Fondaction
Donner du sens à l'argent.

POLITIQUE DE GESTION ET SÉCURITÉ DE L'INFORMATION

Adoptée par le conseil d'administration le 11 novembre 2020

Cette politique remplace la politique de la sécurité de l'information.

1. DÉFINITION

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

2. PRÉAMBULE

Afin de réaliser sa mission, Fondaction recueille, produit, utilise, conserve ou détruit de l'Information abondante qui concerne les actionnaires, les Employés, les entreprises, ainsi que la gestion administrative de Fondaction. L'Information peut revêtir une importance stratégique pour Fondaction et avoir une valeur légale, administrative, financière ou archivistique. En conséquence, il est essentiel de protéger cette Information durant tout son cycle de vie, quel qu'en soit le support ou l'emplacement.

3. MISE EN CONTEXTE

Comme toute autre organisation, Fondaction fait face à une multitude de menaces pouvant porter atteinte à la disponibilité, l'intégrité, l'intégralité et la confidentialité de son Information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol d'identité et d'Information confidentielle, la fraude, l'utilisation, la divulgation et la destruction d'Information, les défaillances techniques et l'erreur humaine.

Fondaction s'assure que la sécurité de l'Information évolue au même rythme que les technologies utilisées et met en place les mécanismes nécessaires afin de bien protéger l'Information qu'il détient.

4. OBJECTIF GÉNÉRAL DOMAINE D'APPLICATION

La Politique de gestion et sécurité de l'Information (ci-après : la « Politique ») fournit des principes généraux sur la sécurité et la protection de l'Information. Les mesures de gestion et de sécurité utilisées doivent permettre :

- ✓ d'assurer la conformité aux lois, politiques et règlements applicables;
- ✓ d'établir les responsabilités et les normes en matière de protection de l'Information;
- ✓ de préserver la confidentialité de l'Information;
- ✓ d'assurer la disponibilité, l'intégrité, l'intégralité et la confidentialité de l'Information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- ✓ d'assurer l'authenticité, la fiabilité et le repérage des Informations par l'adoption de pratiques uniformes en matière de gestion de l'Information ;
- ✓ de se prémunir contre l'altération ou la perte de l'Information;
- ✓ d'empêcher l'accès et l'utilisation de l'Information par des personnes non autorisées ;
- ✓ d'assurer l'archivage ou la destruction des documents en fonction de leur valeur légale, administrative, financière ou archivistique dans le respect du calendrier de conservation et conformément aux bonnes pratiques en vigueur en matière de gestion de l'Information.

Cette Politique chapeaute les directives, procédures et instructions traitant de points précis de gestion et de sécurité de l'Information.

5. CHAMP D'APPLICATION

Cette Politique s'applique sans exception à tous les Employés, administrateurs, RF, RFR et personnes morales ayant accès, sur place ou à l'extérieur des bureaux de Fondaction à l'Information, pour laquelle Fondaction a la responsabilité d'assurer la sécurité (ci-après : les « Utilisateurs »). Elle concerne également l'Information confiée à des tiers et toute forme d'échange ou de communication de l'Information, y compris la prestation électronique de services.

Elle s'applique à toute Information que détient Fondaction dans le cadre de ses activités ou dont elle a la garde, durant tout son cycle de vie, peu importe son support et son emplacement. La Politique vise à assurer la gestion et la sécurité de l'Information à tout moment, notamment, lors de sa création, son traitement, sa communication, sa distribution, son stockage et sa destruction.

6. PRINCIPES DIRECTEURS

Les principes suivants orientent Fondaction en matière de gestion et de sécurité de l'Information :

6.1 Propriété

Toute Information reçue ou créée par un Employé dans le cadre de ses fonctions est la propriété de Fondaction.

6.2 Prudence et diligence

Compte tenu de la nature stratégique des activités de Fondaction, 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.

6.3 Confidentialité de l'information

Toute Information confidentielle doit être protégée contre toute divulgation, de tout accès ou de toute utilisation non autorisée. Conformément à son programme de cybersécurité, Fondaction a mis en place des contrôles stricts face à la protection de l'Information afin d'en assurer la confidentialité.

