems and solutions. This can be obtained by submitting a request via the IT Service Management tool (i.e. ServiceNow).
    - Do not use the same password (or close variation of the same password) for multiple user accounts.
    - Do not use privileged user accounts (user accounts with higher-than-normal system access) for business-as-usual activities. An End-user with privileged accesses (e.g. local admins or administrator access to systems) must be diligent and use it for its intended business purpose, otherwise privilege may be revoked.
    - Never attempt to bypass or subvert system security controls or to use them for any purpose other than that intended. Access control (e.g., password, PIN or biometric) verification must be set and used on a Computing Device that accesses Cogeco Data.
- Return all Cogeco equipment (e.g. workstations, mobile phones and removable devices) to the IT Colleague Services Team upon resignation or termination of employment, or, in the case of a Third Party, when your agreement with Cogeco ends.
- In the case of a Third Party, under a Third Party Access and Confidentiality Agreement (TPACA), ensure that the Third Party access is limited to systems and data covered in the agreement, following Cogeco's Third Party Security Standard.

5. Physical security

- When entering Cogeco premises, the End-user must:
  - have a Cogeco access card;
  - ensure they are not followed through access controlled doors and that these doors close properly after them;
  - escort visitors at all times when entering restricted areas, where it is required to perform a scan of access card;
- not copy, share or lend their access cards;
- Direct physical access to server rooms must be restricted. All accesses to restricted areas must be logged and monitored. Logs must be made available for review.
- End-users must lock their workstations when it will be unattended for any amount of time.
- Remember that they are responsible for the security of their Cogeco Device and Cogeco access card. End-Users should always know where their Cogeco Device and Cogeco access card are and should not leave them unattended in areas they do not control (e.g. public place, parked car, etc.).
- In the event of theft of company-owned equipment, End-users should report the theft to the police and have the police report on hand when reporting it to the IT Colleague Services Team.
- In case of loss of company-owned equipment, report it immediately to the IT Colleague Services Team.

6. Data handling

End-users are responsible for the following:

- Read the Information Classification Schema, which defines Sensitive Data.
- Always protect any Sensitive Data (as identified in the Information Classification Schema) that is sent, received, stored or processed and independently of whether the data is in electronic or paper format, or exchanged verbally.
- Do not send Sensitive Data over the Internet via email or other methods unless appropriate mechanisms (for example encryption) have been used to protect it (see User guide on sending encrypted files).
- The transmission and sharing of any Sensitive Data is subject to data protection controls.
- Not sharing Sensitive Data outside of Cogeco without an agreement in place governing confidentiality (at a minimum a Non-Disclosure Agreement (NDA) or Third Party Access and Confidentiality Agreement (TPACA) or after consulting with the Legal department. Using a Cogeco shared drive with limited access is preferred.
- Exercise caution and double check the recipient of the Sensitive Data. For example, always ensure that the correct email address(es) is entered so that Sensitive Data is not compromised.
- Securely store printed materials containing Sensitive Data and ensure it is securely destroyed when no longer needed (using confidential waste bins or shredders).
- Not using portable mass storage media such as USB drives, which are blocked for security reasons. Exceptions must be requested.
- Return all Cogeco electronic storage devices and physical media to the IT Colleague Services Team at the end of their useful life for proper decommissioning or secure disposal.
- Avoid using a Cogeco Device to store End-User's Personal Information (such as personal emails, ID details, pictures of friends and family). It is the End-User responsibility to regularly check their Cogeco Device to delete any Personal Information that may have been saved.
- Ensure to not leave any documents that include Sensitive Data in a meeting room, a public space, a computer desk or available on a computer screen.

7. Videoconferencing

The End-user should only organize video conferences with their corporate account and company's authorized platforms. It is important for meeting organizers to control screen and file sharing to ensure only trusted sources have the capability to share.

When the meeting starts, the organizer must verify the list of participants connected and remind the participants of the following security rules:

- No recording of the meeting without consent from all participants.
- Only documents authorized by the organizer can be shared and used.
- No Sensitive Data can be shared if a Third Party participant (e.g. supplier or vendor) has not signed a confidentiality agreement (TPACA or NDA).
- Personal Information can never be shared during a video conference.

