Caisse de dépôt et placement du Québec

Le 17 février 2020

PAR COURRIEL

[redacted]

[redacted]

La présente fait suite à votre demande d'accès à l'information reçue par courriel le 17 janvier 2020 et pour laquelle je vous ai transmis un accusé de réception le 17 janvier 2020. Votre demande est ainsi libellée :

> *« …j'aimerais svp obtenir copie de tous les documents utilisés concernant le programme de formation et de sensibilisation de la protection des renseignements personnels, notamment le calendrier des activités, les documents de formation et de sensibilisation, les comptes rendus ou documents de reddition de compte aux différents comités décisionnels, les sondages d'évaluation des connaissances des employés (sauf les résultats), les autres documents promotionnels, etc. »*

Dans un premier temps, il est important de préciser que la Caisse, contrairement à l'administration publique dans son ensemble, ne traite pas avec la population en général et, de ce fait, ne collecte pas de renseignements personnels sur les citoyens du Québec. Toutefois, dans le cadre de ses activités, certains renseignements personnels peuvent être collectés et traités, notamment sur les employés et administrateurs de la Caisse pour des fins légitimes d'emploi et de conformité aux règles d'éthique.

La Caisse prend très au sérieux la protection des renseignements personnels et a mis en place des encadrements et des mesures techniques et organisationnelles pour garantir la sécurité des données. La Caisse a adopté une *Politique – Gestion et sécurité de l'information* dont découlent les deux directives suivantes : *Directive – Gestion et sécurité des ressources informationnelles (TI et Documents)* et *Directive – Protection des renseignements personnels* dont vous trouverez copies ci-jointes.

Par ailleurs, pour veiller à l'application du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, la Caisse a mis en place un comité sur l'accès à l'information et la protection des renseignements personnels. Ce comité réunit les responsables de la Sécurité de l'information, des Affaires juridiques, de la Gestion documentaire et des Ressources humaines. Il s'assure de la mise en œuvre des responsabilités et obligations eu égard à la protection des renseignements personnels.

[redacted]

Quant aux procès-verbaux de ce comité, nous ne pourrons malheureusement pas vous les communiquer parce que ces documents ont un contenu confidentiel et stratégique. En effet, la demande que vous formulez a trait à des documents qui sont au cœur des mesures de sécurité prises par la Caisse pour protéger des renseignements confidentiels. Conséquemment, leur divulgation aurait pour effet de réduire l'efficacité d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne. Nous sommes d'avis que ces documents sont couverts par l'article 29 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels RLRQ, c. A-2.1* (« Loi sur l'accès ») et que leur divulgation risquerait vraisemblablement d'avoir l'un ou l'autre des effets énoncés à ces articles.

Ces documents peuvent contenir des renseignements nominatifs au sens de l'article 53 de la Loi sur l'accès que la Caisse se doit de protéger à ce titre.

Enfin, sachez que la Caisse met en œuvre des outils et des activités pour sensibiliser et former les employés sur la protection des renseignements personnels. Tous les nouveaux employés de la Caisse suivent une formation obligatoire sur le Code d'éthique. Ce Code précise les attentes en matière de protection de la confidentialité de l'information, notamment des renseignements personnels. Des formations sur la protection des renseignements personnels ont été données par des avocats spécialistes aux employés concernés par la gestion de tels renseignements. Depuis l'entrée en vigueur du Règlement général sur la protection des données personnelles de l'Union européenne en 2018, deux séminaires de formation ont été organisés.

Étant donné que la divulgation de ces documents risquerait d'avoir un impact sur des tiers et sur la propriété intellectuelle, ces renseignements ne pourraient vous être communiqués sans qu'ils n'en soient d'abord avisés et qu'ils puissent faire valoir leur représentation, notamment dans le cadre des articles 9, 12, 22, 23 et 24 de la Loi sur l'accès. Nous réservons donc nos droits à cet égard.

Selon nous, les articles 9, 12, 22, 23, 24, 29, 37, 39, 53 et 54 de la Loi s'appliquent en tout ou en partie à votre demande.

En terminant, pour votre information, nous vous joignons copie des articles 9, 12, 22, 23, 24, 29, 37, 39, 53 et 54 et vous faisons part de la teneur de l'article 135 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* :

> «135. Une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission de réviser cette décision.

[redacted]

Une personne qui a fait une demande en vertu de la présente loi peut demander à la Commission de réviser toute décision du responsable sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur l'application de l'article 9 ou sur les frais exigibles.

Ces demandes doivent être faites dans les trente jours qui suivent la date de la décision ou de l'expiration du délai accordé par la présente loi au responsable pour répondre à une demande. La Commission peut toutefois, pour un motif raisonnable, relever le requérant du défaut de respecter ce délai.»

Veuillez agréer, [redacted] mes salutations distinguées.

[redacted]

Simon Denault
Directeur, Éthique et conformité et
Responsable de l'accès à l'information
et de la protection des renseignements personnels

p.j.

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 1
2. Portée 1
3. Gouvernance 2
4. Principes 2
5. Gestion de la sécurité des ressources informationnelles 3
6. Les outils technologiques 4
7. Les documents 5
8. Accès du public aux documents et protection des Renseignements personnels 5
9. Sanctions découlant du non-respect de la politique 6
10. Processus d'adoption et de mise à jour de la politique 6

Annexe 1 : Définitions 7

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.

Caisse de dépôt et placement du Québec

DIRECTIVE – GESTION ET SÉCURITÉ DES RESSOURCES INFORMATIONNELLES (TI ET DOCUMENTS)

Objectifs

- Encadrer l'utilisation des technologies de l'information et de documents afin d'assurer la sécurité de l'information dont la Caisse dispose
- Encadrer l'attribution du matériel technologique et des privilèges d'utilisation des employés de la Caisse

TABLE DES MATIÈRES

1. Définitions 1
2. Principes généraux d'utilisation des outils technologiques 1
3. Poste de travail 2
4. Applications 4
5. Droits d'accès 5
6. Zones de travail 7
7. Mobilité et itinérance 7
8. Utilisation d'Internet et du courrier électronique 8
9. Principes généraux d'utilisation des documents 9
10. Accès du public aux documents et protection des renseignements personnels 10
11. Responsabilités des équipes TI et Gestion des documents 10
12. Révision 10

Annexe 1 : Définitions 11
Annexe 2 : Moratoire sur les changements informatiques 13
Annexe 3 : Avis de rétention de documents 14

1. DÉFINITIONS

Dans la présente directive, les termes commençant par une majuscule sont définis à l'annexe 1.

