Security Policy

Version 1.0, April 21st, 2023

1 – Introduction

Calcul Québec manages and operates Advanced Research Computing (ARC) services to support excellence in research and innovation in Québec and Canada. As a service provider, Calcul Québec offers a diverse set of services, including consulting and professional services, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This policy concerns security measures required to deliver these services.

Calcul Québec's policies apply to all services offered by Calcul Québec, in accordance with the mandate given to CQ by member universities. These services use information systems of which McGill and Laval universities are the main owners. They are part of a national partnership via the Digital Research Alliance of Canada.

As a service provider, Calcul Québec has obligations in regards to assets and data protection, which includes the protection of Personal Information (PI) and Personal Health Information (PHI). The following legislation and the regulations resulting from it is applicable to Calcul Québec activities in Quebec:

- Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information;
- Act Respecting the Protection of Personal Information in the Private Sector;
- Act Respecting the Sharing of Certain Health Information;
- Act Respecting Health Services and Social Services;
- Act to Establish a Legal Framework for Information Technology

As an organization within Canada, Calcul Quebec must also adhere to Canadian federal laws such as the *Personal Information and Electronic Documents Act* (PIPEDA). These laws contain provisions that require Calcul Québec, CQ Users and CQ Tenants to take reasonable steps to ensure that PHI/PI is protected against theft, loss and unauthorized use or disclosure, and to ensure that records containing PHI/PI are protected against unauthorized copying, modification or disposal. When necessary, and to the extent applicable for CQ services, CQ will use reasonable measures to comply with *European General Data Protection Regulation* (GDPR) requirements.

CQ Users and CQ Tenants may be subject to other legal or regulatory requirements that exist within their province, state or country. They may also be bound to specific business or institutional policies and contractual obligations that limit or prevent their use of Calcul Quebec services. It is the sole responsibility of the CQ User or the CQ Tenant to identify and to comply with any additional requirements identified therein.

Security and privacy requirements will be set based on the specific services used by a CQ User or a CQ Tenant and by the level of sensitivity of the Information being transferred, processed or stored therein. The following objectives will be achieved through the implementation of security controls, as described in the remaining sections of this policy.

- **Availability of Information and CQ Information Systems.** The CQ Information and Information Systems must maintain a level of availability consistent with their operational role and be compatible with the specific service, as defined in the Service Level Agreement and Terms of use. CQ Information Systems' architecture and operations must be monitored and protected to prevent or fix accidental or unplanned service interruption.

- **Confidentiality of Information.** Right of access and use are restricted to authorized individuals for authorized purposes and duration. CQ Information Systems' architecture and operations must be monitored to protect, prevent or fix unauthorized access or information disclosure.

- **Integrity of Information and Information Systems.** The CQ Information Systems and the Information used, stored or transmitted on an Information System must maintain a level of integrity consistent with their role and be compatible with the level of service, as defined in the Service Level Agreement and Terms of use. CQ Information Systems' architecture and operation must be monitored to protect, prevent or fix accidental or malicious damage.

- **Access to Information and Information System.** Access to Information and Information Systems must be secure and flexible, while ensuring data privacy without compromising legitimate accessibility and relative ease of use.

- **Compliance with legal, regulatory and contractual requirements and standards of due care.** Compliance with applicable legislation is consistently monitored. Likewise,

security or privacy risks are identified, assessed, and managed. Reasonable actions are taken to detect and prevent malicious activities. Privacy breach and security incidents are managed in compliance with applicable laws and the Service Level Agreement and Terms of Use.

2 – Definitions

Information security terms are defined below and available in the CQ Information Security Glossary[1]:

- **CQ Information Security Framework**: refers to a set of policies, standards, guidelines, and best practices used by Calcul Québec to ensure the security of Information and CQ Information Systems.
- **CQ Information System**: any system that can store, transmit or process information and which is managed, operated, governed or regulated by Calcul Québec.
- **CQ Team Member(s)**: any individual employed by, bound to or working on behalf of Calcul Québec.
- **CQ Tenant(s)**: a CQ User who has been allocated IaaS resources. In doing so, the CQ Tenant is granted access and sole responsibility for managing its dedicated resources.
- **CQ User(s)**: refers to any individual who has access to Information or to a CQ Information System. Individuals accessing information or systems hosted by a CQ Tenant in a CQ IaaS environment are considered CQ Tenant's users and are therefore not CQ Users for the purposes of this policy.
- **Information**: any information or data transmitted, stored or processed by a CQ Information System; this includes, but is not limited to CQ User data and CQ Tenant data.
- **Information Security:** refers to the processes and methodologies designed and implemented to protect the Information and CQ Information Systems from unauthorized access, misuse, disclosure, destruction, modification, or disruption.
- **Infrastructure as a Service (IaaS)**: Services that provide CQ Tenants with a dedicated set of resources that fall solely under the CQ Tenant responsibility. IaaS is akin to a self service, where the CQ Tenant is responsible for their own services, data, users, operating system, network configuration, while leveraging CQ infrastructure to support their environment.
- **Personal Health Information**: any information about an identifiable individual, living or deceased, pertaining to their physical or mental health, health care, or any health related information concerning that individual.

