Rules governing personal information

As part of its mission, the Chambre de la sécurité financière (the "**CSF**") collects and uses personal information. The CSF is an organization subject to the *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1 (the "**Access Act**"). In compliance with the Access Act, the CSF must ensure the personal information it holds is protected.

These Rules governing personal information (the "**Rules**") have been approved and recommended by the CSF's Committee on access to information and the protection of personal information.

These Rules apply to all personal information held by the CSF and to anyone who processes this personal information. Anyone who processes personal information in the performance of their duties or in their relationship with the CSF is bound to protect this personal information.

1. Collection, use and release of personal information

The CSF implements the best practices in terms of protecting personal information.

a. Type of personal information that may be collected

The CSF collects personal information as part of its mission to ensure the protection of the public by overseeing the professional development, ethics and discipline of its members. It only collects what is required in the performance of its duties and for implementing programs to provide services and pursue its mission, in particular personal information concerning members of the CSF, employees, members of the board of directors and members of the discipline committee.

The CSF takes appropriate measures to ensure it collects personal information in a way that is adequate, relevant and not excessive.

When it collects personal information, and thereafter upon request, the CSF notifies the persons concerned about the following: the purposes for which the personal information is collected; the categories of persons who will have access to this personal information; and the rights of access and correction set forth by the *Access Act.*

b. Use of personal information

The use of personal information means the moment when this information is used by persons authorized within the CSF.

Access to personal information will be limited to employees who are qualified to receive personal information within the CSF when this personal information is necessary in the performance of their duties.

The CSF will limit the use of personal information only to the purposes for which it was collected. To use this information for other purposes, the CSF must obtain your consent, unless otherwise permitted by the Access Act.

c. Releasing personal information

At this step, the CSF will ensure to obtain the consent of persons concerned in order to release their information to a third party, unless otherwise permitted by the Access Act. Express consent must be obtained in the event where sensitive personal information is involved. The CSF will comply with its obligations set forth by the Access Act when releasing personal information without the consent of the person concerned.

When the CSF releases personal information to a mandatary or a service provider as part of a mandate or service contract, it will enter into an agreement with this mandatary or service provider that outlines the obligations pertaining to the protection of personal information. Before the personal information is released outside Quebec, the CSF will make sure that the information will benefit from a level of protection that is equal to the protection guaranteed by the Access Act.

d. Consent

Subject to the provisions of the Access Act, the CSF will obtain the consent of persons concerned for the collection, use and release of their personal information. This consent must be clear, free, informed and given for specific purposes, in clear and simple language. The consent is only valid for the time necessary to achieve the purposes for which it was requested.

The person concerned will therefore have access to all the information necessary to make an informed decision. Consent may be withdrawn at any time after it was given. This is namely the case for promotional offers. In these cases, we will process your request as soon as possible.

In some circumstances described by the Access Act, the CSF will be able to use and release personal information collected without the consent of the person concerned.

e. Keeping and destruction

The CSF will keep the personal information it collects in compliance with applicable laws and its retention schedule. Personal information will be kept and archived in Canada.

The CSF will ensure that the personal information it keeps is up to date, accurate and complete in order to serve the purposes for which it was collected or used. The CSF will

also take all the appropriate security measures to ensure the protection of the personal information it keeps.

When the purposes for which the personal information was collected or used have been achieved, the CSF will destroy the information in a secure manner or anonymize it to use it for public interest purposes, subject to applicable laws and as per its retention schedule.