2. PRINCIPES GÉNÉRAUX D'UTILISATION DES OUTILS TECHNOLOGIQUES

2.1 Privilège d'utilisation

L'utilisation des Outils technologiques est un privilège accordé aux Employés et non un droit. Ce privilège peut être révoqué en cas de non-respect des politiques, directives et Code de la Caisse à l'égard de leur utilisation.

2.2 Utilisation personnelle minimale

Les Outils technologiques fournis par la Caisse à ses Employés doivent être dédiés et réservés à la réalisation des activités de la Caisse. Une utilisation personnelle minimale est permise pourvu qu'un tel usage ne nuise pas à la prestation de travail de l'Employé et que les dispositions à cet égard dans les directives et dans le Code sont respectées.

2.3 Traçabilité des actions

Tout accès et toute modification apportée à de l'Information sont suivis de façon à assurer la traçabilité de ces actions.

2.4 Utilisation incorrecte des Outils technologiques

Les Employés doivent informer l'Équipe TI de toute utilisation qui leur parait incorrecte ou non conforme relativement à l'utilisation des Outils technologiques.

2.5 Usage exclusif

Tout outil technologique fourni par la Caisse est à l'usage exclusif de ses Employés qui ne peuvent permettre à toute autre personne non autorisée de l'utiliser.

2.6 Moratoire

Durant la période des fêtes de fin d'année et la période de production des états financiers annuels, la Caisse impose un moratoire (gel) sur tout changement aux Outils technologiques (système, réseau, application) pouvant influer sur leur stabilité opérationnelle. Voir à cet égard l'annexe 2.

2.7 Acquisition d'Outils technologiques

Les Employés doivent communiquer avec l'Équipe TI :

- s'ils veulent faire l'acquisition d'un Outil technologique pour un usage d'entreprise;
- s'ils veulent, pour un usage personnel, faire l'acquisition d'un Outil technologique qui permet de stocker des Renseignements personnels (autres que ceux concernant l'Employé en question) ou de l'Information confidentielle ou privilégiée de la Caisse.

Les Employés peuvent installer des logiciels sans communiquer avec l'Équipe TI lorsque les données qui sont stockées ne constituent pas de l'Information confidentielle ou privilégiée et ne contiennnent pas de Renseignements personnels concernant d'autres Employés.

L'Équipe TI est responsable de coordonner la réalisation de toute acquisition de ce type d'Outil (achat, intégration, déploiement et reddition de comptes) le cas échéant.

3. POSTE DE TRAVAIL

3.1 Appareils fournis par la Caisse

La Caisse fournit à chaque Employé, selon son Profil utilisateur, un ordinateur de bureau ou un ordinateur portable, et, s'il y a lieu, un téléphone intelligent ou une tablette

électronique. Elle peut également fournir tout autre équipement, lorsque justifié par un besoin d'affaires.

Toute attribution d'équipement qui n'est pas conforme au Profil utilisateur doit être justifiée par le responsable d'équipe concerné et autorisée s'il y a lieu par un vice-président ou le premier vice-président du secteur. Les frais liés à cet équipement sont facturés au centre de coûts du secteur requérant.

L'Employé qui perd ou se fait voler un appareil fourni par la Caisse doit en aviser immédiatement l'Équipe TI.

Configuration

Un Employé peut, lorsque la technologie le permet, configurer certains éléments de l'appareil qui lui est fourni comme l'ajout d'imprimante ou de fonds d'écran.

Les éléments liés à la sécurité, comme l'apparition d'un écran de veille, la création de comptes utilisateurs, le pare-feu ou l'antivirus, sont configurés par l'Équipe TI (Exploitation) et ne doivent pas être modifiés par l'Employé.

Protection des appareils mobiles

Les appareils mobiles (ordinateur portable, téléphone, tablette et autres) fournis par la Caisse doivent être protégés par mot de passe et toutes leurs unités de stockage doivent être cryptées.

La possibilité d'écrire sur des unités de stockage amovibles est restreinte à l'Employé qui le requière pour un besoin d'affaires défini et approuvé par le responsable d'équipe.

3.2 Appareil personnel d'un Employé

Conditions d'utilisation d'un appareil personnel

Un Employé qui fournit son propre ordinateur portable, téléphone portable ou sa propre tablette électronique peut avoir accès au Réseau visiteur et donc à certains services de base comme l'Internet, aux conditions suivantes :

- Il ne partage pas de connexion avec un autre appareil;
- Il s'engage à ne pas installer d'Applications qui pourraient permettre le contournement des politiques et directives de la Caisse.

Aucune assistance n'est offerte par l'Équipe TI en cas de problème de connexion avec un appareil personnel.

Synchronisation des courriels, contacts et calendrier Caisse avec une tablette électronique ou un téléphone intelligent personnel

Un Employé peut synchroniser ses courriels, contacts et calendrier Caisse sur sa tablette électronique ou son téléphone intelligent personnel. Dans un tel cas :

- Son appareil doit être compatible avec les environnements de la Caisse;
- Son appareil doit respecter les conditions minimales d'utilisation (cryptage des données, protection par mot de passe, installation d'un certificat Caisse);

- L'Employé qui a perdu son appareil ou dont l'appareil a fait l'objet d'un piratage informatique en informe immédiatement l'Équipe TI et accepte qu'il puisse être vidé de ses données si l'Équipe TI juge que la sécurité de l'Information est en jeu;
- L'Employé s'engage à rendre son appareil disponible à tout moment à l'Équipe TI afin d'en valider la conformité à la présente directive.

La synchronisation des courriels, contacts et calendrier Caisse sur un appareil personnel permet à l'Équipe TI de connaître les Applications installées sur l'appareil et de supprimer à distance le contenu lié à la Caisse ou le contenu global de l'appareil si les circonstances l'exigent pour assurer la sécurité de l'Information de la Caisse.

