RÈGLEMENT SUR LA GESTION ET LE SIGNALEMENT DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION DE CERTAINES INSTITUTIONS FINANCIÈRES ET DES AGENTS D'ÉVALUATION DU CRÉDIT

Loi sur les agents d'évaluation du crédit
(chapitre A-8.2, a. 66 et 73)

Loi sur les assureurs
(chapitre A-32.1, a. 485 et 496)

Loi sur les coopératives de services financiers
(chapitre C-67.3, a. 601.1 et 601.9)

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2, a. 43, par. u) et a. 45.9)

Loi sur les sociétés de fiducie et les sociétés d'épargne
(chapitre S-29.02, a. 277 et 286)

CHAPITRE I
CHAMP D'APPLICATION ET INTERPRÉTATION

1. Le présent règlement s'applique aux institutions financières suivantes :

1° un assureur autorisé en vertu de la Loi sur les assureurs (chapitre A-32.1) et une fédération de sociétés mutuelles visée par cette loi;

2° une fédération et une caisse qui n'est pas membre d'une fédération, visées par la Loi sur les coopératives de services financiers (chapitre C-67.3);

3° une institution de dépôts autorisée en vertu de la Loi sur les institutions de dépôts et la protection des dépôts (chapitre I-13.2.2);

4° une société de fiducie autorisée en vertu de la Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02).

Il s'applique également à un agent d'évaluation du crédit désigné en vertu de la Loi sur les agents d'évaluation du crédit (chapitre A-8.2).

2. Pour l'application du présent règlement, on entend par « incident de sécurité de l'information » une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent.

CHAPITRE II
GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

SECTION I
POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

3. Une institution financière ou un agent d'évaluation du crédit doit établir et mettre en œuvre une politique de gestion des incidents de sécurité de l'information qui comporte, notamment, des procédures et des mécanismes permettant de détecter et d'évaluer les incidents de sécurité de l'information ainsi que d'y répondre, lorsque ces incidents surviennent au sein de l'institution, d'une caisse membre d'une fédération, de l'agent ou d'un tiers à qui cette institution, cette caisse ou cet agent a confié l'exercice de toute partie d'une activité.

La politique de gestion des incidents de sécurité de l'information comporte également une procédure de signalement des incidents de sécurité de l'information aux dirigeants ou, selon le cas, au gestionnaire de l'institution financière ou de l'agent d'évaluation du crédit, y compris une procédure de signalement à ceux-ci lorsque cet incident survient au sein d'une caisse membre d'une fédération ou d'un tiers visé au premier alinéa.

En outre, la politique doit prévoir une procédure de signalement à toute autre partie prenante, notamment aux clients, aux tiers à qui cette institution ou cet agent a confié l'exercice de toute partie d'une activité, aux consommateurs, à l'Autorité des marchés financiers de même qu'aux autres organismes de réglementation.

4. Une institution financière ou un agent d'évaluation du crédit doit désigner, par écrit, un de ses dirigeants ou, dans le cas d'une coopérative de services financiers, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information.

SECTION III
SIGNALEMENT À L'AUTORITÉ DES MARCHÉS FINANCIERS

5. Une institution financière ou un agent d'évaluation du crédit doit signaler à l'Autorité tout incident de sécurité de l'information ayant un risque d'occasionner des répercussions négatives qui a été signalé à ses dirigeants ou, selon le cas, à ses gestionnaires au plus tard 24 heures suivant cet incident.

L'institution financière ou l'agent d'évaluation du crédit doit aussi signaler à l'Autorité, dans ce même délai, tout incident de sécurité de l'information qui a été signalé à un organisme de réglementation, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, ou, contractuellement, est chargé de dédommager le préjudice qui aurait pu être causé par cet incident.

6. Une institution financière ou un agent d'évaluation du crédit doit, lorsqu'il avise la Commission d'accès à l'information, instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), d'un incident de confidentialité visé au deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), le signaler au même moment à l'Autorité.

