Acceptable Use Policy for Cogeco's information technology assets

DOCUMENT INFORMATION			
NAME (ID)	*Acceptable Use Policy for Cogeco's information technology assets*		
OWNER	*Information Security Department (InfoSec)*		
SUMMARY	*This policy outlines the acceptable use of information technology assets at Cogeco*		
VERSION	*V1.0*	**EFFECTIVE DATE**	*June 24, 2022*
PREPARED BY	*Chief Technology Officer*		
APPROVED BY	*Chief Executive Officer*		
AUDIENCES	Cogeco Inc., Cogeco Communications Inc. and the Business Units (collectively "Cogeco"), *employees, and Cogeco contractors, Third parties and suppliers*		

TABLE OF CONTENTS

PURPOSE

This policy outlines the acceptable use of information technology assets at Cogeco. It directs and gives guidance to the appropriate usage of Hardware, Software and applications at Cogeco, with respect to the Code of Ethics. It governs the use of information, electronic and Computing Devices, and network resources to conduct business or interact with Cogeco networks and business systems.

SCOPE

This policy applies to all end-users who access a Cogeco Resource, asset or facility. Employees should be aware that all use of Cogeco Devices is subject to monitoring by Cogeco and as such, Employees have no right to, or expectation of, privacy with respect to their use of Cogeco Devices, subject to applicable laws.

POLICY STATEMENTS

Cogeco proprietary information stored on electronic and Computing Devices, whether owned or leased by Cogeco, an Employee or a third party, remains the sole property of Cogeco. All aforementioned parties have a responsibility to promptly report the theft or loss of Cogeco Devices or the unauthorized disclosure of Cogeco Data to the IT Service Desk at each Business Unit. Employees must ensure that Cogeco Data is protected by following the steps below. Information must only be shared to the extent it is authorized and necessary to fulfill assigned job duties.

Employees are responsible for exercising reasonable due diligence regarding the appropriate use of Cogeco Devices. If some actions are not referred to in this policy, it does not make them permitted. Employees should be guided by Business Unit practices or guidance on personal use and if there is any uncertainty, Employees should consult their reporting manager.

1. ACCEPTABLE USE

1.1. Collaboration, Email and Communication Activities

1.1.1. Logging into corporate accounts must only be done through devices provided by Cogeco or authorized Personal Devices having the appropriate means of protection.
1.1.2. Cogeco email must be used for business purposes or limited personal use. Users must realize that they represent Cogeco in all communication activities.
1.1.3. Cogeco email communications must only originate and be received by corporate email accounts to avoid misrepresentation and bypass of security scanning (e.g., use of personal accounts for business purposes is prohibited)

1.1.4. Forwarding any sensitive information is subject to data protection processes. Security tools will scan e-mail and files for Sensitive Information and if shared, will warn users that the information being shared could be of a sensitive nature. Sharing Sensitive Information outside of Cogeco is only permitted with Third Parties that have signed a Non-Disclosure Agreement (NDA) or Third Party Access and Confidentiality Agreement (TPACA).

1.2. Electronic Storage / Physical Media

1.2.1. Employees handling sensitive business-related waste shall shred their documents using confidential waste bins or shredders that are available in any office or by cutting the documents into smaller pieces and disposing of them in a recycling bin.

1.3. Data Handling

1.3.1. Cogeco Data must be handled, stored, transmitted and processed according to applicable international and/or local laws, regulations and Cogeco standards.

1.4. Wireless / Internet

1.4.1. Company-provided devices must be connected to a corporate VPN at all times while connected to a wired/wireless network that is not owned/operated by Cogeco. (i.e., connecting a Cogeco laptop to a password-protected wired/wireless network).

1.4.2. Cogeco allows only company-approved wireless devices to be connected and used to access Cogeco’s internal network.

1.5. Computing Devices

1.5.1. Only Cogeco-approved devices may access Cogeco’s network or in the case of a Third Party, under a Third Party Access and Confidentiality Agreement (TPACA).