Un support de type temps/matériel est offert et facturé au centre de coûts de l'Employé en cas de problèmes de configuration du service de courrier.

Conditions de stockage d'Information

L'appareil personnel d'un Employé ne doit en aucun temps contenir de Renseignements personnels obtenus dans le cadre du travail ou de l'Information privilégiée, à moins que ce ne soit nécessaire pour assurer la sécurité de l'Information ou la continuité des affaires. Si l'appareil contient de l'Information Caisse, l'Employé doit respecter les exigences de l'article 7.2 et les exigences suivantes :

- Les mises à jour de sécurité doivent être appliquées de façon automatique;
- Les appareils doivent être supportés par leur fournisseur;
- Les données doivent être chiffrées;
- L'appareil doit être protégé par mot de passe;
- Une fonction de mise en veille après un maximum de 15 minutes de non-utilisation est activée;

4. APPLICATIONS

4.1 Normalisation

Pour être installée sur un appareil fourni par la Caisse, une Application doit être normalisée. De façon générale, les Applications qui sont critiques à une fonction d'affaires et celles qui permettent le stockage de données de la Caisse chez des tierces parties (fournisseurs) sont normalisées.

Seuls les employés du centre de services (2888) ou les employés qui sont administrateurs de leur poste peuvent installer une Application sur l'appareil fourni par la Caisse.

4.2 Privilèges d'installation

L'Employé qui est administrateur de son poste de travail peut installer une Application non normalisée. Pour ce faire, il doit suivre une formation offerte par l'équipe TI relativement aux points suivants :

- Les conditions d'installation de l'Application puisque l'Employé est personnellement responsable des frais qui peuvent être engagés;

- Le paiement par l'Employé de droits d'utilisation au tarif entreprise, de toute Application non normalisée que l'Employé utilise dans le cadre du travail, et ce, même si l'utilisation personnelle de l'Application est sans frais. Il en va de même pour toute Application installée sur un appareil personnel utilisé au travail;
- L'envoi au responsable d'équipe et à l'Équipe TI de la liste d'Applications installées sur le poste de travail;
- Le retrait sans préavis de toute Application non normalisée que l'Équipe TI juge problématique pour le Réseau interne;
- Le retrait possible du privilège d'installation de l'Application s'il y a abus ou si les directives en vigueur ne sont pas respectées;
- L'absence de support TI sur les Applications non normalisées. En cas de problème avec une telle Application, l'Équipe TI peut effectuer une réinstallation du poste de travail, selon le Profil utilisateur. Les frais entourant cette réinstallation sont facturables au centre de coûts de l'Employé. Par ailleurs, la réinstallation des Applications non normalisées incombe à l'Employé.

4.3 Logiciels antivirus

Les logiciels servant à assurer la sécurité sur le poste de travail (par exemple antivirus, protection contre logiciel malveillant, pare-feu) doivent être actifs en tout temps sur tous les appareils connectés au Réseau interne. Seule l'équipe TI peut désactiver de tels logiciels.

4.4 Interdictions

Il est interdit de copier, à des fins personnelles, les Applications normalisées. À cet égard, les Employés doivent aussi respecter les droits de propriétés intellectuelles des Applications installées sur leur poste de travail.

5. DROITS D'ACCÈS

5.1 Code utilisateur et mot de passe

L'accès au Réseau interne et à l'Information Caisse se fait par l'utilisation d'un code utilisateur et d'un mot de passe.

L'attribution d'un code utilisateur et d'un mot de passe relève de l'Équipe TI. Un Employé ne peut se donner accès à lui-même sans qu'une alerte ne soit déclenchée à l'Équipe TI.

Caractéristiques des mots de passe

Les mots de passe doivent :

- Être différents du code utilisateur;
- Avoir minimalement huit caractères;
- Contenir des lettres, des chiffres et des caractères spéciaux;
- Ne pas avoir été utilisés dans les 12 derniers mois.

Les mots de passe du répertoire primaire (accès au réseau et à Windows) expirent après 90 jours tandis que ceux des systèmes d'authentification secondaires (comme Murex) expirent après 120 jours.

Il est interdit aux Employés de divulguer leur mot de passe. Tous les fichiers contenant des mots de passe doivent être chiffrés et n'être accessibles que par les Employés autorisés.

Modification des mots de passe

La modification d'un mot de passe doit être faite par l'Employé détenteur du code utilisateur et non par une tierce personne.

Lorsqu'un nouveau mot de passe est requis de l'équipe TI, cette dernière le donne de vive voix à l'Employé (si l'Employé a été positivement identifié) ou le laisse sur sa boîte vocale; elle ne le fournit jamais par courriel ni par l'intermédiaire d'un tiers.

Verrouillage des comptes utilisateurs

Tout compte utilisateur est verrouillé après cinq saisies infructueuses de mot de passe.

Une session de travail est automatiquement verrouillée après 15 minutes d'inutilisation du compte d'utilisateur. Malgré ce verrouillage automatique, tout Employé doit lui-même verrouiller sa session de travail Windows dès qu'il quitte son poste de travail.

5.2 Certificat

L'authentification d'un appareil mobile (fourni par la Caisse ou personnel) au réseau de la Caisse s'effectue au moyen d'un certificat numérique. Ce certificat est l'identifiant unique de l'appareil pour l'accès au réseau de la Caisse. L'Employé doit suivre la procédure d'authentification établie par l'Équipe TI.

5.3 Changement de rôle ou départ d'un Employé

Lorsqu'un Employé change de rôle :

- L'analyse du nouveau rôle de l'Employé se fait préalablement à l'attribution de nouveaux droits d'accès; l'analyse porte notamment sur les fonctions incompatibles;
- Les accès associés à l'ancien rôle de l'Employé sont retirés après le changement de rôle, selon les instructions de l'ancien responsable d'équipe de l'Employé ou en fonction de la nature de l'Information à laquelle il avait accès.

Lorsqu'un Employé quitte la Caisse, son accès au Réseau interne, y compris son code VPN d'accès à distance, ainsi que les accès aux autres Applications lui sont retirés par l'Équipe TI.

Après deux mois d'inactivité, un compte utilisateur est suspendu. L'Équipe TI détermine après analyse s'il y a lieu de réactiver ce compte.

