Caisse de dépôt et placement du Québec

POLITIQUE – GESTION ET SÉCURITÉ DE L'INFORMATION

Objectifs

- Encadrer la gestion de l'information conformément aux lois et règlements en la matière
- Promouvoir une utilisation efficace, appropriée et sécuritaire des ressources informationnelles
- Assurer une gestion permettant le repérage précis et complet de l'ensemble de l'information

TABLE DES MATIÈRES

1. DÉFINITIONS

Dans la présente politique, les termes commençant par une majuscule ont été définis à l'annexe 1.

2. PORTÉE

La gestion et la sécurité de l'Information sont établies en tenant compte de la nature de l'Information et de la Ressource informationnelle qui l'utilise.

La Caisse détient de l'Information de nature confidentielle, personnelle, privilégiée ou publique. Il existe par ailleurs au sein de la Caisse trois grands types de Ressources informationnelles : les Employés, les Documents et les Outils technologiques.

La présente politique énonce les principes de gestion et d'accès à l'Information et détermine l'utilisation appropriée et sécuritaire des Documents et des Outils technologiques qui transportent de l'Information. Elle est complétée par la Directive – Gestion et sécurité des ressources informationnelles (TI et Documents) (la « Directive ») et par la Directive – Protection des renseignements personnels.

2.1. Autres encadrements Caisse touchant l'Information

Les règles relatives aux Employés ainsi qu'à l'Information qu'ils obtiennent dans le cadre du travail sont prévues au Code.

En outre, le Code et la directive - Titres à transactions restreintes prévoient des mesures spécifiques relatives au traitement de l'Information confidentielle et privilégiée.

Enfin, la façon dont la Caisse divulgue aux médias et au public une Information la concernant est énoncée à la politique – Divulgation de l'information financière.

3. GOUVERNANCE

La présente politique est approuvée par le comité de gestion de la Caisse.

Des directives découlant de la présente politique peuvent être adoptées. Elles sont approuvées par le comité stratégique TI ou par le comité risques opérationnels, selon le sujet abordé.

Par ailleurs, pour se conformer à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics*, le comité stratégique TI doit s'assurer de la mise en place des outils de planification et de gestion suivants :

- un plan directeur en ressources informationnellles;
- une programmation des investissements et des dépenses en ressources informationnelles (plan triennal);
- un inventaire des actifs informationnels, incluant une évaluation de leur état (registre de la dette);
- un portrait de la main-d'œuvre et du recours à des consultants affectés aux ressources informationnelles;
- un portrait de l'utilisation des sommes consacrées aux investissements et aux dépenses en ressources informationnelles.

Les premières vice-présidences Affaires juridiques et secrétariat ainsi qu'Opérations et TI se partagent la responsabilité de la présente politique et des directives qui en découlent.

4. PRINCIPES

4.1. Propriété

Toute Information produite ou reçue par un Employé dans le cadre de son travail est la propriété de la Caisse.

4.2. Prudence et diligence

Compte tenu de la nature stratégique des activités de la Caisse, tout Employé qui a accès à de l'Information, doit agir avec prudence et diligence, en tenant compte de la nature de l'Information en cause.

4.3. Droit d'accès minimal

Les droits d'accès à une Information, y compris aux Renseignements personnels, sont attribués aux Employés en fonction de ce qui leur est nécessaire dans l'exécution de leur fonction et conformément aux dispositions législatives pertinentes.

4.4. Séparation des fonctions incompatibles

Un même Employé ne peut, de par ses fonctions et à l'aide de ses accès aux Ressources informationnelles, contrôler toutes les phases d'un processus et avoir ainsi la possibilité de dissimuler ou de retarder la découverte d'une situation préjudiciable.

4.5. Classement

Toute Information doit être classée et conservée de façon à en permettre le repérage, en conformité avec le Plan de classification de la Caisse.

4.6. Innovation technologique

Dans la mesure où la gestion et la sécurité de l'Information sont assurées, la Caisse favorise l'implantation d'Outils technologiques novateurs qui rendent sa gestion plus efficace et efficiente et favorise la responsabilisation des Employés dans leur utilisation quotidienne des Ressources informationnelles.