2. Obligations, roles and responsibilities

The CSF's roles and responsibilities in terms of the security and protection of personal information are defined for each level of management within the CSF and for each area pertaining to the security and protection of information.

a. The CSF's executive committee

i) Approves the Rules governing personal information, the Terms of Use of its website and the Privacy Policy as well as any amendments made to these documents;

ii) Ensures the CSF's managers apply and comply with these documents;

iii) Approves the measures aimed at promoting the Rules governing personal information, the Terms of Use of its website and the Security of Information Policy as well as the legal obligations of the CSF in terms of the protection and security of information;

iv) Approves the strategic guidelines pertaining to the protection and security of information;

v) Approves action plans and receives quarterly reports on the protection and security of information.

b. President and CEO

i) As the person exercising the highest authority within the CSF, the President and CEO defines the values and guidelines in terms of the protection and security of information and ensures compliance with applicable laws, policies and guidelines pertaining to the protection and security of information;

ii) Designates the Person in charge of access to document and the protection of personal information.

c. The CSF's person responsible for security of information

i) Consults the CSF's executive committee when establishing strategic guidelines and priorities;

ii) Ensures the implementation of the regulatory framework for information resources and risk mitigation measures;

iii) Ensures information assets remain protected throughout their lifecycle by deploying the appropriate security and protection measures that have been approved by information system owners/managers;

iv) Makes sure that provisions pertaining to the security and protection of the CSF's information are included in contracts and agreements involving the CSF;

v) Acts as the CSF's first responder in terms of the protection and security of information;

vi) Ensures that background checks for candidates applying to positions with high access to information are carried out and if needed, ensures that background checks for members of staff or consultants involved in the security of information are carried out;

vii) Ensures the robustness of the network is periodically tested;

viii) Ensures they have an inventory of systems;

ix) Enforces the appropriate sanctions in the event of violations of policies, regulations, guidelines and codes of conduct pertaining to the protection and security of information;

x) Is responsible for producing status reports;

xi) Is responsible for ensuring the application of the Rules governing personal information, the Terms of Use of the website and the Security of Information Policy;

xii) Identifies information system owners/managers.

d. Person in charge of access to information and the protection of personal information

i) The Person in charge of access to documents and the protection of personal information ensures compliance with the Access Act.

e. Information system managers

Every information system manager must:

i) Ensure the accessibility, appropriate use, efficient management and security of information assets under their control;

ii) Help categorize the information under their control and ensure this information is protected.

f. System users

i) Comply with these Rules governing personal information, the Terms of Use of the website, the Security of Information Policies and any other guideline pertaining to the security of information and use of information assets;

ii) Comply with security measures in effect without bypassing, disabling or modifying them;

iii) Employee users must complete each information security awareness course under the terms of the CSF's awareness program.

g. Employees.

Employees of the CSF who have access to personal information in the performance of their duties must:

- preserve the confidentiality of the information;
- immediately notify their supervisor and the Person in charge of access to documents and the protection of personal information of situations where the confidentiality of personal information may have been compromised.

3. Committee on access to information and the protection of personal information

The CSF has created a Committee on access to information and protection of personal information (the "**Committee**") that is responsible for supporting the CSF in its responsibilities and obligations under the Act.

More specifically, the Committee supports the Person in charge of access to documents and the protection of personal information in their duties and obligations under the Access Act, namely for:

- defining guidelines and issuing recommendations in terms of protecting personal information;
- approving the rules governing the CSF with respect to personal information;
- keeping track and updating the document pertaining to the Terms of Use of the website and these Rules;
- being consulted at the beginning of any project to acquire, develop or overhaul an information system or electronic service delivery involving the collection, use, release, keeping or destruction of personal information, for the purposes of carrying out a privacy impact assessment;
- keeping track of the register of confidentiality incidents.

4. Managing access to personal information

The CSF limits access to personal information. It only authorizes access to members of its staff who need this information in the performance of their duties. Moreover, the CSF authorizes access while taking into account the sensitivity of the personal information.

The CSF also carries out follow ups to review and revoke access based on the need to access personal information. The CSF also ensures that this information is only used for the purposes identified or authorized.

5. Release of personal information as part of a contract

In some situations, personal information may need to be released. For instance, when hiring staff or during security inquiries.

When personal information is released, the CSF will require concerned providers to fill out a cybersecurity form or to send proof of certification (ex.:ISO27001). The risk and threat analysis as per the form must be to the full satisfaction of the CSF. Providers concerned must also sign a confidentiality agreement.