5.4 Compte générique

Les Employés doivent communiquer avec l'Équipe TI pour obtenir le droit d'utiliser un compte générique (code utilisateur et mot de passe partagés par plus d'une personne).

5.5 Accès à un poste de travail par une personne de l'externe

Dans le cadre de certaines formations ou sessions de travail Web et de façon exceptionnelle, une personne de l'externe peut demander à un Employé d'avoir accès à son poste de travail afin d'ajuster certains paramètres qui faciliteront le déroulement de la session.

À partir du moment où l'Employé donne son consentement explicite, la personne de l'externe est en mesure de prendre possession du poste de travail. Conséquemment, l'Employé doit en tout temps surveiller ce que la personne de l'externe fait sur son poste puisqu'il est responsable des actions effectuées avec son compte utilisateur. L'Employé doit également signaler à l'Équipe TI tout écart par rapport à ce qui était convenu dans l'intervention (qui doit être restreinte au poste de travail de l'Employé). En aucun temps la personne de l'externe ne doit pouvoir se connecter à d'autres systèmes ou Applications de la Caisse. L'Employé peut se faire accompagner par une personne du centre de services (7777) s'il le souhaite.

6. ZONES DE TRAVAIL

Deux zones de travail coexistent à la Caisse. Une première zone permet de maintenir toutes les Informations, qu'elles soient privilégiées, personnelles ou confidentielles dans une zone contrôlée et gérée par l'Équipe TI. Une seconde zone dite analytique est gérée par l'Employé et auditée par l'Équipe TI. Cette zone analytique a pour but de répondre aux besoins d'agilité informationnelle et analytiques des stratégies d'investissement, de démocratiser l'accès à l'Information et d'améliorer les façons de faire.

L'Équipe TI est responsable d'établir les normes d'utilisation d'une zone analytique. Ainsi, les Employés doivent communiquer avec cette équipe pour l'obtention d'une zone analytique.

7. MOBILITÉ ET ITINÉRANCE

7.1 Connexion à distance

Aucun accès externe direct n'est possible sur le Réseau interne de la Caisse. Les Employés devant se connecter à distance au Réseau interne doivent passer par un réseau privé virtuel (« **VPN** ») avec une authentification à deux facteurs.

Les appareils Caisse ou personnels qui se connectent au Réseau interne par l'entremise de VPN doivent respecter des critères de configuration minimale de sécurité qui sont validés lors de chaque connexion.

7.2 Stockage d'Information

Les Informations doivent être protégées en tout temps et stockées dans un outil de gestion électronique des documents (« GED ») afin de respecter les lois en matière de gestion documentaire.

S'il advient que des Informations sont aussi stockées dans un appareil mobile, elles doivent y être stockées de façon temporaire et détruites dès que possible. La version officielle de ces Informations est celle qui est stockée dans un outil de GED.

Par ailleurs, OneDrive CDPQ est le seul site de stockage en ligne autorisé pour les documents Caisse.

Aucun Document ne doit résider sur un réseau social d'entreprise; seul un lien URL pointant vers un outil de GED peut y être déposé.

La Caisse se réserve le droit de procéder à des contrôles ponctuels sur le stockage d'Information. À cet égard, elle peut exiger de tout Employé une confirmation qu'autant qu'il sache, toute Information obtenue dans le cadre de son travail est enregistrée dans un outil de GED et qu'il a détruit en temps opportun toute Information stockée de façon temporaire sur un appareil personnel.

8. UTILISATION D'INTERNET ET DU COURRIER ÉLECTRONIQUE

8.1 Utilisation d'Internet

L'utilisation d'Internet doit se faire conformément aux règles établies dans le Code, notamment en ce qui a trait aux médias sociaux et autres sites de collaboration.

Avant de souscrire à une solution ou Application d'un fournisseur, hébergée à l'externe, l'Équipe TI doit évaluer les risques de sécurité.

8.2 Utilisation du courrier électronique

Confidentialité de l'information

L'Information transmise par courriel à l'extérieur du réseau Caisse doit être protégée.

Dans certains cas, des canaux sécurisés ont été mis en place afin de protéger tous les échanges de courriels entre la Caisse et une organisation externe. Un Employé peut consulter l'Équipe TI pour savoir si une organisation avec laquelle il communique est visée par un tel canal sécurisé.

En l'absence de tels canaux sécurisés, les fichiers transmis à l'extérieur du réseau Caisse doivent être protégés par mot de passe.

En outre, chaque courriel envoyé à l'extérieur du réseau Caisse porte automatiquement une mention de confidentialité.

Conservation et destruction des courriels

Les courriels à valeur administrative, légale, financière ou historique, servant à documenter les activités, droits ou obligations de la Caisse doivent être conservés et archivés dans un outil de GED et classifiés selon le sujet traité.

Les courriels éphémères, généralement reçus à titre d'information et qui ont une utilité à court terme doivent être détruits lorsqu'ils ne sont plus utiles.

Les courriels sans valeur pour la Caisse, comme les courriels personnels, les pourriels et les copies de courriels, doivent être détruits dès leur réception.

9. PRINCIPES GÉNÉRAUX D'UTILISATION DES DOCUMENTS

Chaque Employé doit s'assurer de protéger l'Information contenue dans les Documents en prenant les mesures nécessaires à cette fin comme de ne pas laisser à la vue les Documents, d'en assurer la protection physique et d'apposer la mention « confidentiel » sur les Documents appelés à circuler.

Les Employés doivent se conformer aux mesures de protection de l'Information prévues au Code.

Par ailleurs, la gestion et la conservation des Documents doit se faire en conformité des règles établies par l'équipe Gestion des documents

9.1 Numérisation

La numérisation des Documents, dont le but est de détruire les exemplaires papier, doit être faite en suivant le processus de numérisation et de transfert de support établi par l'équipe Gestion des documents.

9.2 Archivage

Les Documents qui ne sont plus régulièrement consultés doivent être archivés; pour ce faire, chaque première vice-présidence doit réviser annuellement l'ensemble de ses Documents.

