Directive on Information Security Classification

Version 1.0, April 21st, 2023

1 – Introduction

Information Security Classification is a fundamental part of any security program. Information varies in its level of sensitivity, as does the corresponding risk and impact of its disclosure. It is therefore important to classify Information according to its requirements for confidentiality, integrity and availability to ensure it always has the appropriate level of protection. The purpose of this directive is to establish the Calcul Québec Information Security Classification model and to provide direction and guidance on its use. This classification is compliant with the data classification policy of the Digital Research Alliance of Canada.

2 – Definitions

Information Security definitions are available in the Calcul Québec Information Security Glossary[1]. In addition, the following definitions are required for the purpose of Information Security Classification:

- **Information Custodian**: individual who has custody or access to Information or data and is responsible for implementing security or privacy controls. An Information Custodian applies the privacy and security rules, as set forth by the Information Steward.

- **Information Security Classification:** refers to an Information categorisation to ensure that appropriate security controls are being used for its protection.

- **Low Risk Information**: Information should be classified as low-risk when the

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

unauthorized disclosure, alteration, unavailability or destruction of that Information could cause minor or no harm to the Data Subjects, Calcul Québec and/or its affiliates.

- **Moderate Risk Information**: Information should be classified as moderate-risk when the unauthorized disclosure, alteration, unavailability or destruction of that Information could cause moderate harm to the Data Subjects, Calcul Québec and/or its affiliates or Information that must be protected under non-disclosure principles.
- **High Risk Information**: Information should be classified as high-risk when the unauthorized disclosure, alteration, unavailability or destruction of that Information could cause major harm to the Data Subjects, Calcul Québec and/or its affiliates or Information that must be protected by law or industry regulation from unauthorized access or use.
- **Very High Risk Information**: Information should be classified as very high-risk when the Information is not covered in previous classifications but whose unauthorized disclosure, alteration, unavailability or destruction of that Information could cause critical harm to the Data Subjects, Calcul Québec and/or its affiliates.
- **Sensitive Information**: Information that is classified as High Risk Information or Very High Risk Information

3 – Scope

All Information in scope of the Calcul Québec Information Security Policy[2] are required to comply with this directive.

4 – Classification

The CQ Information Security Classification model classifies Information under four levels of risks: Low Risk, Moderate Risk, High Risk, and Very High Risk. The classification of Information is not static and may change over time. For example, unpublished research data may be initially classified as Moderate Risk Information, but after publication re-classified as Low Risk Information. The sensitivity levels are established based on the potential impacts that a loss of confidentiality, integrity, or availability of that Information would have (on Calcul Quebec, CQ Users, CQ Tenants, etc.) in the case of its unauthorized disclosure, as described below:

Low Risk Information
Examples: ● Information that requires no protection

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

- Information that is publicly accessible (e.g. Published annual reports, press releases, new articles)
- Names and work contact information of CQ Team Members
- Information that may be posted to public websites
- Information of a non-personal and non-proprietary nature including anonymous research data where access to that data is not restricted

Potential disclosure impact or risk:

- Minor embarrassment but very limited in scope

Moderate Risk Information

Examples:

- Proprietary information received from a third party under non-disclosure agreements (NDA) or that we would share under non-disclosure agreements if higher-risk categories are not applicable
- Restricted circulation library journals
- Aggregate financial information and reports
- Technical information about systems or facilities that is unlikely to result in any harm.
- Information of a non-personal, possibly proprietary nature including anonymous research data where access to that data should be restricted

Potential disclosure impact or risk:

- Limited impact on reputation or finances within CQ or affiliate
- Limited impact on operations within CQ or affiliate
- Loss of priority of publication (e.g. first to publish)
- Loss of access to journals or other copyrighted materials

High Risk Information

Examples:

- Controlled data requiring protection by law, NDA or industry regulation
- Data associated with patents or patent applications
- Personally identifiable information
- Confidential financial information and records
- Technical information that facilitates compromise of systems or facilities
- Research data that would take significant efforts or cost to collect or reproduce (e.g. additional funding may be required)

Potential disclosure impact or risk:

- Impact on reputation or finances of at CQ or affiliate
- Impact on operations of at CQ or affiliate

- Potential for identity theft
- Potential for fraud or spear fishing

Very High Risk Information

Examples:

- Customer Payment Card Information when CQ or affiliate is acting in a merchant capacity
- Personal Health Information as defined by provincial or federal legislation (PHI)
- Personally identifiable genetic data
- Biometric data
- Copy of government identification card
- Strategic or sensitive research software or dataset
- Personally identifiable data protected by regulation/legislation (e.g. GDPR)
- Research data that may not be possible to collect or reproduce

Potential disclosure impact or risk:

- Serious impact on reputation or finances for CQ or affiliates
- Serious impact on operations for CQ or affiliates
- Financial loss (regulatory fines or damages from litigation)
- Loss of competitiveness of key strategic research area
- Identity theft severely impacting individuals

5 – Directives

1. The Information Steward is responsible for determining the Information Security Classification for Information under his/her control. CQ may treat or handle Information as if its classification is of a higher level, but never use a lower level of classification.

2. The Information Custodian is responsible for being informed about the types of Information under their control; this includes their Information Security Classification and within what Information System corresponding Information is being stored.

3. Information about Sensitive Information under the authority of CQ must be kept in an inventory, in compliance with requirements identified in NORM 8 - Asset Management. CQ also recommends that CQ Users maintain an inventory of Sensitive Information in their custody.

4. Information must be stored or processed in a CQ Information Systems that is compatible with its designated Information Security Classification or above.

5. All Information, except Low Risk Information, is confidential and should be subject to caution prior to its use, sharing or disclosure. CQ Documents must identify the authorized sharing and the Information Security Classification using a label as per the CQ Directive on Document Labeling.

6. Information must be protected according to their Information Security Classification as defined and documented in the CQ Information Security Framework.

6 – Directive Version History

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