7. Une institution financière ou un agent d'évaluation du crédit signale à l'Autorité un incident de sécurité de l'information en remplissant le formulaire disponible sur le site Web de l'Autorité.

8. Une institution financière ou un agent d'évaluation du crédit doit aviser l'Autorité de l'évolution de la situation au plus tard 3 jours suivant l'avis visé à l'article 5 et au plus tard tous les 3 jours suivant l'avis précédent jusqu'à la clôture de l'incident.

9. Dans les 3 jours suivants la clôture de l'incident, une institution financière ou un agent d'évaluation du crédit transmet à l'Autorité un avis confirmant que l'incident est maîtrisé et que les activités ont repris leur cours normal.

10. Une institution financière ou un agent d'évaluation du crédit transmet à l'Autorité un rapport dans un délai de 30 jours suivant la clôture de l'incident de sécurité de l'information. Le rapport contient, notamment, les éléments suivants :

1° l'identification de la source et du type d'incident;

2° l'appréciation de l'institution financière ou de l'agent d'évaluation du crédit quant à la récurrence potentielle de l'incident;

3° les moyens pris pour réduire la probabilité que de nouveaux incidents de même nature ne se produisent.

SECTION IV
REGISTRE DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

11. Une institution financière ou un agent d'évaluation du crédit doit tenir à jour un registre des incidents de sécurité de l'information qui comprend, pour chaque incident :

1° la date et l'heure de celui-ci;

2° sa localisation;

3° sa nature;

4° une description détaillée de celui-ci, incluant les renseignements contenus au paragraphe 2° de l'article 10;

5° les préjudices engendrés par celui-ci;

6° les tiers concernés par l'incident;

7° les actions prises;

8° l'acceptation ou non du risque résiduel et les justificatifs afférents;

9° les actions prévues;

10° la date de sa clôture.

12. Une institution financière ou un agent d'évaluation du crédit doit conserver les renseignements consignés au registre de manière sécurisée et confidentielle, afin d'en maintenir l'intégrité pour une période minimale de 7 ans à compter de la date du rapport visé à l'article 10.

CHAPITRE III
SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

13. Une sanction administrative pécuniaire d'un montant de 250 $ dans le cas d'une personne physique ou de 1 000 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit visé à l'article 1 :

1° qui, en contravention à l'article 4, n'a pas désigné, par écrit, un de ses dirigeants ou, selon le cas, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information;

2° qui, en contravention de l'article 5, ne signale pas à l'Autorité un incident au plus tard 24 heures suivant cet incident;

3° qui, en contravention à l'article 6, ne transmet pas à l'Autorité le signalement prévu à cet article au moment où un avis est transmis à la Commission d'accès à l'information;

4° qui, en contravention à l'article 8, n'avise pas l'Autorité de l'évolution de la situation, au plus tard 3 jours suivant l'avis visé à l'article 7 et au plus tard tous les 3 jours suivant l'avis précédent, jusqu'à la clôture de l'‘incident;

5° qui, en contravention à l'article 9, ne transmet pas à l'Autorité un avis conforme à cet article, dans les 3 jours suivant la clôture d'un incident de sécurité de l'information.

14. Une sanction administrative pécuniaire d'un montant de 500 $ dans le cas d'une personne physique ou de 2 500 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit l'entité visée à l'article 1 :

1° qui, en contravention à l'article 3, n'établit pas ou ne met pas en œuvre une politique de gestion des incidents de sécurité de l'information;

2° qui, en contravention à l'article 11, ne tient pas à jour un registre des incidents de sécurité de l'information;

3° qui, en contravention à l'article 12, ne conserve pas les renseignements au registre des incidents de sécurité de l'information pour une période minimale de 7 ans à compter de la date du rapport visé à l'article 10.

CHAPITRE IV
DISPOSITION FINALE

15. Le présent règlement entre en vigueur le (*indiquer ici la date d'entrée en vigueur du présent règlement*).