Caisse de dépôt et placement
du Québec

INFORMATION MANAGEMENT AND SECURITY POLICY

Objectifves

- Provide a framework for managing information in accordance with the relevant legislation and regulations
- Promote the effective, appropriate and secure use of information resources
- Provide management for accurate and comprehensive tracking of information

TABLE OF CONTENTS

1. DEFINITIONS

The italicized terms in this policy are defined in Appendix 1.

2. SCOPE

Information management and security are established in consideration of the type of information and the information resource using it.

CDPQ holds confidential, personal, privileged and public information. There are three major types of information resources within CDPQ: employees, documents and technological tools.

This policy lays out the management and access to information principles and identifies the appropriate and secure use of documents and technological tools carrying information. It is supplemented by the Information Resource Management and Security Directive (IT and Documentation) ("the Directive") and by the Protection of Personal Information Directive.

2.1. Other Caisse regulations involving information

The rules regarding employees as well as the information they obtain within the scope of their work are set out in the Code of Ethics and Professional Conduct for Officers and Employees ("the Code").

In addition, the Code and the Restricted Transaction Securities Directive provide specific measures for handling confidential and privileged information.

Lastly, the manner in which CDPQ discloses information on itself to the media and the public is set out in the Financial Information Disclosure Policy.

3. GOVERNANCE

This policy has been approved by CDPQ's Management Committee.

Directives stemming from this policy may be adopted. They are approved by the IT Strategic Committee or the Operational Risk Committee, depending on the topic covered.

Furthermore, in order to comply with the Act respecting the governance and management of the information resources of public bodies and government enterprises, the IT Strategic Committee must ensure the implementation of the following planning and management tools:

- An information resource master plan;
- A program for investing in and spending on information resources (three-year plan);
- An inventory of informaiton assets, including an assessment of their conditions (debt register);
- An overview of the workforce and use of consultants assigned to information resources;
- An overview of the use of amounts allocated to investments and information resource expenses.

The Executive Vice-Presidents of Legal Affairs and Secretariat and Operations and Information Technology share responsibility for this policy and the directives stemming from it.

4. PRINCIPLES

4.1. Ownership

Any information produced or received by an employee as part of his or her duties is Caisse property.

4.2. Caution and diligence

Given the strategic nature of Caisse business, any employee with access to information must act with care and diligence, taking into account the nature of the information involved.

4.3. Principle of least privilege

Rights to access information, including personal information, are attributed to employees based on what is needed in carrying out their duties and in accordance with the relevant legislation.

4.4. Segregation of incompatible functions

A single employee may not, by virtue of his or her responsibilities and with the help of the employee's access to information resources, control all phases of a process and therefore have the ability to conceal or delay the discovery of a prejudicial situation.

4.5. Classification

All information must be classified and saved in a manner in which it can be tracked, in accordance with CDPQ's classification plan.

4.6. Technological innovation

As long as the management and security of information is ensured, CDPQ promotes the implementation of innovative technological tools that make its management more effective and efficient and facilitates the accountability of employees in their day-to-day use of information resources.

5. MANAGING THE SECURITY OF INFORMATION RESOURCES

A process for managing the security of information resources has been established to ensure the availability, integrity, confidentiality, authenticity and irrevocability of documents and technological tools throughout their life cycle.

5.1. Analyzing security risks

The process for the security and management of information resources is based on an analysis of the security risks that might affect CDPQ's documents or technological tools. The analysis takes into account such things as the type of information conveyed by the information resource, the probability of occurrence of the risk and its potential impact.

5.2. Security master plan

A security master plan stems from the analysis of security risks. The plan provides for the implementation of measures to mitigate security risks.

CDPQ's Executive Committee carries out an annual review of the security risk analysis and the effectiveness of the mitigation measures and adjusts its master plan accordingly. The annual review includes analyses of the gaps in security directives, results of audit work and internal and external vulnerability tests.

5.2.1. Safeguards

The security measures applied to information resources are managed and applied during the life cycle of a document or technological tool, from its acquisition or development, to its use, replacement, storage or destruction.

CDPQ uses a variety of security measures such as the use of passwords, the preventive monitoring of security risks, and measures for the encryption of information in transit or electronically transferred.

The Directive provides guidelines for all employees on the implementation of security measures. Other security measures are set out in the security directives specifically addressing CDPQ's technology teams.

5.2.2. Identity and access management

Management of the identity of employees and their access to information resources is based on the principles of "segregation of incompatible functions" and "least privilege."

This management is centralized under the Chief Operations and IT Officer and the Records Management team.

5.2.3. Centralized management of incidents and exceptions

CDPQ's information security team is responsible for all security incidents, all exceptional measures and all requests for exemption to a security measure.

5.3. CDPQ's managerial right

As an employer, CDPQ has a right to examine its employees' use of the information resources it makes available to them. CDPQ can intervene when it detects actual or potential non-compliance with its policies or directives. In that regard, employees should refer to the Code and the Directive for rules on the proper use of information resources.

5.4. Business continuity

All information resources and physical infrastructure that are crucial to CDPQ's critical business in the event of a disaster or major crisis must be listed and subject to appropriate protection and availability measures. Reporting on this matter is provided to the IT Strategic Committee.

6. TECHNOLOGICAL TOOLS

6.1. Approval and accountability processes

CDPQ has a three-year plan for projects and activities affecting technological tools and establishes the resulting budget. An annual plan of projects and activities as well as the allocated budget are also adopted.

The IT Strategic Committee reviews each project and ensures the accountability of all projects on an annual basis.

6.2. Allocation

The IT team makes available to employees the technological tools required to efficiently perform their work. It also provides the support required for the technological tools to work properly.