8. Electronic messaging

Electronic messaging covers email and various forms of instant messaging such as SMS texts, messaging apps, web chats and messaging facilities within social media platforms.

End-users must ensure that:

- They always use organization-provided electronic messaging tools and Cogeco email accounts when communicating with others in their work capacity.
- Cogeco's communication systems must be used for business purposes only and with Cogeco-approved Devices.
- They never use personal email accounts to send or receive electronic messages in their work capacity.
- They take steps to validate the legitimacy of electronic message links before clicking on them, since many security breaches occur due to phishing (where an email or other type of message is sent which either has a malicious attachment or includes links to websites which are set up to steal information).
- They report any phishing or other suspicious activity as described in Section 17.
- They follow the Social engineering guides on tips and tricks.
- Messages they send do not contain material which is defamatory, obscene, does not follow the Cogeco's Code of Ethics or the Harassment, Discrimination and Violence-Free Workplace policy or which a recipient might otherwise reasonably consider inappropriate. In particular, organization electronic messaging facilities must not be used:
    - for the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organizations
    - for activities that corrupt or destroy other users' data or disrupt the work of others
    - to distribute any offensive indecent images, data, or other material
    - to transmit material that either discriminates or encourages discrimination
    - for activities that violate the privacy of other users
    - send anonymous messages - i.e. without clear sender identification.

9. Internet browsing

Internet access on Cogeco Devices is primarily provided for tasks related to Cogeco work such as access to information and systems that is pertinent to operating Cogeco's business and consistent with an End-User role and responsibilities.

Cogeco recognizes that End-users may occasionally need to use their workstations for personal tasks, such as pursuing educational opportunities or managing limited personal matters. While a certain level of personal use is tolerated on Cogeco Devices, it should be kept to a minimum and should not interfere with the End-user's job responsibilities or the Cogeco's network performance. End-users are expected to exercise good judgment and discretion when using their workstations for personal activities during work hours and should not use their Cogeco Device as a storage for personal files.

Cogeco Devices must not be used for personal endeavors such as conducting a separate personal business as per the Code of Ethics. Engaging in inappropriate or excessive personal use, such as accessing explicit content or participating in illegal activities, is strictly prohibited and may cause disciplinary action, up to and including termination of employment.

Unless a specific exception is granted by InfoSec, End-users must not use the Internet access provided by Cogeco to knowingly create, download, upload, display or access data, images, audio files or video files the transmission of which is illegal or any other material that is against the rule, essence and spirit of this and other organizational policies. This includes, but is not limited to :

- creating, downloading, uploading, displaying or accessing knowingly, sites that contain pornography or other inappropriate material that might be deemed illegal, obscene or offensive;
- subscribing to, entering or using peer-to-peer networks or installing software that allows the sharing of music, video or image files;
- subscribing to, entering or using online gaming, betting sites, “money making” sites/programs;
- downloading any unapproved and/or insecure software (Shadow IT);
- running any insecure program/script/command with the intent to interfere or gain unauthorized access to systems;
- altering any information on Cogeco publicly facing web assets;
- misrepresenting, obscuring, suppressing, or replacing their own or other End-users’ information or identities on the Internet or on any of Cogeco’s information systems.

Internet browsing creates risk for Cogeco and the Cogeco network and End-users must be vigilant at all times and avoid knowingly or inadvertently accessing malicious sites. Websites that are flagged by anti-malware or browser software as being potentially unsafe, or which appear otherwise suspicious should not be accessed. This includes Internet browsing in a remote location (i.e. home), since the compromise of any connected device on the same remote network may endanger the Cogeco Device.

10. Cogeco Devices

End-users are responsible for exercising reasonable due diligence regarding the appropriate use of Cogeco Devices, also referred as User Endpoint Devices. Cogeco Devices include items such as laptops, notebooks, tablet devices and mobile phones.

