CDPQ

TITLE **Information and Technology Asset Security Policy**	APPROVAL Board of Directors
ISSUING BUSINESS UNIT Executive Vice-Presidency (EVP), Technology	DATE 2022-06-10

RELATED LEGISLATION, POLICIES AND GUIDELINES

- Acts:
  - Archives Act
  - Act respecting Access to documents held by public bodies and the Protection of personal information
  - Act to establish a legal framework for information technology
  - Act respecting the governance and management of the information resources of public bodies and government enterprises
- Code of Ethics and Professional Conduct for Officers and Employees
- Financial Information Disclosure Policy
- Directives:
  - Secure and Acceptable Use of Information and Technology Assets
  - Administrative and Disciplinary Measures for Breaches of the Code of Ethics and Professional Conduct
  - Protection of Personal Information
  - Management of Privileged Information
- Information and Technology Asset Security Operational Guide

OBJECTIVES

- Establish the principles guiding the management framework for the security of CDPQ's information and technology assets
- Promote a healthy cybersecurity risk management culture at all levels of the organization
- Define the stakeholders' roles and responsibilities and the governance structure
- Establish a framework for the main cybersecurity risks to which CDPQ is exposed

1. Definitions

Capitalized terms are defined in this *Information and Technology Asset Security Policy* (the "Policy"). Terms in italics refer to official CDPQ documents.

- Information Asset: Any resource providing Information that is used by CDPQ. This includes Information, Documents, databases and business software packages, or any combination thereof, acquired or developed within CDPQ, whether or not hosted at CDPQ.
- Technology Asset: All computer hardware, software and services used to collect, process and transmit Information Assets. This includes workstations, phones, tablets, keyboards and other data input or output devices. Software includes word processing software, desktop, server and hardware operating systems, business software packages, network management tools, development tools, courseware and device drivers.

- Retention Schedule: A schedule establishing such things as the lifecycle of a document, from its creation to when it must be destroyed or provided to the Bibliothèque et Archives nationales du Québec ("BAnQ") for permanent preservation.
- Cybersecurity: All the processes and means used to ensure the security of CDPQ's Information and Technology Assets against malicious actors, both inside and outside CDPQ. It is intended to protect against the risk of loss or disclosure of CDPQ's sensitive information, as well as the risk of degradation or interruption of CDPQ's critical business functions resulting from a cybersecurity incident.
- Document: Any Information medium, whether paper, electronic, magnetic, optical, wireless or other. The Information is delimited and structured, according to the medium used, by tangible or logical features and is intelligible in the form of words, sounds or images.
- Information: Data, indications, series of information, including Personal Information, recorded by CDPQ in a Document or held by CDPQ, including Information from a third party.
- Person: Any individual who works for CDPQ, full- or part-time, or who has access (onsite or remote) to a CDPQ Information or Technology Asset. This includes, but is not limited to, regular and casual employees, contractors, consultants, students, interns and any other CDPQ worker.
- Data Steward: A person responsible for an Information Asset, as defined in the Policy. This role is granted to the producer of data and/or the owner of a data repository (e.g. SharePoint site) working within the CDPQ's business lines. The Data Steward's responsibilities are defined in the *Governance* section of this Policy.
- Digital Product Manager: Person responsible for a product-type Technology Asset. This includes business applications and digital solutions, developed internally or acquired externally, that are implemented in CDPQ's technology environment to meet its business needs. The Digital Product Manager's responsibilities are defined in the *Governance* section of this Policy.
- Digital Platform Manager: Person responsible for a platform-type Technology Asset. This includes cybersecurity, cloud-based, data, operations and development, integration, and augmented intelligence platforms. The Digital Platform Manager's responsibilities are defined in the *Governance* section of this Policy.

2. Context

Cybersecurity threats are on the rise, constantly evolving, and increasingly complex. This Policy's adoption falls within that context and takes into account the importance for CDPQ of protecting its Information and Technology Assets (the "Assets") and mitigating the risks of cybersecurity incidents it may face.

The Policy applies to any Person who is granted authorized access to CDPQ Assets, and covers all aspects of CDPQ's business operations, activities and functions.

The Policy applies to all CDPQ Assets, whether they are accessed and used on a permanent or occasional basis, whether they are provided by CDPQ internally or as part of contractual commitments, and whether they are commercialized or accessible via the Internet.