Employees must refer to the Directive for the rules of use for the technological tools.

6.3. Use of personal technology devices

CDPQ allows employees to use their personal technology devices to access its visitor network. This network no longer provides access to CDPQ's systems, applications, data, and so on, but rather to basic services such as the Internet. The conditions for using personal technology devices are set out in the Directive.

6.4. Inventory

CDPQ continually updates an inventory of technological tools, including information on where the tools can be found and the person who is responsible for them and who authorizes access to them.

7. DOCUMENTS

7.1. Classification plan and retention schedule

In order to abide by its legal obligations for information management under the Archives Act and the Act respecting Access to documents held by public bodies and the Protection of personal information (the "Act respecting Access"), CDPQ has adopted a classification plan and retention schedule. All documents must be listed according to the classification plan and retained in accordance with the retention schedule.

7.2. Document management in the case of disputes or requests for access to information

All documents involved in a dispute or request for access to information, or in cases where there is reason to believe that a file might be disputed, are retained regardless of the timelines set out in the retention schedule.

7.3. Technological tools for managing documents

The technological tools used for document management must ensure the preservation, integrity and security of all files and documents and allow for specific and extensive research to be conducted on them.

8. PUBLIC ACCESS TO DOCUMENTS AND THE PROTECTION OF PERSONAL INFORMATION

8.1. Right of public access

Every person who makes a request has a right of access to Caisse *documents*, except with respect to the exemptions contained in the Act respecting Access, which, in CDPQ's view, are of two key types:

- personal information;
- strategic, financial or business information.

This right does not extend to personal notes written on a document or to sketches, outlines, drafts, preliminary notes or other documents of the same nature.

The Directive sets out how requests for access are to be processed. An employee who receives a request for access must forward it without delay to the person at CDPQ responsible for matters under the Act respecting Access (Senior Vice-President, Compliance and Responsible Investment), in accordance with the terms of the Directive.

8.2. Control of personal information

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

An access to information and privacy committee is in place to:

- review procurement, development and redesign projects for any technological tool that uses, collects, saves, communicates or destroys personal information and to suggest those that should be controlled by special protection measures;
- establish special privacy measures that must be adhered to when conducting surveys or using video surveillance technology;
- keep abreast of electronic services for collecting, using, saving, communicating or destroying personal information.

9. PENALTIES FOR FAILURE TO COMPLY WITH THE POLICY

Failure to comply with this policy, including through the unauthorized use, modification, destruction, distribution or disclosure of information, may result in penalties, which will be based on the seriousness of the act. Such penalties can be as severe as dismissal.

10. PROCESSES FOR ADOPTING AND UPDATING THE POLICY

This policy is submitted to the Management Committee for approval. It must be revised every three years, unless it is necessary to do so earlier.

APPENDIX 1: DEFINITIONS

- **Retention schedule**: A schedule establishing such things as the life cycle of a document, from the time it was created to the time it must be destroyed or provided to the Bibliothèque et Archives nationales du Québec for permanent preservation.
- **Code**: CDPQ's Code of Ethics and Professional Conduct for Officers and Employees
- **Directive**: CDPQ's Information Resource Management and Security Directive (IT and Documentation).
- **Document**: Any data 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.
- **Active document:** Any document regularly consulted by one or more employees.
- **Employee**: Any person working for CDPQ on a full- or part-time basis, as a regular or casual employee, including trainees and students.
- **Document management**: All of the activities, systems, technical means, and methods that can be used to create, receive, classify, save, locate or use documents until such time as they are destroyed or provided to the Bibliothèque et Archives nationales du Québec.
- **IT team**: Based on the situation, the Chief Operations and IT Officer, Vice-President, Operations, Vice-President, Planning, Architecture and Governance, and the managers of information resources.
- **Information**: Data, indications, a series of information, including personal information, recorded by CDPQ in a document or held by CDPQ, including information from a third party. Information can be:
  - **Confidential information**: Any information concerning CDPQ, information on industry or sector trends or any information of a strategic nature that is not public knowledge and that, if it were known by a person other than an employee, would be likely to give the person in question an advantage or compromise the carrying out of an activity in which CDPQ is involved. Confidential information also includes all information relating to investments or to legal persons, companies and investment funds in which CDPQ holds or is considering holding an interest, including information from a third party.
  - **Privileged information**: Any information not yet publicly known and likely to affect the decision of a reasonable investor or to have a significant influence on the value or price of shares of a company that has made an initial public offering. All privileged information is considered confidential. See the Code for a more comprehensive definition.
  - **Public information**: Information that, even if it were known by a person other than an employee, would not likely give the person in question an advantage or compromise the carrying out of an activity in which CDPQ is involved.
  - **Personal information**: See the definition of Personal Information and Personal Information That Is Public
- **Act respecting Access:** The Act respecting Access to documents held by public bodies and the Protection of personal information.
- **Technological tools**: All of the information technology equipment (including smart devices), systems, applications, networks, models (e.g. cloud computing) and other similar components as well as the networks, infrastructure and any technology component used to provide telephone service or access to the Internet or CDPQ's intranet and extranet.

- **Classification plan**: A document establishing the hierarchical and logical structure of files based on Caisse business. It defines where employees must file documents to allow their retrieval.
- **Information**: Indication, specification that is provided or obtains about someone or something.
  - **Personal information**: Information concerning a natural person that allows the person to be identified.
  - **Personal information that is public**: Personal information as defined in section 57 of the Act respecting Access, namely the name, title, duties, classification, salary (or salary scale, as applicable), address and telephone number at work of an employee of CDPQ.
- **Information resources**: The set of resources providing various types of information that are used by CDPQ in carrying out its mandate. Information resources include human, material and technological resources.