9.3 Destruction

La destruction de tout Document doit être faite en collaboration avec l'équipe Gestion des documents, à l'exception de notes personnelles, esquisses, ébauches, brouillons, courriels, messages téléphoniques et notes préparatoires qui peuvent être détruits lorsqu'ils ne sont plus jugés utiles, et ce, sans tenir compte du Calendrier de conservation.

9.4 Documents visés par un litige ou une demande d'accès à l'information

Dans le cadre d'un litige ou lorsqu'il y a lieu de croire qu'un dossier pourrait devenir litigieux ou encore dans le cadre d'une demande d'accès à l'information, tous les Documents visés par un avis de rétention de Documents (voir annexe 3) seront conservés nonobstant les délais prévus au Calendrier de conservation.

Dans ce cas, la transmission de tout Document à des tiers ou à la partie adverse ou la communication de tout Document pouvant être produit au dossier de la Cour doit être approuvée par la première vice-présidence, Affaires juridiques et secrétariat.

9.5 Conservation de Documents légaux

Les Documents légaux originaux signés qui sont en format papier doivent être numérisés pour une conservation en version électronique, puis archivés.

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

10.1 Traitement d'une demande d'accès à un Document de la Caisse

Tout Employé qui reçoit d'une personne du public (une personne physique, un organisme, une entreprise, etc.), une demande d'accès à un Document de la Caisse, que cette demande soit formulée ou non en vertu de la Loi sur l'accès, doit la transmettre sans délai au responsable au sein de la Caisse de l'application de la Loi sur l'accès (le « Responsable de l'accès à l'information »).

À la Caisse, le Responsable de l'accès à l'information est le VPP Conformité et Investissement responsable. Dans le cadre de son travail, celui-ci peut accéder à toute Ressource informationnelle faisant l'objet d'une demande présentée à la Caisse en vertu de la Loi sur l'accès.

10.2 Communication d'un Renseignement personnel

Un Employé ne peut communiquer un Renseignement personnel sans le consentement de la personne concernée, sauf dans certains cas et à de strictes conditions prévues par la Loi sur l'accès.

11. RESPONSABILITÉS DES ÉQUIPES TI ET GESTION DES DOCUMENTS

Chacun dans leur domaine respectif d'expertise, les Équipes TI et Gestion des documents doivent :

- Assurer une sensibilisation continue à la gestion et la sécurité de l'Information et de la continuité des affaires.
- Accompagner les employés dans l'application des normes de gestion, des exigences de sécurité de l'Information et de continuité des affaires.
- Contrôler les accès à l'Information.
- Approuver ou obtenir du responsable d'équipe visé l'autorisation pour toute demande qui va au-delà du Profil utilisateur d'un Employé.

12. RÉVISION

La présente directive est soumise au comité stratégique TI-Opérations pour approbation. Elle doit être révisée tous les trois ans, sauf s'il est nécessaire de le faire avant.

ANNEXE 1 : DÉFINITIONS

- **Appareil utilisateur** : Tout appareil, fourni par la Caisse ou non, permettant d'accéder à de l'Information ou à des systèmes de la Caisse.
- **Applications** : Applications informatiques, incluant les progiciels, logiciels et modèles qui permettent d'accéder à de l'Information de la Caisse.
  - **Application normalisée :** application acquise et installée de façon standardisée sur les postes de travail et supporté par l'Équipe TI.
- **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** : le code d'éthique et de déontologie des dirigeants et employés.
- **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.
- **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 téléphones intelligents et les tablettes électroniques), systèmes, applications, réseaux, modèles (ex. 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.
- **Profil utilisateur** : Profil qui détermine où la majeure partie du temps de travail d'un employé est effectuée et à quels Outils technologiques il a accès.

- **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.
- **Réseau interne** : Réseau connecté directement, sans pare-feu, respectant en continu les contrôles, politiques et directives de la Caisse. Il s'agit du réseau auquel les Utilisateurs ont accès selon leur Profil utilisateur.
- **Réseau visiteur :** Réseau externe de la Caisse qui ne respecte pas en tout ou en partie les contrôles, politiques et directives 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.

ANNEXE 2 : MORATOIRE SUR LES CHANGEMENTS INFORMATIQUES

Pour réduire le risque d'instabilité des systèmes d'information pendant le temps des fêtes de fin d'année et la période de production des états financiers annuels, un moratoire est imposé par la Caisse sur tout changement à ses Outils technologiques.

Type de moratoire

Il existe deux types de moratoire :

- Un moratoire général pour minimiser le risque de défaillance pendant le temps des fêtes. Ce moratoire s'applique à tous les systèmes sur la chaîne transactionnelle. Il commence le troisième samedi de décembre et se termine la première journée ouvrable de l'année suivante.
- Un moratoire financier pour minimiser le risque de défaillance durant la période de production des états financiers. Ce moratoire s'applique seulement aux systèmes d'information et aux composantes technologiques des systèmes d'information visés par le programme d'attestation financière. Il commence le troisième samedi de décembre et se termine au moment de la publication des résultats annuels de la Caisse.

À moins d'une urgence, aucune modification aux Outils technologiques (systèmes d'information et composantes technologiques de ces systèmes) pouvant influer sur la stabilité opérationnelle de ces Outils n'est permise durant ces moratoires.

Poste de travail

Les changements majeurs aux postes de travail pouvant influer sur la stabilité d'exécution des systèmes d'information sont prohibés durant le moratoire financier.

Les changements mineurs à un poste de travail, comme une mise à jour de composantes non applicatives, peuvent être déployés durant les moratoires.

Dérogation

Toute dérogation à un moratoire doit être demandée par le gestionnaire de l'équipe de livraison et approuvée par le propriétaire du système et par la vice-présidence, TI-Exploitation

Ces dérogations sont soumises pour information au comité risques opérationnels.

ANNEXE 3 : AVIS DE RÉTENTION DE DOCUMENTS

AVIS DE RÉTENTION DE DOCUMENTS

Vous avez été identifié comme l'un des intervenants dans le dossier ABC. Ce dossier fait ou pourrait faire l'objet de procédures judiciaires litigieuses. Par les présentes, vous êtes avisés que vous ne devez détruire aucun document papier ou électronique lié directement ou indirectement à ce dossier. Veuillez communiquer avec [nom du Conseiller juridique aux Affaires juridiques (514-847-xxxx)] afin de prendre les dispositions nécessaires visant la transmission de votre dossier aux Affaires juridiques et secrétariat dans les meilleurs délais.