5. GESTION DE LA SÉCURITÉ DES RESSOURCES INFORMATIONNELLES

Un processus de gestion de la sécurité des Ressources informationnelles est établi pour assurer la disponibilité, l'intégrité, la confidentialité, l'authenticité et l'irrévocabilité des Documents et Outils technologiques tout au long de leur cycle de vie.

5.1. Analyse des risques de sécurité

Le Processus de gestion de la sécurité des Ressources informationnelles repose sur une analyse des risques de sécurité pouvant toucher les Documents ou Outils technologiques de la Caisse. L'analyse tient notamment compte de la nature de l'Information véhiculée par la Ressource informationnelle, de la probabilité de survenance du risque et de son impact potentiel.

5.2. Plan directeur de sécurité

Un plan directeur de sécurité découle de l'analyse effectuée des risques de sécurité. Ce plan prévoit la mise en œuvre de mesures d'atténuation des risques de sécurité.

La direction de la Caisse revoit annuellement l'analyse des risques de sécurité et l'efficacité des mesures d'atténuation et ajuste son plan directeur en conséquence. Pour ce faire, elle utilise notamment des analyses d'écarts aux directives de sécurité, des résultats de travaux d'audit et des tests de vulnérabilité tant interne qu'externe.

5.2.1. Mesures de sécurité

Les mesures de sécurité appliquées aux Ressources informationnelles sont gérées et appliquées durant le cycle de vie d'un Document ou d'un Outil technologique, de son acquisition ou développement, à son utilisation, remplacement, archivage ou destruction.

La Caisse utilise différentes mesures de sécurité comme l'imposition de mots de passe, la surveillance préventive des risques de sécurité et des mesures de cryptage des Informations en transit ou transférées électroniquement.

La Directive fournit les lignes directrices à l'égard de l'application des mesures de sécurité pour tous les Employés. D'autres mesures de sécurité sont énoncées dans les directives de sécurité s'adressant spécifiquement aux équipes technologiques de la Caisse.

5.2.2. Gestion des identités et des accès

La gestion de l'identité des Employés et de leur accès aux Ressources informationnelles repose sur les principes de la séparation des fonctions incompatibles et des droits d'accès minimaux.

Cette gestion est centralisée à la PVP TI-Opérations et auprès de l'équipe de la Gestion documentaire.

5.2.3. Gestion centralisée des incidents et des exceptions

Tout incident de sécurité, toute mesure d'exception et toute demande de dérogation à une mesure de sécurité sont pris en charge par l'équipe de sécurité de l'information de la Caisse.

5.3. Droit de gérance de la Caisse

En tant qu'employeur, la Caisse peut examiner l'utilisation que font ses Employés des Ressources informationnelles qu'elle met à leur disposition. Elle peut intervenir lorsqu'elle détecte une situation réelle ou potentielle de non-conformité à ses politiques et directives. À cet égard, les Employés doivent consulter les règles du Code et de la Directive relatives à l'utilisation appropriée des Ressources informationnelles.

5.4. Continuité des affaires

Les Ressources informationnelles et infrastructures physiques essentielles aux activités critiques de la Caisse en cas de sinistre ou de crise majeure doivent être répertoriées et faire l'objet de mesures appropriées de protection et de disponibilité. Une reddition de comptes est effectuée à cet égard au comité stratégique TI.

6. LES OUTILS TECHNOLOGIQUES

6.1. Processus d'approbation et de reddition de comptes

La Caisse se dote d'un plan triennal des projets et activités touchant ses Outils technologiques et établit le cadre budgétaire qui en découle. Un plan annuel des projets et des activités ainsi que le budget alloué sont aussi adoptés.

Un bilan de chaque projet réalisé est effectué et une reddition de comptes sur l'ensemble des projets est régulièrement faite au comité stratégique TI.

6.2. Attribution

L'Équipe TI met à la disposition des Employés les Outils technologiques nécessaires à l'accomplissement efficace de leur travail. Elle fournit également le support requis pour le bon fonctionnement de ces Outils technologiques.