3. Guiding principles

3.1 Ownership and responsibility for Information and Technology Assets

CDPQ is the sole owner of any Asset produced or managed by a Person, or to which a Person has access in the course of his or her duties. This includes any Documents and Information produced or received as well as any technology equipment provided to a Person.

This excludes externally sourced Information which, while it must be adequately protected by the Persons accessing it, remains the property of its originator.

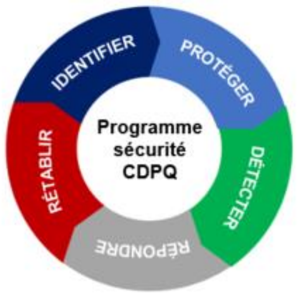
In terms of Asset management, a designated manager (Data Steward, Digital Product Manager or Digital Platform Manager) is associated with each Asset. This manager is assigned when an Asset is created or introduced. This assignment is updated when a designated manager changes position.

The designated manager ensures that, for the Assets under his/her responsibility, the security measures set out in this Policy and its associated frameworks are adhered to and enforced throughout the Assets' lifecycle in order to secure them and mitigate the cybersecurity risks.

3.2 Reference and guidance model

The EVP, Technology uses two recognized reference frameworks to ensure the completeness, appropriateness and consistency of the guidance presented in this Policy and the resulting Directive and Operational Guide. These frameworks are the *National Institute of Standards and Technology Cybersecurity Framework* (NIST-CSF) and ISO 27001.

The NIST-CSF, shown opposite, guides the EVP, Technology in the design of its program and its desire to define, frame, and evolve CDPQ's Asset security behaviors and practices. It is based on the following five pillars:



NIST National Institute of Standards and Technology

1. **IDENTIFY**, categorize and prioritize the cybersecurity risks related to the Assets. This pillar aims to develop a comprehensive picture of the cybersecurity risks, prioritize the actions to be taken based on their evolution, and integrate the risk mitigation actions prioritized in the program. It structures the governance of the cybersecurity program based on an integrated risk management approach, related to the risk appetite monitored and endorsed by the Executive Committee.

2. **PROTECT** the Assets from risks and threats. This pillar aims to implement appropriate safeguards to secure the Information Assets and various layers of the technology environment (e.g., data, application, termination point, network) in order to mitigate the probability and risk of a cybersecurity incident.

3. **DETECT** the events affecting the Assets' security. This pillar aims to develop and implement appropriate activities with the objective of identifying the occurrence of a potential or actual cybersecurity incident. It includes the monitoring mechanisms deployed by CDPQ to verify the effectiveness of the safeguards.

4. **RESPOND** when an event affecting the Assets' security occurs. This pillar aims to develop and implement appropriate processes and activities to react as quickly and effectively as possible to a detected cybersecurity incident, in coordination with the identified internal and external stakeholders. It also aims to enhance CDPQ's ability to contain the impact of a cybersecurity incident.

5. **RECOVER** CDPQ's critical Assets and business processes following an incident. This pillar aims to develop and implement the appropriate activities to maintain CDPQ's resilience plans and restore business functions that may be degraded or interrupted as a result of a cybersecurity incident.

More specifically, the guiding principles to be followed and measures to be implemented in terms of security, inspired by NIST-CSF and ISO 27001, are set out in the following documents:

- The *Secure and Acceptable Use of Information and Technology Assets Directive*, which defines, frames and specifies how Persons should use the Assets.

- The *Information and Technology Asset Security Operational Guide*, which outlines the guiding principles to be followed and measures to be implemented within the Executive Vice-Presidency, Technology to protect the Assets and mitigate the risks of cybersecurity incidents that CDPQ may face.

3.3 Adoption of secure behaviours and monitoring

All Persons are required to use the Assets in a responsible and secure manner by applying the rules set out in the *Secure and Acceptable Use of Information and Technology Assets Directive*.

The Cybersecurity Department is responsible for the cybersecurity training and awareness program to develop a CDPQ cybersecurity culture. This program aims to reinforce in all Persons their responsibility for cybersecurity and clarify the role they must play to minimize this risk.

The EVP, Technology has monitoring mechanisms in place to identify behaviour that violates the guiding principles and obligations detailed in its frameworks. If the EVP, Technology detects an actual or potential situation of non-compliance, it reserves the right, with the support and agreement of the Legal Affairs and Secretariat group and Talent and Performance group, to investigate the event and take action based on the criteria set out in the *Administrative and Disciplinary Measures for Breaches of the Code of Ethics and Professional Conduct Directive*.