Caisse de dépôt et placement du Québec

DIRECTIVE – PROTECTION DES RENSEIGNEMENTS PERSONNELS

Objectifs

- Définir les exigences minimales de protection et de confidentialité des Renseignements personnels
- Établir des procédures pour encadrer la gestion des Renseignements personnels

TABLE DES MATIÈRES

1. Contexte 2
2. Définitions 2
3. Principes généraux de protection des renseignements personnels 2
   - 3.1 Légalité et transparence 2
   - 3.2 Limitation des finalités 2
   - 3.3 Minimisation des données 2
   - 3.4 Exactitude 2
   - 3.5 Protection des Renseignements dès leur conception 3
   - 3.6 Limitation de la conservation 3
   - 3.7 Intégrité et confidentialité 3
   - 3.8 Responsabilité 3
4. Gestion des renseignements personnels 3
   - 4.1 Collecte et utilisation 3
   - 4.2 Stockage et conservation 4
   - 4.3 Communication et transfert 4
   - 4.4 Suppression ou destruction 4
5. Gestion des fournisseurs 4
6. Outils de conformité 5
   - 6.1 Registre des Traitements 5
   - 6.2 Analyse d'impact sur la protection des données 5
   - 6.3 Portail dédié à la conformité en matière de protection des Renseignements personnels 5
7. Droits des personnes concernées 5
8. Sécurité 6
9. Gestion des incidents 7
10. Formation et point de contact 7
11. Rôles et responsabilités 7
12. Révision 8

1. CONTEXTE

Dans le cadre des activités de la Caisse, des Renseignements personnels sont collectés, traités et conservés. La présente directive fournit un encadrement à l'égard de ces Renseignements personnels traités par la Caisse.

Elle vise à :

- Définir les principes directeurs en matière de protection des Renseignements personnels devant guider la Caisse et son personnel en vue d'assurer l'intégrité et la confidentialité de l'information ainsi que de prévenir toute atteinte aux règles visant la protection des Renseignements personnels;
- Se conformer aux lois applicables, notamment à la *Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels* (« Loi sur l'accès ») et au Règlement Général Européen sur la Protection des Données (« RGPD »).

2. DÉFINITIONS

Dans la présente directive, les termes commençant par une majuscule sont définis à l'annexe 1.

3. PRINCIPES GÉNÉRAUX DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les exigences qui suivent constituent les principes directeurs de protection des Renseignements personnels traités par la Caisse. Ces principes découlent de l'environnement légal applicable à la Caisse.

3.1 Légalité et transparence

Tout Traitement de Renseignements personnels doit être nécessaire à l'exercice des activités de la Caisse et conforme aux lois applicables. Les personnes visées par la collecte de Renseignements personnels sont informées du Traitement et des droits qu'elles peuvent exercer concernant leur utilisation.

3.2 Limitation des finalités

Les Renseignements personnels doivent être collectés pour des fins déterminées, explicites et légitimes dans le cadre des activités de la Caisse, et ne pas être traités ultérieurement d'une manière incompatible avec celles-ci.

3.3 Minimisation des données

Les Renseignements personnels doivent être adéquats, pertinents et limités à ce qui est nécessaire au regard des fins pour lesquelles ils sont traités.

3.4 Exactitude

Les Renseignements personnels doivent être exacts et tenus à jour. Toutes les mesures raisonnables doivent être prises pour que ces renseignements, s'ils sont inexacts, soient rectifiés ou effacés sans tarder.

3.5 Protection des renseignements dès leur conception

L'organisation intègre des mesures de protection des Renseignements personnels dès l'étape de conception d'un projet, d'un service ou de tout autre outil lié à la manipulation de Renseignements personnels (principe du *privacy by design*).

3.6 Limitation de la conservation

Les Renseignements personnels doivent être conservés sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des fins pour lesquelles ils sont traités.

3.7 Intégrité et confidentialité

Les Renseignements personnels doivent être traités de façon à garantir une sécurité appropriée, y compris la protection contre le Traitement non autorisé ou illicite et contre la perte ou la destruction, à l'aide de mesures techniques ou organisationnelles appropriées.

3.8 Responsabilité

Le Responsable du traitement s'assure de l'application de la présente directive et du respect des principes de protection des renseignements qui en découle.

Par ailleurs, certains Renseignements personnels peuvent toutefois revêtir un caractère public. Au Québec, la Loi sur l'accès énumère une série de Renseignements personnels qui ont un caractère public et, dans ce cas, perdent leur caractère confidentiel.

4. GESTION DES RENSEIGNEMENTS PERSONNELS

4.1 Collecte et utilisation

Base légale – La collecte et le Traitement de Renseignements personnels doivent être licites, c'est-à-dire prendre appui sur une base légale et sur les règles liées à la collecte, l'utilisation, la communication et la conservation des Renseignements personnels.

La Caisse ne recueille que les renseignements nécessaires à l'exercice de ses activités. Sauf exception, la Caisse ne peut communiquer les Renseignements personnels sans avoir, au préalable, obtenu le consentement de la personne concernée.

Consentement – Dans le cas de certains Traitements de Renseignements personnels, le consentement préalable est nécessaire. Le consentement de la personne concernée doit être manifeste, libre, éclairé et être donné à des fins spécifiques.

Il peut être donné par une déclaration écrite, y compris par la voie électronique. Le consentement doit être univoque et ne peut se déduire d'une case précochée ou d'une absence d'action.

Minimisation des données – Au moment de la collecte des données, la Caisse ne collecte que les données strictement nécessaires aux finalités poursuivies.

4.2 Stockage et conservation

Supports – Il existe différents types de supports pour les Traitements de Renseignements personnels et de lieux de stockage de ces renseignements. Il est essentiel de bien les identifier pour protéger les données correctement et limiter les risques de Violations de la confidentialité des Renseignements personnels. L'information confidentielle est protégée par l'application des mesures de sécurité prévues à la Directive – Gestion et sécurité de l'information.