1.5.2. Using access control (e.g., password, PIN or biometric) verification must be set and used on a Computing Device that accesses Cogeco Data.

1.5.3. Device passwords must be complex and must not be shared to limit access and keep data secure.

1.5.4. Cogeco owned or leased Computing Devices must be protected.

1.5.5. Reasonable due diligence must be exercised on the personal use of technology assets.

1.5.6. When you leave your Cogeco Device unattended, you should log out, lock or protect the information with a screen lock mechanism.

1.5.7. In the event of theft or loss of company-owned equipment, report it immediately to your service desk.

1.5.8. Upon resignation or termination of employment, all Cogeco equipment (e.g. workstations, portable, mobile and removable devices) must be returned by contacting HR or your IT Service Desk.

1.5.9. Personal devices are only allowed with the installation of mobile device management (MDM) software controlling all data on the device and installed by authorized Cogeco IT representatives.

1.6. Remote Work

1.6.1. Employees working remotely in their country (reporting center) must follow the Remote Work Policy.

1.6.2. With approved business justification, Cogeco's systems that store Cogeco Data may be accessed remotely by appropriate remote access tools, as designated by the Cogeco IT representatives.

1.6.3. Remote access may be used by Employees only in compliance with guidelines issued by the Cogeco IT representatives.

1.6.4. Upon termination or end of assignment, immediate deactivation of remote access must occur.

2. UNACCEPTABLE USE

Under no circumstances are Employees of Cogeco authorized to engage in any activity that is illegal under local, provincial/state, federal or international law while utilizing Cogeco-owned resources. The lists below shall not be considered exhaustive but provide a framework for activities which fall into the category of unacceptable use. The following activities are, in general, prohibited.

2.1. System and Network Activities

The following activities are strictly prohibited:

2.1.1. Access to corporate platforms from a Public Device.
2.1.2. Processing, storing and sharing Cogeco Data on/through a personal account.
2.1.3. Unauthorized use of information protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations. Including, but not limited to, the installation or distribution of "pirated" or other Software products that are not appropriately licensed for use by Cogeco.

2.1.4. Downloading copyrighted, patented or trademarked material (e.g. music media and video files) without authorization.
2.1.5. Using unauthorized, free web-based Software solutions (e.g. calendar integration, survey and event registration platforms).
2.1.6. Opening email attachments received from unknown senders, which may contain malware.
2.1.7. Publishing personal websites on Cogeco-owned or leased information resources
2.1.8. Personal use that affects Employee’s business performance and is detrimental to Cogeco (using Cogeco email to make personal gains or conducting personal business).
2.1.9. Using Cogeco email systems that could affect the email service’s reliability or effectiveness (e.g. distributing chain letters or spam).
2.1.10. Using external accounts for Cogeco business purposes (e.g. email account).
2.1.11. Using a Computing Device to actively engage in procuring, storing or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
2.1.12. Providing Sensitive Information to parties outside Cogeco without an approved and executed non-disclosure agreement.
2.1.13. Providing access to Cogeco’s network to third parties without a TPACA.
2.1.14. Accessing Cogeco Data, a Cogeco server or a Cogeco account for any purpose other than conducting business, even if you have authorized access.
2.1.15. Providing unauthorized access to a Cogeco Device or Cogeco Data to another individual, either deliberately or through failure to secure system access.
2.1.16. Revealing your Cogeco account password to others or allowing use of your Cogeco account by others. This includes administrators at work and family and other household members.
2.1.17. Personal passwords should not be stored unencrypted on company owned devices.
2.1.18. Work-related passwords should not be stored in clear text in documents without access control and should be password protected.
2.1.19. Circumventing user authentication or security of any host, network or account.
2.1.20. Involvement in security breaches or malicious disruptions of network communication.
2.1.21. Interfering with or denying service to any user other than the Employee's host (for example, denial of service attack).
2.1.22. Using any program/script/command or sending messages of any kind, with the malicious intent to interfere with or gain unauthorized access to systems by any means, locally or via the Internet/Intranet.
2.1.23. Executing any form of network monitoring that will intercept data not intended for the Employee’s host, unless this activity is a part of their normal job/duty.
2.1.24. Port scanning or security scanning is expressly prohibited unless part of Employee's job duties.
2.1.25. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
2.1.26. Copying, moving or storing Cogeco Data onto local drives, including removable media when using remote access technologies, unless using a Cogeco managed device.