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

- **Personal Information**: Any information concerning a physical person and which allows, directly or indirectly, its identification.
- **Platform as a Service (PaaS)**: Services that grant CQ Users with access to Information and CQ Information Systems in a way that allow them to manage their own software and data. Other system components, such as the operating system, storage infrastructure and network layer are managed and operated by CQ.
- **Privileged Access**: a type of access that grants someone permission to perform an action that is normally unauthorized or restricted and that grants extra control over the Information or a CQ Information System.
- **Sensitive Information**: Information that is classified as High Risk Information or Very High Risk Information (See Directive on Information Security Classification[2]).
- **Service Level Agreement (SLA)**: is an agreement where both the service provider (CQ) and a CQ User or CQ Tenant commit to terms about the level of service being offered by CQ. It includes, but it is not limited to, the expected level of service availability, the assignment of responsibilities, the terms of access, and additional terms of use specific to the service.
- **Software as a Service (SaaS)**: services that grant CQ Users with access to Information and CQ Information Systems through a software interface that allows them to manage their own data. Other system components, such as the operating system, software, storage infrastructure and network layer are managed and operated by CQ.
- **Terms of Use**: is an agreement where both the service provider (CQ) and a CQ User or a CQ Tenant commits to rights and obligations with respect to the Global Calcul Québec service offering.

3 – Scope

This policy applies to all Information and CQ Information Systems and to all CQ Team Members, CQ Users, and CQ Tenants. CQ Tenant services or infrastructure made available to the CQ Tenant's users in the IaaS environment are out of scope of this policy, as they are the responsibility of the CQ Tenant and not of CQ itself.

4 – Implementation

The implementation and enforcement of security policies is the duty of all CQ Team Members, CQ Users and CQ Tenants. Failure to comply with this policy may result in their access revocation, as well as disciplinary actions for CQ Team Members, as documented in the CQ

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

Information Security Framework. Non-compliance with the applicable laws may be deemed a criminal offense, and referred to the appropriate authorities for further action.

Compliance with the CQ Information Security Framework is mandatory. In case there is a perceived or apparent conflict between Calcul Québec policies, CQ Team Members, CQ Users, and CQ Tenants should communicate with Calcul Québec, as described in the Service Level Agreement or Terms of Use, for immediate resolution.

Periodic internal or external independent audits or assessments shall be undertaken to review or assess the adequacy and effectiveness of implemented security controls, including compliance with this policy. The CQ CISO is responsible for the routine periodic review of the CQ Security Policy Framework, at least annually, to ensure its effectiveness, accuracy and compliance.

5 – Roles and responsibilities

CQ General management: Reporting to the CQ board of directors, is responsible for setting forth the organizational objectives for Information Security and for allocating resources to enable and support the required Information Security functions. CQ Management is also responsible for approving and adopting CQ policies required to support this policy and granting them exceptions where appropriate.

CQ CISO (Chief Information Security Officer): CQ senior-level employee who oversees the CQ Information Security Framework. The CQ CISO is part of the CQ Management and is responsible for:

- Developing and implementing Calcul Québec's Information Security Framework.
- Assessing privacy and security risks and be responsible for the protection of personal information within CQ responsibility.
- Reviewing existing security measures and controls (e.g. procedures and technologies to verify the identity of those to whom access rights are to be granted, pseudonymization or anonymization when possible, physical measures to protect infrastructure from natural hazards as well as from tampering attacks, etc.) and reporting on their effectiveness.
- Keeping track of new laws, regulations, policies, expectations, and best practices associated with privacy and security and sharing them with the CQ Team Members when appropriate.
- Documenting and maintaining the Information Security policies and procedures and ensuring relevant documents are made available to CQ Users and Tenants.
- Developing, implementing and coordinating Information Security and privacy training and awareness programs on the appropriate organizational, physical and technical measures for the privacy and security of Calcul Quebec and the services it offers.

- Having a procedure in place, or designating an individual, to receive and respond to the reports on data or security breaches/incidents from CQ Team Members, CQ Users or CQ Tenants.
- Coordinating Calcul Québec's response to actual or suspected breaches, with respect to the confidentiality, integrity and availability of Information and CQ Information Systems.