Environnements de développement informatique – Toute utilisation de Renseignements personnels dans un environnement de développement informatique doit respecter des requis sécuritaires additionnels tels que l'anonymisation, le masquage, le chiffrement. Ces renseignements doivent être stockés selon les normes de sécurité de la Caisse.

Conservation des renseignements – Les Renseignements personnels ne doivent pas être conservés sous une forme permettant l'identification de la personne concernée plus longtemps que nécessaire aux fins pour lesquelles elles ont été obtenues ou pour une durée supérieure à celle requise par les exigences réglementaires applicables.

4.3 Communication et transfert

Destinataires – Toute personne ayant accès à un Renseignement personnel, qu'elle soit de l'interne ou de l'externe. La Caisse ne communique les Renseignements personnels qu'aux Destinataires nécessaires au regard des fins poursuivies.

Transfert Hors frontière – Un transfert, vers une autre province ou un autre pays, de Renseignements personnels qui font ou sont destinés à faire l'objet d'un Traitement après ce transfert ne peut avoir lieu que si ces renseignements bénéficient d'un niveau de protection équivalent ou suffisant, au sens de la Loi sur l'accès et du RGPD.

4.4 Suppression ou destruction

Durée de conservation – La Caisse a défini des durées de conservation pour les catégories de Renseignements personnels en fonction des finalités poursuivies et de ses obligations légales. Elle s'est dotée d'un Plan de classification et d'un Calendrier de conservation. À l'expiration de la durée de conservation, les Renseignements personnels ne peuvent être stockés que conformément aux lois et réglementations locales applicables.

5. GESTION DES FOURNISSEURS

En tant que Responsable du traitement

Pour tout Traitement impliquant des sous-traitants et fournisseurs, la Caisse met en place des contrats incluant ce qui est requis par le RGPD et spécifiant les instructions de Traitement que doit suivre le sous-traitant ou fournisseur. Un modèle de convention incluant les clauses essentielles est disponible. Celles-ci portent notamment sur le respect des droits des personnes, la sécurité des données, la notification de toute Violation de la confidentialité des Renseignements personnels, les transferts transfrontaliers, l'audit et la responsabilité du sous-traitant.

En tant que sous-traitant

La Caisse est considérée comme un sous-traitant lorsqu'elle traite des Renseignements personnels pour l'une de ses filiales.

6. OUTILS DE CONFORMITÉ

6.1 Registre des traitements

La Caisse tient à jour un registre des Traitements des Renseignements personnels. Ce registre devra être mis à disposition des autorités de contrôle sur demande.

6.2 Analyse d'impact sur la protection des données

Lorsqu'un type de Traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du Traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, la Caisse effectue, avant le Traitement, une analyse de l'impact des opérations de Traitement envisagées sur la protection des Renseignements personnels.

6.3 Portail dédié à la conformité en matière de protection des renseignements personnels

La Caisse maintient un intranet collaboratif (SharePoint) rassemblant tous les outils et documents devant encadrer et faciliter la gestion des Renseignements personnels et leur protection.

7. DROITS DES PERSONNES CONCERNÉES

Les personnes concernées disposent de certains droits concernant leurs Renseignements personnels :

Droit à l'information

Lorsque des Renseignements personnels relatifs à une personne concernée sont collectés, le Responsable du traitement lui fournit, au moment où les renseignements en question sont obtenus, l'information sur les objectifs du Traitement et les droits dont elle dispose. Le Responsable de traitement doit également lui fournir des informations lorsqu'elles n'ont pas été collectées auprès de la personne concernée, sous réserve des exceptions prévues par la loi.

Droit d'accès

La personne concernée a le droit d'obtenir du Responsable du traitement la confirmation que ses Renseignements personnels sont ou ne sont pas traités et, lorsqu'ils le sont, elle a le droit d'obtenir l'accès auxdits Renseignements personnels ainsi qu'à un certain nombre d'informations complémentaires.

Droit de rectification

La personne concernée a le droit de demander que ses Renseignements personnels soient rectifiés ou complétés, et ce dans les meilleurs délais.

Droit d'effacement (ou droit à l'oubli)

La personne concernée a le droit d'obtenir du Responsable du traitement l'effacement, dans les meilleurs délais, de Renseignements personnels la concernant. Toutefois, ce droit n'est pas général. Il s'applique lorsque :

- les Renseignements personnels concernés ne sont plus nécessaires au regard des finalités pour lesquelles ils ont été collectés;
- la personne concernée retire son consentement au Traitement des Renseignements personnels et il n'existe pas d'autre fondement juridique justifiant le Traitement;
- la personne concernée s'oppose au Traitement et il n'existe pas d'autre fondement juridique au Traitement;
- les Renseignements personnels ont fait l'objet d'un Traitement illicite;
- les Renseignements personnels doivent être effacés pour respecter une obligation légale.

Droit à la limitation des Traitements

La personne concernée a le droit de restreindre le Traitement de ses Renseignements personnels, dans certaines circonstances.

Droit à la portabilité des données

La personne concernée a le droit de recevoir les Renseignements personnels la concernant qu'elle a fournis à un Responsable du traitement, dans un format structuré et couramment utilisé, lorsque le Traitement est fondé sur le consentement direct ou sur un contrat et lorsque le Traitement est effectué à l'aide de procédés automatisés.

Droit d'opposition

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un Traitement de Renseignements personnels la concernant fondé sur l'intérêt public ou l'intérêt légitime du Responsable de traitement, y compris le profilage.

8. SÉCURITÉ

La Caisse et ses sous-traitants mettent en œuvre des mesures visant à assurer la confidentialité et la protection des Renseignements personnels collectés :

Mesures physiques – Il peut s'agir de mesures de sécurité physiques comme des contrôles d'accès aux locaux, salles de serveurs, salles de câblage, au système d'alarme, etc.

Mesures technologiques – Pour protéger les données utilisées par ses divers systèmes d'information, la Caisse met en œuvre plusieurs mesures de sécurité prévues dans la Politique et Directive sur la Gestion et sécurité de l'information.

9. GESTION DES INCIDENTS

Notification en cas de Violation de la confidentialité des Renseignements personnels – En cas de Violation de la confidentialité des Renseignements personnels, la Caisse notifie l'autorité compétente, lorsque requis, dans les plus brefs délais. Le vice-président, Chef éthique et conformité informe les utilisateurs touchés par l'incident.