Here is what End-users need to take care of:

- Cogeco Devices are for business use only. It must not be shared with anyone, including with family or friends or used for personal activities.
- Cogeco only allows company approved wireless devices to be connected and used to access Cogeco’s network (other wireless devices not approved by the company must only connect to Cogeco’s guest wifi).
- Should not remove any identifying marks or stickers on the device such as a company asset tag or serial number.
- Cogeco Devices must not be connected to non-corporate networks such as public Wi-Fi or the Internet unless a Virtual Private Network (VPN) is used.

- Cogeco highly encourages users to connect to Cogeco's VPN for enhanced threat protection, application of IT and security updates and to better secure communications.
- To accept software updates (from Cogeco or from manufacturer) to keep Cogeco Devices protected.
- Take precautions to protect Cogeco Devices when using them outside of Cogeco's premises.
- Ensure that the device is locked away when being stored and that the key is not easily accessible.
- Permission must be obtained before the device is taken out of the country (Canada and United States), and security measures should be taken following the Working Out of Country Standard.
- If the device is supplied with encryption, End-users are not permitted to disable it.
- For Cogeco supplied mobile devices, streaming video, large downloads, or personal hotspot usage that could lead to data overages is prohibited unless essential for business purposes.
- Employees taking a leave of absence (i.e. maternity leave, disability, etc.) are required to follow the guidelines set out by Human Resources pertaining to all corporate Cogeco Devices. Please contact the local Human Resources Representative for details.

11. Bring your own (BYOD) device

End-users are responsible to exercise reasonable due diligence when using their personal devices for work purposes. The following applies:

- Personal mobile devices (i.e. smartphones, tablets) are allowed with the installation of mobile device management (MDM) software.
- Personal computers are not allowed unless their use is specifically approved.
- End-users must protect company data by using strong passwords, device encryption and approve security software.
- Cogeco will not view or monitor any personal data stored on your personal device, except as described below or as required by law.
- Cogeco reserves the right to access, review, monitor or delete any Cogeco business information or data transmitted between Cogeco's information technology assets and the personal device.
- Cogeco can also, without notice, remotely delete all data from the personal device, including all personal data unrelated to Cogeco, if there is any reason to believe that its business information stored on their personal device may be at risk of being compromised or misappropriated, including if the personal device is lost or stolen.
- Cogeco may, in its sole discretion, require access to the End-user's personal device or the company information stored on it for legitimate business purposes, including for investigative purposes and to implement a litigation hold.
- End-users must not attempt to change or disable any security settings applied to the device by the IT team.
- End-users should consult the manufacturer/vendor/carrier for support of their personal devices.
- Cogeco is not responsible for servicing and maintaining personal devices.

12. Applications and cloud computing

Cogeco makes extensive use of cloud services to enable business processes in a responsive and flexible way. These services are subject to a due diligence procedure to ensure that they meet our business, security and legal requirements. End-users should only use cloud services (including any external cloud storage) that have been put in place or approved by Cogeco.

End-Users are not permitted to use any unauthorized software or cloud solutions (Shadow IT). The onboarding of any new software or cloud solution by Cogeco must go through procurement and follow the Procurement Policy.

13. Working from home / outside of office

Cogeco has adopted a hybrid work model, where End-users have the flexibility to work from the office or from home. This also means that End-users are responsible for keeping company information secure in all locations.

End-users working from home must follow the Remote Work Policy.

End-users who are working remotely and outside of Canada or the United States must follow the Remote Work Policy and the Working Out of Country Standard.

14. Legal obligations

End-users should not take any action or use a Cogeco Device or network in a manner that either (i) violates a law, regulation or standard applicable to the End-user or Cogeco or (ii) puts Cogeco in a situation of breach of any such applicable law, regulation or standard. “Applicable laws, regulations or standards” includes, but is not limited to, criminal, intellectual property, defamation and privacy laws applicable to Cogeco or the End-user.

In fulfilling this obligation, End-users are required to:

- Follow all Cogeco’s internal policies, standards and guidelines, available here: InfoSec page.
- Avoid using the intellectual property of others, such as software, videos, music, books, documentation, photographs and logos, even when the usage is for internal purposes only. This includes, but is not limited to, the download, installation or distribution of "pirated" content and the use of solutions that are not appropriately licensed for use by Cogeco. Unless specifically stated otherwise, all material on the Internet must be considered copyrighted.
- Not extract and store Cogeco Data or intellectual property, developed or gained during the period of employment, beyond termination or reuse for any other purpose.