Les Employés doivent consulter la Directive pour connaître les règles d'utilisation des Outils technologiques.

6.3. Utilisation d'appareils technologiques personnels

La Caisse permet aux Employés d'utiliser leurs appareils personnels pour avoir accès au réseau visiteur de la Caisse. Ce réseau ne donne pas accès aux systèmes, applications, données, etc. de la Caisse, mais plutôt à certains services de base comme l'Internet. Les conditions d'utilisation de ces appareils sont prévues à la Directive.

6.4. Inventaire

La Caisse maintient à jour, de façon continue, un inventaire des Outils technologiques, incluant de l'information sur leur localisation et sur la personne qui en a la garde et en autorise les accès.

7. LES DOCUMENTS

7.1. Plan de classification et Calendrier de conservation

Afin de respecter ses obligations légales en matière de Gestion des documents découlant notamment de la *Loi sur les Archives* et de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « loi sur l'accès »), la Caisse se dote d'un Plan de classification et d'un Calendrier de conservation. Tous les Documents doivent être répertoriés selon ce Plan et respecter les règles de conservation établies dans le Calendrier.

7.2. Gestion documentaire en cas de litige ou de demande d'accès à l'information

Tous les Documents visés dans le cadre d'un litige, d'une demande d'accès à l'information ou lorsqu'il y a lieu de croire qu'un dossier pourrait devenir litigieux sont conservés nonobstant les délais prévus au Calendrier de conservation.

7.3. Outils technologiques de gestion documentaire

Les Outils technologiques utilisés pour la Gestion des documents doivent assurer la conservation, l'intégrité et la sécurité de l'ensemble des dossiers et Documents et permettre d'y faire des recherches précises et exhaustives.

8. ACCÈS DU PUBLIC AUX DOCUMENTS ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

8.1. Droit d'accès d'une personne du public

Toute personne qui en fait la demande a le droit d'avoir accès aux Documents de la Caisse, sauf à l'égard des exceptions prévues par la Loi sur l'accès et qui sont pour la Caisse principalement de deux natures :

- les Renseignements personnels;
- les Informations à caractère stratégique, financier et commercial.

Le droit d'accès d'une personne du public ne s'étend pas aux notes personnelles inscrites sur un Document ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres Documents de même nature.

Le traitement des demandes d'accès est prévu à la Directive. Un Employé qui reçoit une telle demande doit sans délai la transmettre à la responsable au sein de la Caisse de la Loi sur l'accès (la VPP Conformité et investissement responsable), conformément aux termes de la Directive.

8.2. Encadrement des Renseignements personnels

La cueillette, l'utilisation et la conservation des Renseignements personnels doivent s'effectuer dans le respect du cadre légal applicable. La Directive – Protection des renseignements personnels prévoit les lignes directrices à suivre dans la gestion des Renseignements personnels.

Un comité sur l'accès à l'Information et la protection des Renseignements personnels est constitué pour :

- Examiner les projets d'acquisition, de développement et de refonte de tout Outil technologique qui utilise, recueille, conserve communique ou détruit des Renseignements personnels et suggérer ceux qui doivent être encadrés de mesures particulières de protection;
- Établir les mesures particulières de protection des Renseignements personnels à respecter dans le cadre de sondages et relativement à une technologie de vidéosurveillance;
- Être informé des prestations électroniques de services qui recueillent, utilisent et conservent, communiquent ou détruisent des renseignements personnels.

9. SANCTIONS DÉCOULANT DU NON-RESPECT DE LA POLITIQUE

Le non-respect de la présente politique, notamment par l'utilisation, la modification, la destruction, la diffusion ou la divulgation non autorisée d'Information peut entrainer des sanctions, lesquelles sont fonction de la gravité de l'acte commis. Ces sanctions peuvent aller jusqu'au congédiement.

10. PROCESSUS D'ADOPTION ET DE MISE À JOUR DE LA POLITIQUE

La présente politique est soumise au comité de gestion pour approbation. Elle doit être révisée tous les trois ans, sauf s'il est nécessaire de le faire avant.