Suivi et documentation des Violations – En cas de Violation de la confidentialité des Renseignements personnels, la Caisse entreprendra une enquête approfondie sur l'incident de sécurité et prendra les mesures raisonnables pour remédier au risque et minimiser tout dommage potentiel ou futur. La Caisse a mis en place un Plan de gestion des incidents. Enfin, un registre des Violations de la confidentialité des Renseignements personnels est tenu.

10. FORMATION ET POINT DE CONTACT

Formation pour les personnes clés – La Caisse a identifié les personnes qui, dans le cadre de leurs activités professionnelles, sont amenées à traiter des Renseignements personnels. Ces personnes reçoivent une formation adéquate.

Sensibilisation pour l'ensemble des employés – La Caisse réalise régulièrement des activités de sensibilisation destinées à l'ensemble des employés afin de rappeler les règles et principes de protection des Renseignements personnels.

Point de contact – La Caisse a désigné un responsable de l'accès à l'information et de la protection des Renseignements personnels, qui agit en vertu de la Loi sur l'accès :

[redacted]
Vice-président, Chef éthique et conformité
[redacted]

Un Délégué à la Protection des Données (« DPO ») a aussi été nommé pour veiller au respect du Règlement Général Européen sur la Protection des Données :

[redacted]
Directeur principal, juridique
CDPQ London
[redacted]

Toute demande relative à la protection des Renseignements personnels doit être envoyée par courriel à l'adresse suivante : protectionRP@cdpq.com.

11. RÔLES ET RESPONSABILITÉS

VP, Chef éthique et conformité
Désignée responsable de l'accès à l'information et de la protection des Renseignements personnels

- Assurer la mise en œuvre des responsabilités de la Caisse découlant de la Loi sur l'accès, notamment en matière de protection des Renseignements personnels
- Mettre à jour la présente directive

Délégué à la Protection des Données (DPO)

- Veiller au respect du RGPD par la Caisse et interagir avec les autorités européennes de contrôle
- Recevoir et traiter les réclamations des résidents européens concernées par les Traitements

Comité sur l'accès à l'information et la protection des Renseignements personnels

- Recommander la mise en place de mesures relatives à la protection des Renseignements personnels encadrant les activités de la Caisse, en conformité avec les lois et règlements applicables aux organismes publics au Québec et aux exigences du RGPD

Comité stratégique TI

- Recommander l'approbation de la présente directive au Comité de gestion.

12. RÉVISION

La présente directive doit être révisée tous les trois ans, sauf s'il est nécessaire de le faire avant.

ANNEXE 1 : DÉFINITIONS

Les définitions suivantes s'appliquent à la présente directive :

Destinataire
La personne physique ou morale, l'autorité gouvernementale, le service ou tout autre organisme qui reçoit communication de Renseignements personnels.

Renseignement personnel
Est un Renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. Cette définition englobe les données à caractère personnel, au sens du Règlement Général Européen sur la Protection des Données (« RGPD »).

Responsable du traitement
La personne physique ou morale, l'autorité gouvernementale, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant
La personne physique ou morale, l'autorité gouvernementale, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Traitement
Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de renseignements personnels (collecte, utilisation, enregistrement, conservation, modification, consultation, communication, diffusion, rapprochement, effacement, destruction, etc.).

Violation de la confidentialité
Une violation de la confidentialité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de renseignements personnels ou l'accès non autorisé à de tels renseignements.

L.R.Q., chapitre A-2.1

LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

9. Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public.

Ce droit ne s'étend pas aux notes personnelles inscrites sur un document, ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.

1982, c. 30, a. 9.

12. Le droit d'accès à un document s'exerce sous réserve des droits relatifs à la propriété intellectuelle.

1982, c. 30, a. 12.

22. Un organisme public peut refuser de communiquer un secret industriel qui lui appartient.

Il peut également refuser de communiquer un autre renseignement industriel ou un renseignement financier, commercial, scientifique ou technique lui appartenant et dont la divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à l'organisme ou de procurer un avantage appréciable à une autre personne.

Un organisme public constitué à des fins industrielles, commerciales ou de gestion financière peut aussi refuser de communiquer un tel renseignement lorsque sa divulgation risquerait vraisemblablement de nuire de façon substantielle à sa compétitivité ou de révéler un projet d'emprunt, de placement, de gestion de dette ou de gestion de fonds ou une stratégie d'emprunt, de placement, de gestion de dette ou de gestion de fonds.

1982, c. 30, a. 22; 2006, c. 22, a. 11.

23. Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement.

1982, c. 30, a. 23.

24. Un organisme public ne peut communiquer un renseignement fourni par un tiers lorsque sa divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers, sans son consentement.

1982, c. 30, a. 24.

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi.

Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

1982, c. 30, a. 29; 2006, c. 22, a. 16.

37. Un organisme public peut refuser de communiquer un avis ou une recommandation faits depuis moins de dix ans, par un de ses membres, un membre de son personnel, un membre d'un autre organisme public ou un membre du personnel de cet autre organisme, dans l'exercice de leurs fonctions.

Il peut également refuser de communiquer un avis ou une recommandation qui lui ont été faits, à sa demande, depuis moins de dix ans, par un consultant ou par un conseiller sur une matière de sa compétence.

1982, c. 30, a. 37.

39. Un organisme public peut refuser de communiquer une analyse produite à l'occasion d'une recommandation faite dans le cadre d'un processus décisionnel en cours, jusqu'à ce que la recommandation ait fait l'objet d'une décision ou, en l'absence de décision, qu'une période de cinq ans se soit écoulée depuis la date où l'analyse a été faite.

1982, c. 30, a. 39.

§ 6. — *Renseignements ayant des incidences sur la vérification*

53. Les renseignements personnels sont confidentiels sauf dans les cas suivants:

1° la personne concernée par ces renseignements consent à leur divulgation; si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale;

2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

1982, c. 30, a. 53; 1985, c. 30, a. 3; 1989, c. 54, a. 150; 1990, c. 57, a. 11; 2006, c. 22, a. 29.

54. Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.

1982, c. 30, a. 54; 2006, c. 22, a. 110.