15. Use of social media

Cogeco makes extensive use of social media to communicate directly with our customers as part of our marketing activity, to provide support for our products and services, and to obtain useful feedback on how our organization is perceived.

End-users are not permitted to post or direct messages on social media on behalf of Cogeco unless they have been designated an authorized Cogeco Social Media representative in accordance with Cogeco’s Social Media Use Policy.

Any mention of Cogeco or Cogeco’s information by an End-user on their own social media account must always be in alignment with the Disclosure Policy, Social Media Use Policy, Information Security Policy and the Code of Ethics.

Cogeco reserves the right to request a Cogeco-related Internet posting deemed inappropriate be deleted by the individual who made the post or the website where the post was made.

16. Use of generative Artificial Intelligence (AI)

At Cogeco, the use of generative AI tools is restricted to the tools officially approved by the CTIO team (“Approved Gen-AI”).

End-users shall:

- Not use any publicly available platforms such as ChatGPT, Edge Copilot or other open source AI systems for business purposes, unless duly authorized by the CTIO team;
- Follow the principles of responsible AI usage identified below and comply with any additional guidelines, policies or standards developed by Cogeco in relation to AI usage:
    - do not disclose Sensitive Data (confidential information or intellectual property of Cogeco or Personal Information of individuals) when using Approved Gen-AI, unless the platform was approved for such usage;
    - Be mindful that AI products and technologies should only be used when they can deliver better, safer, more efficient and equitable services and products to our customers and/or improve efficiency and productivity for internal staff;
    - Take reasonable steps to determine that the information or results obtained through an AI system are accurate and free of bias. It is strongly recommended to use human review to validate the outputs and results;
    - Ensure that Cogeco’s Legal department is engaged to evaluate the intellectual property status of any output of an Approved Gen-AI solution.
- Never use any generative AI tool to perform malicious or inappropriate actions.

17. Information security incidents

If an End-User detects, suspects or witnesses an incident that may be a breach of security, submit an incident via the IT Service Management tool (i.e. ServiceNow). Unusual or unexplained events, such as messages appearing on your device, can indicate that an incident is happening, and these should be reported as soon as possible.

If an incident is detected by CogecoEnd-users may be asked to take specific action, such as logging off systems or closing their device. Users should follow such requests as soon as possible.

In addition, the End-user must not use, be involved or take part in:

- security breaches;
- malicious disruptions of network communication;
- interfering with or denying service to any Cogeco asset;
- any technique/program/script/command or establish contacts of any kind, with the malicious intent to interfere with or gain unauthorized access to systems;
- network monitoring or intercepting of communications of any kind unless this activity is a part of their normal duties;
- Port scanning or any other type of security assessment unless this activity is a part of End-user's job duties;
- circumventing any IT/security controls applied to Cogeco Devices, systems or networks;
- introducing viruses or other malware into the system or network, for example by inserting unknown peripherals or media into Cogeco devices.

18. Monitoring

All Cogeco End-users are accountable for all activities performed under their Cogeco-related accounts and assigned devices.

By accessing Cogeco's network, intranet, and other corporate systems, the End-user understands and accepts that Cogeco may log and monitor their activities, as permitted by law. Cogeco electronic communications and data storage are monitored and archived. These may be analyzed for reasons such as troubleshooting, security, ethics or legal investigations, and backup and recovery. Cogeco reserves the right to log, monitor and archive all inbound and outbound network traffic and block any communications that pose a risk to Cogeco's assets and resources.

Authorized individuals must do the logging and monitoring for information misuse, compliance with applicable laws and regulations.

Cogeco reserves the right to deny the use of devices deemed to have inadequate security configurations, measures or capabilities.

19. Roles and responsibilities

19.1. End-users

Review, understand and follow this policy.

