Privacy and Data Protection Policy

Version 1.0, April 21st, 2023

1 – Introduction

In the course of its operations, CQ, CQ Users and CQ Tenants, will store, transmit and use data on CQ Information Systems. This policy is intended to inform all stakeholders of CQ's commitment to protect such information, including certain information that may be considered confidential. More specifically, it sets out the basic requirements that ensure that CQ Information and Information Systems have appropriate safeguards in place to maintain the expected level of integrity and confidentiality, both for CQ Users and for CQ Tenants. This policy complements the CQ Security Policy[1].

2 – Definitions

Information security terms are defined in the CQ Security Policy and are also available in the CQ Information Security Glossary.[2] The following additional definition is required in this policy:

- **Information Steward**: individual who oversees the lifecycle of Information and other types of data assuring the quality, integrity, and access arrangements of Information and data from the moment of its collection. They are responsible for determining the data Information

[1] https://www.calculquebec.ca/security-policy
[2] https://www.calculquebec.ca/information-security-glossary

Security Classification (as defined in the Directive on Information Security Classification[3]), for identifying security and confidentiality requirements or controls to be used for its protection, for implementing internal and external security reviews and audits, and for keeping logs. For CQ Tenants and CQ Users, they are each responsible for identifying or assigning the role of Information Steward as part of their management plan for the Information in their custody. For Information under the authority of CQ, a CQ Team Member will be the Information Steward.

3 – Scope

The Privacy and Data Protection Policy supports the CQ Information Security Framework and will be implemented and enforced in accordance with the CQ Security Policy.

4 – Roles and responsibilities

In addition to the roles defined in the CQ Security Policy, the following role is required for the purposes of this policy:

Information Steward: while using or accessing Information or CQ Information Systems, they are responsible for:

- Ensuring the quality, integrity, and access arrangements of Information from the moment of collection to the end of its life cycle.
- Determining the Information Security Classification for the data under their responsibility (as defined in the Directive on Information Security Classification) and identifying appropriate Information Systems for the use of such data.
- Identifying and ensuring security and confidentiality requirements or controls used for the protection of the Information under their responsibility.
- Establishing, in accordance with CQ policies, the parameters for accessing, sharing, and curating Information, and where applicable, conduct internal and/or external security reviews and audits to assess its effectiveness.
- Creating and maintaining logs or records on data curation.
- With respect to Information under the authority of CQ, recording all required Information about the CQ asset in the asset inventory in a timely manner, as defined by CQ management.

5 – Policy

Collection

1. During the course of its operations, CQ will only collect Personal Information that is necessary for the services CQ offers and for their improvement. This will include system level information (usage, system metrics, network and access information, etc.) that may

[3] https://www.calculquebec.ca/directive-on-information-security-classification

be used to identify an individual. This may also include Personal Information about CQ Users and CQ Tenants. Only Personal Information essential to CQ operations shall be collected and consent must be obtained by the individual prior to its collection or use. In accordance with the law, consent must be manifest, free, enlightened and be given for specific purposes. Each of these purposes shall be described in simple and clear terms. Consent is only valid for the duration necessary for the realization of the purposes for which it has been requested. Any other use of Personal Information shall require a new consent to be obtained from the individual prior to its collection and use.

2. Calcul Québec or a CQ Team Member may request a CQ User or CQ Tenant to disclose Personal Information about another individual in order to provide requested services. It is the CQ User or CQ Tenant's responsibility to obtain, provide and document the consent of the individual in accordance with this policy. Calcul Quebec and the CQ Team Members will follow all the reasonable safety measures to maintain the confidentiality of this Personal Information in the course of the provision of the requested services.

3. As part of the partnership with the Digital Research Alliance of Canada "Alliance", access to QC Information Systems and Information may be provided by the Alliance. For the purposes of this policy, data obtained through the Alliance constitutes Information to which the CQ Information Security Framework applies. Such Information will be treated in accordance with the applicable Alliance policies or any other agreement relating thereto. In the absence of a clear policy or agreement to this effect, CQ undertakes to treat this Information as Sensitive Information.