2.1.27. Extracting and storing Cogeco Data or intellectual property, developed or gained during the period of employment, beyond termination or reuse for any other purpose.

2.1.28. Making fraudulent offers of products, items, or services originating from any of Company's accounts.

2.2. Internet

Use of the Internet on Cogeco managed-devices should be for Cogeco business purposes. Internet access is provided to Employees with a business need. While tools are used to prevent connections to offensive and non-business Web sites, the ability to visit a specific Web site does not mean Employees are permitted to access the site or that Cogeco accepts the content of the site.

The following activities are strictly prohibited:

2.2.1. Connecting Cogeco Devices to the Internet by circumventing security controls.

2.2.2. Utilizing the Cogeco name or conducting Cogeco business on public websites by unauthorized Employees.

2.2.3. Using a Cogeco Device, the Internet or Cogeco email for harassment or abuse of any kind (e.g. profanity, obscenities or derogatory remarks).

2.2.4. Employees must not attempt to circumvent Cogeco Web filter/proxy while using Cogeco-owned networks to access the Internet.

2.2.5. Employees must not use copyrighted materials for business purposes unless authorized by the Legal department. Unless specifically stated otherwise, all material on the Internet must be considered copyrighted.

2.2.6. 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.

2.2.7. Employees who use a Cogeco Device to connect to a Website containing sexually explicit, controversial, harassing or other potentially offensive material must disconnect from that site immediately.

2.2.8. Accessing, downloading, sending or receiving any data (including images) using a Cogeco Device without exercising reasonable due diligence.

2.2.9. Altering any information on Cogeco publicly facing web assets or making official comments through the Internet on behalf of Cogeco without authorization.

2.2.10. Using personal portable storage devices or cloud storage with non-Cogeco approved cloud providers are prohibited from connecting to the corporate network or directly connected to a PC without prior approval by management and IT.

2.2.11. Employees must not misrepresent, obscure, suppress, or replace their own or other Employees' identities on the Internet or any Cogeco's information system.

2.3. Blogging and Social Media

The following activities are strictly prohibited:

2.3.1. Sharing Sensitive Information in alignment with Social Media Use Policy, Information Security Policy and the Code of Ethics.

2.3.2. Disclosing Corporate Information, as defined under the Disclosure Policy, in violation of said policy.

2.3.3. Representing yourself as a spokesperson or speaking on behalf of Cogeco without business reason (i.e. someone working in the Public Relations department, Legal department, or marketing agencies managing Cogeco's social media posts).

2.3.4. Posting of Cogeco Data to blogs, forums or other social media that is deemed political, objectionable, controversial, or harassing in nature.

2.4. Computing Devices

The following activities are strictly prohibited:

2.4.1. Leaving Cogeco Devices and media unattended in public places and/or in an unlocked vehicle.

2.4.2. Leaving Cogeco Data on work printers, photocopiers, facsimile machines and desks when not present.

2.4.3. Sharing Cogeco-related user accounts and passwords.

2.4.4. Using Cogeco systems for purposes other than for their primary business function.

2.4.5. Initiating malicious disruptions of network communication:

2.4.5.1. Port or security scanning;
2.4.5.2. Executing unauthorized network monitoring;
2.4.5.3. Circumventing user authentication or the security of any host, network or account; and Introducing honeypots, honeynets or similar technology on the network.

2.4.6. Removing or disabling company-installed Software (e.g. anti-virus protection, patches or firmware, etc.).

2.4.7. Use of Cogeco Devices to operate a personal side business.

3. MONITORING

3.1. All Cogeco Employees are accountable for all activities performed under their Cogeco-related accounts.

3.2. By accessing Cogeco's network, intranet, and other corporate systems, all Employees understand and accept that Cogeco is entitled to the logging and monitoring of their accounts.