L'information confidentielle comprend, entre autres, les renseignements personnels des actionnaires, des administrateurs, des Employés, les informations sur les entreprises, ainsi que la documentation interne stratégique et administrative.

6.4 Intégrité de l'information

Conformément à son programme de cybersécurité, Fondaction met en place des contrôles afin que ses Actifs informationnels ne subissent aucune altération ou ne soient pas détruits par erreur ou sans autorisation. La destruction s'effectue conformément au calendrier de conservation. Ces Actifs Informationnels sont également conservés sur un support leur procurant stabilité et pérennité.

6.5 Disponibilité de l'information

Conformément à son programme de cybersécurité, Fondaction assure à ses Utilisateurs que les Actifs informationnels nécessaires dans la réalisation de leurs tâches sont disponibles. Cette disponibilité de l'Information est en ligne avec son programme de continuité des affaires.

6.6 La sécurité physique

Fondaction protège physiquement ses Employés et ses Actifs informationnels contre les menaces d'atteinte à la sécurité et les dangers potentiels pour son environnement (accès illégal aux locaux, incendie, etc.) ainsi qu'à l'accès non autorisé des documents. Des mesures de sécurité physique sont déployées selon la nature des lieux et des actifs à protéger.

6.7 La gestion du plan de continuité des affaires

Fondaction s'assure de la continuité des activités nécessaires à la réalisation de sa mission lors d'un sinistre ou d'une défaillance majeure affectant les Actifs informationnels jugés essentiels. Un plan de continuité des affaires, prévoyant notamment une cellule de crise ainsi qu'une relève informatique, a été élaboré afin de limiter les impacts liés à un incident majeur. L'application de ces mesures facilitera la reprise et la continuité des services essentiels dans les délais prévus aux termes du plan de continuité des affaires.

6.8 Formation et sensibilisation

Fondaction offre un programme de sensibilisation à la sécurité de l'Information. Tout utilisateur (ce qui inclut les Employés, les fournisseurs de service et les consultants ayant accès à l'Information de Fondaction) doit se soumettre à ce programme. De plus, des formations plus ciblées sont obligatoires pour le personnel de la vice-présidence, Transformation numérique et systèmes d'information (TNSI) responsable d'assurer la sécurité de l'Information tant au niveau développement qu'au niveau des opérations.

6.9 Imputabilité

Considérant l'impact potentiel de l'exploitation d'une vulnérabilité de sécurité de l'Information sur la confiance des parties prenantes ainsi que sur la réputation et la situation financière de Fondaction, la gestion et la sécurité de l'Information concerne tous les Utilisateurs ayant accès à l'Information de Fondaction. Les vice-présidences sont collectivement imputables des risques liés à la gestion et sécurité de l'Information dans leur qualité de détenteur de l'Information. Cette imputabilité s'applique à l'Information, aux processus et aux systèmes sous leur responsabilité ou leur contrôle, incluant ceux délégués à un tiers.

7. RÔLES ET RESPONSABILITÉS

7.1 Conseil d'administration

Le conseil d'administration adopte la Politique ainsi que toute modification à celle-ci. Il est régulièrement informé des actions de Fondaction en matière de gestion et sécurité de l'Information.

7.2 Comité de Gestion Intégrée des Risques (CGIR)

Le CGIR recommande l'approbation de la Politique au conseil d'administration, s'assure de sa mise en œuvre et en fait le suivi de son application. Le CGIR est informé dans les meilleurs délais possibles par la vice-présidence Gouvernance et gestion des risques des rapports d'incidents susceptibles d'exposer Fondaction à des risques de poursuite judiciaire ou réputationnelle. Il effectue le suivi de l'application des mesures correctives apportées.

7.3 Présidence-direction générale

À titre de plus haut dirigeant de Fondaction, il fait partie du rôle de la présidence-direction générale de s'assurer de la gestion et sécurité de l'Information à Fondaction. À cet égard, elle doit s'assurer que chacune des vice-présidences de Fondaction exerce les responsabilités inhérentes à sa tâche dans le cadre de la Politique.