ANNEXE 1 : DEFINITIONS

- **Calendrier de conservation** : Calendrier qui établit notamment la durée de vie d'un document, de sa création jusqu'au moment où il doit être détruit ou versé à Bibliothèque et Archives nationales du Québec (« BAnQ ») pour conservation permanente.
- **Code** : Code d'éthique et de déontologie des dirigeants et des employés de la Caisse
- **Directive** : directive de la Caisse relative à la sécurité des Ressources informationnelles (TI et Documents).
- **Document** *:* Tout support d'Information, qu'il soit papier, électronique, magnétique, optique, sans fil ou autre. L'Information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images.
- **Document actif :** Tout Document régulièrement consulté par un ou des employés.
- **Employé** : Toute personne travaillant pour la Caisse à plein temps ou à temps partiel, à titre d'employé régulier ou occasionnel, incluant les stagiaires et les étudiants.
- **Gestion des documents** : Ensemble des activités, systèmes, moyens techniques et méthodes qui permettent de créer, recevoir, classifier, conserver, repérer et exploiter les Documents jusqu'à leur destruction ou versement à BAnQ.
- **Équipe TI** : selon le contexte, la PVP Opérations et TI, la VP Exploitation, la VP Planification, architecture et gouvernance, les responsables de ressources informationnelles.
- **Information** : Données, indications, ensemble de renseignements, incluant des Renseignements personnels, consignés par la Caisse sur un Document ou détenus par la Caisse, y compris une Information provenant d'un tiers. Une Information peut être :
  - **Information confidentielle** : Toute information ayant trait à la Caisse, aux tendances d'une industrie ou d'un secteur ou toute information de nature stratégique, qui n'est pas connue du public et qui, si elle était connue d'une personne qui n'est pas un employé, serait susceptible de lui procurer un avantage ou de compromettre la réalisation d'une opération à laquelle la Caisse participe. Cette expression comprend également toute information relative aux investissements ou aux personnes morales, sociétés et fonds d'investissement dans lesquels la Caisse détient ou examine une participation, y compris une information provenant d'un tiers.
  - **Information privilégiée** : Toute information encore inconnue du public et susceptible d'influencer la décision d'un investisseur raisonnable ou susceptible d'exercer une influence appréciable sur la valeur ou le cours des titres d'une société ayant fait un appel public à l'épargne. Toute information privilégiée constitue une information confidentielle. Voir le Code pour une définition plus exhaustive.
  - **Information publique** : Information qui, même si elle est connue d'une personne qui n'est pas un Employé, n'est pas susceptible de procurer à cette personne un avantage ou de compromettre la réalisation d'une opération à laquelle la Caisse participe.
  - **Information personnelle** : Voir définition de Renseignements personnels et de Renseignements personnels ayant un caractère public
- **Loi sur l'accès :** La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

- **Outils technologiques** : l'ensemble des équipements informatiques (incluant les appareils intelligents), systèmes, applications, réseaux, modèles (comme l'infonuagique) et autres éléments de même nature ainsi que les réseaux, les infrastructures et toute composante technologique qui sert à offrir les services de téléphonie et d'accès à internet, l'intranet et l'extranet de la Caisse.
- **Plan de classification** : Document qui établit la structure hiérarchique et logique des dossiers en fonction des activités de la Caisse. Il définit où les employés doivent classer les Documents afin d'en permettre le repérage.
- **Renseignement** : Indication, précision que l'on donne ou que l'on obtient sur quelqu'un ou sur quelque chose.
  - **Renseignements personnels** : Renseignements qui concernent une personne physique et permettent de l'identifier.
  - **Renseignements personnels ayant un caractère public** : Renseignement personnel au sens de l'article 57 de la loi sur l'accès, notamment le nom, le titre, la fonction, la classification, le traitement (ou l'échelle salariale selon le cas), l'adresse et le numéro de téléphone du lieu de travail d'un Employé de la Caisse.
- **Ressources informationnelles** : Ensemble des ressources apportant des éléments d'information de différentes natures, qui sont utilisées par la Caisse pour mener à bien sa mission. Les ressources informationnelles incluent notamment les ressources humaines, matérielles et technologiques.