3.4 Protection of Personal Information

The access to and collection, use, retention, communication and destruction of Personal Information must comply with the applicable laws. The *Protection of Personal Information Directive* sets out guidelines to follow in managing Personal Information.

In order to abide by its legal obligations for protecting Personal Information and managing Documents, in particular under the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the “Act respecting Access”), the EVP, Technology has adopted a Classification Plan[1] and Retention Schedule[2]. All Documents must be classified according to this Plan and retained in accordance with the Retention Schedule.

4. Penalties for failure to comply with the Policy

A breach of the Policy can have a significant impact on CDPQ's legal and reputational liability and operations. Consequently, failure to comply with the Policy may result in penalties, which are based on the seriousness of the act. These penalties are imposed in accordance with the *Administrative and Disciplinary Measures for Breaches of the Code of Ethics and Professional Conduct Directive* and may include dismissal.

5. Governance

- The Board of Directors:
  - Reviews and approves the Policy;
  - Ensures that CDPQ management allocates the necessary human and financial resources to implement the Policy.

- The EVP, Technology:
  - Defines, maintains and ensures compliance with the Policy.

- The Operational Risk Committee (ORC):
  - Reviews and approves the *Secure and Acceptable Use of Information and Technology Assets Directive* and *Information and Technology Asset Security Operational Guide* as well as the objectives and scope of the standards that detail the parameters, specific requirements and implementation specifics of the Operational Guide;
  - Endorses CDPQ's risk assessment criteria and risk appetite with respect to cybersecurity;

[1] The Classification Plan can be viewed here.

[2] The Retention Schedule can be viewed here.

  - Monitors the evolution of the cybersecurity posture with respect to CDPQ's cybersecurity risk appetite.

- Risk Management and Depositor Relations:
  - Supports the Cybersecurity Department in monitoring its priority risks;
  - Conducts an objective review of cybersecurity activities.

- The Global Security Committee (GSC):
  - Provides the vision and strategic direction for cybersecurity and ensures alignment of the decisions made with CDPQ's risk appetite;
  - Confirms the objectives, priorities and directions of CDPQ's cybersecurity program;
  - Monitors the execution of CDPQ's cybersecurity program transformation initiatives and the evolution of the resulting cybersecurity posture;
  - Endorses the security standards for Information and Technology Assets as well as the cybersecurity postures resulting from the Policy;
  - Tracks the major cybersecurity incidents, exemptions and exclusions, performance indicators and progress of the cybersecurity culture program.

- The Access to Information and Privacy Committee:
  - Defines, maintains and ensures compliance with the *Protection of Personal Information Directive*;
  - Approves the governance rules that CDPQ must adopt with respect to Personal Information.

- The Cybersecurity Department:
  - Provides a comprehensive picture of the cybersecurity risks, prioritizes the actions to be taken based on their evolution, and integrates the risk mitigation actions prioritized in CDPQ's cybersecurity program;
  - Plans and deploys the program to develop a cybersecurity culture, including the associated training and awareness activities;
  - Develops and implements the:
    - Safeguards required to protect CDPQ's Information and Technology Assets and thus limit the risk of a cybersecurity incident;
    - Appropriate activities with the objective of identifying the occurrence of a potential or actual cybersecurity incident;
    - Appropriate processes and activities to react as quickly and effectively as possible to a detected cybersecurity incident, in coordination with the identified internal and external stakeholders;
  - Defines, maintains and ensures compliance with the Directive, Operational Guide and standards derived from the Policy.

- The Data Stewards, Digital Product Managers and Digital Platform Managers:
  - Apply the security measures set out in this Policy and the resulting Directives throughout the lifecycle of the Assets for which they are responsible;
  - Determine the specific security requirements for the Assets for which they are responsible, which must be consistent with the normative framework;
  - Determine the classification rating or categorization of the Assets for which they are responsible and periodically review this classification and the security level;

- Approve the assignment of access rights for the Assets for which they are responsible, based on the requirements.

6. Audit and control

CDPQ has in place a specific control process to monitor and review the performance and effectiveness of the security frameworks and measures and to verify compliance with the legal and regulatory requirements. It includes adapted testing and controls conducted by the Cybersecurity Department at its discretion.

The lessons learned from these controls and audits are applied to ensure systematic treatment and guide the actions of the Information and Technology Asset security Policy and management framework.

7. Review

This Policy is reviewed at least every three years.

Initial approval date: 2015-06-16

Date of revision: 2018-06-12; 2022-06-10