CQ Team Members: are responsible for protecting the Information and CQ Information Systems by complying with the privacy and security objectives and associated requirements identified in the CQ Information Security Framework and this policy. These responsibilities include:

- Operating, maintaining and supporting Calcul Québec services and CQ Information Systems.
- Staying informed about security policies, requirements and operational procedures in place at Calcul Québec.
- Ensuring that their account and device are secured.
- Complying with the privacy and security measures and controls approved by the CQ CISO and included in this policy and the CQ Information Security Framework.
- Reporting to the CQ CISO (or the person he/she designates) any security incidents or privacy breaches, as identified in this policy and in the CQ Information Security Framework.
- Supporting the CQ CISO on the response to reported breaches with respect to the confidentiality, integrity and availability of Information and CQ Information Systems and implementing the necessary actions as mandated.

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

- Complying with Calcul Quebec policies as well as with any other policies that may be applicable to their use or access of CQ services.
- Ensuring that their account and device are secured.
- Reporting to Calcul Québec any security vulnerabilities, incidents or privacy breaches as identified in the CQ Information Security Framework.

CQ Tenants: while using the CQ IaaS environment, they are responsible for:

- Complying with Calcul Quebec policies as well as with any other policies that may be applicable to their use or access of CQ services.
- Monitoring and maintaining the privacy and security of the services or infrastructure they are hosting in the CQ IaaS environment
- Providing Calcul Québec with a contact for handling or reporting security events.
- Ensuring that their account and device are secured.
- Reporting to Calcul Québec any security vulnerabilities and/or incident or privacy breach, as identified in this policy or the CQ Information Security Framework.
- Managing and granting access to their own users.
- Deploying and operating their own services and infrastructure in a secure manner and being responsible for any privacy or security incident while doing so.

- Adopting adequate policies, standards, and processes to ensure appropriate safeguards exist within their area of responsibilities.
- Having a procedure in place with their own users to receive and respond to incidents on privacy and security and report these to CQ where appropriate.

6 – Policy

1. All Information and CQ Information Systems must be protected in a manner that is considered reasonable and appropriate to their life cycle and sensitivity, as approved by CQ Management and in accordance with the CQ information Security Framework. This information security framework, based on a risk management approach, aims to understand the existing risks as well as the strategies and controls put in place to deal with them.

2. The CQ Information Security Framework will define the terms and restrictions of access to CQ Information and Information Systems. Access must be limited to authorized services or Information Systems. Access to information will be restricted on a “need to know” basis. Access to or use of CQ Information or Information Systems must be made in a verifiable and auditable manner.

3. CQ Team Members must periodically receive training or awareness sessions relating to information security as well as to the security policies and standards in force at CQ. Access to Sensitive Information requires specific privacy and security training.

4. As a service provider, Calcul Québec will ensure that CQ Tenants are isolated from each other to ensure privacy and confidentiality are maintained within its Information Systems. CQ will ensure that the service and infrastructure it offers are secured and compliant with its commitments, as defined in the applicable Service Level Agreement or Terms of Use. However, the management of the data, infrastructure and services hosted in a CQ IaaS environment are the sole responsibility of the CQ Tenant. This includes, but is not limited to, the management of user access and rights, back-ups of the environment and its data, maintenance and updates of the operating system and software, monitoring (security and operational), and ensuring secured communications. Privileged Access by CQ Team Members to CQ Tenant services or infrastructure hosted in an IaaS environment are not allowed except where a written agreement to this effect exists between the CQ Tenant and Calcul Québec.

5. All Information Systems must be monitored to detect intrusion and unauthorized use or access. Detection of such events by CQ Team Members must be reported to the CQ CISO, and must be investigated and appropriate mitigation must be put in place to prevent further exploitation, as described in the CQ Information Security Framework. Any security issues, abuses or unauthorized access detected by a CQ Tenant or a CQ User shall be reported immediately to Calcul Québec[3]. In the situation where the security

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

event is considered by the CQ CISO to have a serious impact on the services or infrastructure hosted in the IaaS environment, all affected CQ Tenants will be notified as soon as possible.

6. In the event where a security incident is confirmed on an Information System, 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. For incidents where there is also a privacy breach or an impact on data security, the response must comply with requirements identified in the Privacy and Data Protection Policy[4]. Significant security incidents must be logged and documented according to the CQ Information Security Framework.

7. CQ Information Systems will be maintained and supported to minimize the exposure to security vulnerabilities and to minimize risk exposure, as described in the CQ information Security Framework. CQ Information System changes must be managed and authorized only by CQ Team Members with the appropriate Privileged Access, as identified in the CQ Information Security Framework. Every change implemented will be reviewed so as to assess and minimize its impact on the privacy and security of the Information System prior to implementation. Only those changes that require an action from the CQ Tenant or the CQ User or those that have a serious impact on the CQ Information System will be notified to the CQ Tenants and CQ Users.

8. Access to CQ Information System logs is restricted to authorized CQ Team Members. Service Level Agreement or Terms of use may include provisions, which allow a CQ Tenant to access CQ Information Systems logs, provided that confidentiality and privacy of other CQ Users and Tenants is respected.

7 – 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.

8 – 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.

[4] https://www.calculquebec.ca/privacy-and-data-protection-policy