3.3. Cogeco email messages and electronic files are monitored and saved and these email messages may be inspected for reasons such as troubleshooting, legal investigations, or backup and recovery.

3.4. Cogeco reserves the right to monitor all inbound and outbound network traffic and block any communications that pose a risk to Cogeco's assets and resources.

3.5. The logging and monitoring for information misuse and compliance with applicable laws and regulations must be done by authorized individuals only.

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

4. ROLES AND RESPONSIBILITIES

All Cogeco Employees are responsible for protecting company information in accordance with Cogeco security standards and procedures.

4.1. InfoSec in collaboration with the Business Units

4.1.1. Review, update and publish this policy.
4.1.2. Implement/define applicable security controls.
4.1.3. Validate that security controls are implemented and effective.
4.1.4. Review adherence to policy and report any violations through appropriate channels.
4.1.5. Work with Business Units to communicate the policy to ensure that Cogeco's Employees, Third-Parties, contractors, and business partners are aware of this policy.

4.2. Managers, Directors and Officers

4.2.1. Ensure that Employees are aware of this policy.

4.3. Employees

4.3.1. Review, understand and abide by this policy.

4.4. Contractors

4.4.1. Review and abide by this policy.

4.5. Internal Audit

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

4.6. Legal

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

4.7. Third Parties

4.7.1. Review and abide by this policy, most specifically the following provisions:1.2, 1.3, 1.5, 1.6, 2.1.

5. COMPLIANCE

Failure to comply with this policy could increase security risk to Cogeco, unless exceptions have been documented/reviewed by InfoSec and approved by the Employee's manager. All Employees and Third Parties found to have violated this policy may face disciplinary action, including termination and/or potential civil or criminal liability, subject to applicable laws.

Employees who witness a violation to the Policy can report it to the ethics line at +1 877 706 2640 or online at www.clearviewconnects.com.

6. 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, as well as the Cogeco's policies and guidelines.

7. OWNERSHIP

This Policy is owned by InfoSec. Any questions or issues arising from the interpretation of this Policy should be addressed to the Information Security Governance, Risk and Compliance (GRC) team at infosec.grc@cogeco.com.

8. MANAGEMENT COMMITMENT

Management is committed to the direct participation by the highest level of leadership in all specific and critically important aspects of security for Cogeco. It is important that the responsibility for creating an environment of continuous improvement belong to all levels of management and employees.

9. REVIEW & REVISION

This document will be reviewed annually by the Business Units and InfoSec, or as needed. Any amendments to this document must be approved by the Business Units and InfoSec.

10. REFERENCE TO OTHER POLICIES AND STANDARDS

- Code of Ethics
- Social Media Use Policy
- Disclosure Policy
- Remote Work Policy

11. GLOSSARY OF TERMS

Term	Definition
Business Units	Referred to as Cogeco Connexion, Breezeline and Cogeco Media
Cogeco	Cogeco Inc., Cogeco Communications Inc. and the Business Units
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 Information. 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	Any equipment/device (e.g laptop, tablet, or smartphone) owned and provided by Cogeco
Cogeco Resource	Materials, money, staff, and other assets owned and provided by Cogeco
Computing Device	Electronic equipment that connects to the internet, such as a smartphone, tablet, or laptop computer.
Employee	All Cogeco part-time and full-time employees.

InfoSec	Information Security Department
Personal Device	Any devices (e.g laptop, tablet or smartphone) owned by an individual
Public Device	Devices used in shared spaces where multiple people will be sharing the same outlet (e.g Public library PC, cyber cafe PC)
Sensitive Information	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.
Software	Set of instructions, commands for a computer to perform specific operations, or tasks for an end-user
Third Parties	Service providers, integrators, vendors, telecommunications and infrastructure support that are external to Cogeco.