19.2. Information Security (InfoSec)

- Review, update and publish this policy.
- Implement/define/validate applicable security controls.
- Work with HR to communicate the policy to ensure that Cogeco's End-users are aware of and understand its application.

19.3. IT Colleague Services Team

Act as the first point of contact for End-users when incidents are reported and requests are submitted.

19.4. Management

Ensure that End-users are aware of this policy and understand how to apply it.

19.5. Internal Audit

May periodically review and report Cogeco's compliance with this policy.

19.6. Legal

Identify, interpret and communicate legal and regulatory requirements (and any changes to them) that are applicable to this policy.

20. Compliance

Failure to comply with this policy increases security risk to Cogeco, unless exceptions have been documented/reviewed by InfoSec and approved by IT and, as applicable, the End-user's manager. All End-users found to have violated this policy may face disciplinary action, including termination and/or potential civil or criminal liability, subject to applicable laws.

21. Exception management

Exceptions to this policy must be requested via email to the Information Security Governance, Risk and Compliance (GRC) team at infosec.grc@cogeco.com. An exception may be granted only if the benefits of the exception outweigh the associated risks, taking into account applicable laws and regulations, and Cogeco's policies, standards and guidelines and following the existing Risk Management process.

22. References

- Code of Ethics
- Harassment, Discrimination and Violence-Free Workplace policy
- Information Security Policy
- Disclosure Policy
- Remote Work Policy
- Social Media Use Policy
- Employee Privacy and Confidentiality Policy
- Procurement Policy
- Third Party Security Standard
- Working Out of Country Standard
- Identity and Access Management Standard
- Information Asset and Protection Standard
- Information Classification Schema
- Risk Management process
- TPACA/NDA form
- PCI DSS
- Cogeco personal data definition
- Social engineering guides
- User guide on sending encrypted files

23. Glossary

Term	Definition
Cogeco	Cogeco Inc., Cogeco Communications Inc., Cogeco Connexion, Breezeline and Cogeco Media.
Cogeco Data	Data created or used in support of Cogeco's business activities, which may also include personal information that Cogeco has collected from its customers and/or Employees or other Sensitive Data. Cogeco Data can also include, collectively, all data and information in electronic format created, collected or received from whatever or whichever source by Cogeco or by any of Cogeco's Employees, or any other Third Party on Cogeco's behalf, that is either confidential, proprietary or business sensitive in nature. It may be based on either any law or regulation or any of Cogeco's interests, as any of them may evolve from time to time.
Cogeco Device / User Endpoint Device	Any equipment/device (e.g. laptop, tablet,smartphone, etc.) owned, approved and provided by Cogeco
Computing Device	Electronic equipment that may connect to the internet, such as a smartphone, tablet, or laptop computer.
Employee	All Cogeco part-time and full-time employees.
End-user	All board members, Management, Employees, contractors and other Third Parties
Information Security (InfoSec)	Information Security team

Term	Definition
InfoSec GRC	InfoSec Governance Risk and Compliance team
Management	Manager level and above. Colleague(s) who is responsible for planning, directing, and overseeing the work of others to achieve specific organizational goals.
Personal Information	Personal information is information about an identifiable individual. See documented Cogeco definition on Personal Information.
Sensitive Data	At Cogeco, Sensitive Data is considered as information whose use is limited, shared only on a need to know basis and/ or can only be distributed internally with the data owner's approval. Some examples: • client or employee Personal Information • product information that would impact competitive advantage (price, detail, etc.) • corporate financial information • employee organizational charts • business process maps These types of information must be handled and shared with caution. If Employees are unsure on what data they can or cannot share, they have been asked to discuss this with their manager.
Shadow IT	The use of applications, devices and services without the knowledge or approval of the IT and Security departments of an organization. While perceived by the user as a quick fix to an everyday problem, the use of unsanctioned and unauthorized applications poses a significant cybersecurity threat to the organization.
Third Party	Service providers, integrators, vendors, telecommunications and infrastructure support that are external to Cogeco.
Virtual Private Network (VPN)	A remote access virtual private network (VPN) is a mechanism for creating a secure connection between a Computing Device and a computer network, using an insecure communication medium such as the public Internet.