When personal information is released to a mandatary or service provider as part of a mandate or service contract without the consent of the person targeted, the CSF will record this release in a register.

6. Privacy impact assessment:

The CSF will carry out a privacy impact assessment ("PIA") in the following instances:

- During projects to acquire, develop or overhaul an information system or electronic service delivery involving the collection, use, release, keeping or destruction of personal information;
- When personal information is released outside Quebec;
- When personal information is collected in collaboration;
- When personal information is released under article 68 of the Access Act;
- For study or research purposes or for the production of statistics.

The PIA takes into account the sensitivity of personal information, the purposes for which it is used, its quantity, its distribution, the medium on which it is stored and the proportionality of the measures recommended to protect the information. In the case where personal information must be released outside Quebec, the PIA will take into account protection measures such as contractual measures and the applicable legal regime in the jurisdiction where the information would be released, including any applicable privacy principles.

The Committee on access to information and the protection of personal information will be consulted at the start of any PIA.

7. Complaints Handling Procedure

The CSF has implemented a procedure to handle complaints submitted by consumers and members.

Any complaint pertaining to the protection of personal information must be submitted to the CSF as per the Complaints Handling Procedure.

Complaints pertaining to our personal information protection practices, including the ways in which we use your personal information, will be handled by the CSF's Person responsible for access to information and privacy who must issue a response within 30 days.

8. Managing confidentiality incidents

For the purposes outlined herein and in accordance with article 63.9 of the Access Act, a "confidentiality agreement" is defined as access, use or release not authorized by law of personal information, the loss of personal information or breach of the protection of a personal information.

In the event of a breach of confidentiality, a security incident is opened using the CSF's ticketing system. The Committee will assess the criteria to determine if a confidentiality incident has occurred. If the CSF has reasons to believe that a confidentiality incident involving personal information has taken place, it will carry out a diagnosis and take the measures necessary to diminish the risk of injury and prevent any other incidents from occurring. The incident must be recorded in the Register of confidentiality incidents.

If the incident presents a risk of serious injury, the CSF must notify the *Commission d'accès à l'information* as well as any person whose personal information is concerned by the incident. To determine if there is a risk of serious injury, the CSF, in consultation with the Person responsible for access to information and privacy, will take the following into consideration:

- The sensitivity of the information concerned
- The anticipated consequences of its use
- The likelihood that such information will be used for injurious purposes

9. Register of confidentiality incidents

The Person responsible for access to information and privacy or the person who is responsible for this task, will maintain a Register of confidentiality incidents that includes the following:

- Date of the event (date or period when the incident took place) or if this date is unknown, an approximate date;
- Date the CSF was made aware of the incident;
- Description of the circumstances of the incident;
- Description of the information targeted by the incident, or if unknown, the reason justifying why it is impossible to provide this description;
- Number of persons concerned by the incident or if unknown, an approximate number;
- Description of the elements that led the CSF to conclude whether or not a risk of serious injury exists;
- Date the notice was sent to the *Commission d'accès à l'information*, if there is a risk of serious injury;
- Measures the CSF has taken to mitigate the risks of injury.

The information in the Register will be updated and kept by the CSF for a minimum of 5 years after the date or period during which the CSF became aware of the incident.

10. Training and awareness activities

Every CSF employee must periodically follow and successfully complete training activities pertaining to cybersecurity led by an expert third party hired by the CSF. These training activities are intended to raise awareness about cybersecurity.

11. Surveys

The CSF occasionally surveys its members and consumers as part of its mission. The CSF only collects personal information necessary for this purpose. When the CSF retains the services of third-party providers, it will conduct a risk and threat analysis via a cybersecurity form or will validate the third-party's certifications. The CSF takes the appropriate protection measures with respect to the personal information collected or used as part of its surveys. The CSF has adopted an internal governance rule that includes an assessment required to conclude a survey is necessary as well as an assessment of the ethics of conducting a survey taking into account the sensitivity of the personal information collected and the purposes for which it is used.