Use and access

4. CQ's reporting obligations may also require the disclosure of service-related system-level information that could result in individual identification. Where possible, CQ will limit access and use of this Personal Information to the fulfillment of those reporting obligations and where possible, it will remove all unnecessary identifying elements (i.e. the information should not be identifiable down to the individual CQ Tenant or CQ User).

5. Access to Sensitive Information will be restricted to CQ Team Members, with a legitimate need for such information so they can perform their duties. CQ Team Members will not access data in CQ User or CQ Tenant custody unless they provide their consent, it is required by law, or it is agreed on in the conditions set out in the Service Level Agreement or Terms of Use. The access that CQ Team Members have to the data in CQ User or CQ Tenant custody will be monitored, minimized, and limited to the scope and timeframe of the investigation or monitoring function. Data hosted by a CQ Tenant in an IaaS environment will not be accessed for monitoring purposes, except where such access is explicitly defined and permitted in the Service level agreement or Terms of Use or required by law. Privileged Access by CQ Team Members to CQ Tenant services or infrastructure hosted in an IaaS environment are not allowed, unless there is a written agreement to this effect between the CQ Tenant and Calcul Québec.

6. Any requests for access to CQ User or CQ Tenant data, outside of the monitoring and investigative functions required by CQ operations to detect, track and preserve CQ Information Systems level of service, should be directed to the Information Steward. In the situation where there is a legal reason or requirement to retrieve information in CQ User or CQ Tenant custody, CQ will work with the Information Steward to follow due process, in accordance with applicable institution policies, before any information is released.

Conservation and security

7. CQ Users and CQ Tenants are responsible and accountable for compliance with applicable laws and regulations concerning the information in their custody. They may also be subject to additional specific business or institutional policies and contractual obligations with respect to data protection and confidentiality with third parties. It is the sole responsibility of the CQ User or CQ Tenant to identify and to comply with any additional requirements identified therein.

8. CQ Team Members are responsible to ensure that Information within CQ responsibility (including PI/PHI) is kept secured at all times and that appropriate CQ Information Systems are being used to store, process or transmit it, in compliance with the CQ Information Security Framework.

Communication

9. If CQ Users and CQ Tenants store, process or transmit Sensitive Information (including PI/PHI), they must do so under the most secure conditions, using reasonably appropriate security measures. If deficiencies are noted, CQ will promptly notify the CQ User or CQ Tenant and request that corrective actions be taken. If the CQ User or CQ Tenant fails to act to remediate the situation, CQ reserves the right to revoke access and remove the Sensitive Information from the corresponding CQ Information Systems, as described in the Service Level Agreement or Terms of Use.

Incidents management

10. Security or privacy issues pertaining to services or infrastructure hosted in the IaaS environment must be reported directly to the appropriate CQ Tenants. In the event of a suspected privacy breach, CQ Team Members, CQ Users, and CQ Tenants must notify the CQ CISO immediately upon its discovery[4]. The Information Steward will be notified as well without delay as outlined in the applicable Service Level Agreement or Terms of Use. The CQ CISO will oversee that the Information Steward verifies, in collaboration with the designated CQ Team Members, the suspected privacy breach and determines to what extent the breach can be confirmed.

[4] You can send an email to security@calculquebec.ca

11. In the event a case of privacy breach is confirmed, the CQ CISO will immediately coordinate the response to the breach with the CQ Team Members responsible for implementing the measures to restore, in a timely manner, the confidentiality, integrity and availability of Information and CQ Information Systems. All suspected and confirmed privacy breaches must be logged and documented. These logs must be kept and made available for the corresponding audits. Any unauthorized access to PI/PHI will be referred to law enforcement according to applicable legislation.

6 – Final provision

The policy comes into effect on the date of its adoption. Any questions regarding this policy or its interpretation may be directed to CQ General management. This policy will be reviewed at least annually, in order to better meet the needs of our partners or new requirements from the federal and provincial governments.

7 – Policy Version History

Please refer to the document change log for the full version history of this policy. Previous official versions can be made available upon request.