7.4 Comité de sécurité des opérations (CSO)

Le CSO révise cette Politique. Il assure un suivi du programme de cybersécurité, des risques, des incidents, des enjeux, des tendances et des initiatives en matière de sécurité. Le CSO analyse les rapports d'incidents et effectue le suivi de l'application des mesures correctives apportées.

7.5 Vice-présidence, TNSI

La vice-présidence, TNSI formule des recommandations au CSO à l'égard des orientations, de la politique, des directives, des cadres de gestion, des plans d'action et des bilans de sécurité de Fondaction. En outre, elle assure la coordination et la cohérence des actions de sécurité de l'Information menées. Elle assure également la coordination de la reddition de comptes de Fondaction auprès du CGIR.

7.6 Responsable de la sécurité de l'Information

Relevant de la vice-présidence, TNSI, la personne responsable de la sécurité de l'Information recommande les moyens et les mécanismes de sécurité nécessaires pour assurer la protection de l'Information ainsi que la relève des services informatiques nécessaires à la continuité des services essentiels en cas de sinistre. La personne responsable détermine l'équipement et les logiciels qui sont autorisés et assure la mise en œuvre des mesures de sécurité qui sont appropriées et conformes aux attentes définies par la vice-présidence, TNSI. Cette personne collabore avec la vice-présidence, Gouvernance et gestion des risques.

7.7 Vice-présidences

Chaque vice-présidence est tenue de s'assurer que les contrôles relatifs à la gestion et sécurité de l'Information qui sont sous sa responsabilité sont mis en œuvre. Elle a la responsabilité de communiquer à ses Employés l'importance de leurs rôles et les responsabilités qui s'y rattachent.

7.8 Utilisateurs

Fondaction fournit des outils de communication et des ressources informatiques (cellulaires, ordinateurs, réseau, systèmes de courriel, accès internet, connexion à distance) qui sont sa propriété. L'utilisation de ces outils et ressources doit se faire dans le respect des normes de sécurité fixées par Fondaction. L'utilisation restreinte aux fins personnelles est permise pourvu que cela demeure raisonnable. Toutefois, une telle utilisation ne permet pas :

- de divulguer à quiconque et par quelques moyens que ce soit de l'information confidentielle appartenant à Fondaction incluant par le biais des médias sociaux;
- de consulter des sites internet de nature discriminatoire, pornographique, à caractère sexuel ou qui entretiennent des propos haineux, diffamatoires ou calomnieux, ou de participer à des casinos en ligne.

Tout Utilisateur qui accède à l'Information, la consulte ou la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette Information. Il est de sa responsabilité de consulter et de connaître les différentes directives, procédures et instructions qui sont mises à sa disposition afin de respecter ladite Politique de gestion et sécurité de l'Information de Fondaction. Il utilise les Actifs Informationnels de Fondaction seulement dans le cadre de ses fonctions. Aucune utilisation de l'Information à des fins personnelles n'est autorisée.

8. SANCTION

Lorsqu'un Utilisateur contrevient à la présente Politique ou aux directives, procédures ou instructions en découlant, il s'expose à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges d'accès, la réprimande, la suspension, le congédiement et même des poursuites judiciaires, criminelles ou pénales.

9. RESPONSABLE ET RÉVISION

La fréquence minimale de révision est tous les 2 ans ou plus fréquemment si cela s'avère nécessaire.

Annexe 1

Employé : Désigne toute personne à l'emploi de Fondaction incluant les dirigeants, cadres, gestionnaires, les employés syndiqués, les stagiaires, les étudiants travaillant à temps plein ou à temps partiel, à titre permanent ou temporaire. Cette expression englobe également les personnes embauchées sur une base contractuelle, et toute personne qui agit en vertu d'une entente, d'un contrat d'emploi ou d'un mandat dans la mesure prévue à cette entente, ce contrat ou ce mandat.

Actif informationnel : Toute information, quel que soit son canal de communications ou son support, une plateforme technologique et solution d'affaires numériques ou une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par Fondaction et sous sa responsabilité.

Information : La notion d'information au sens de la présente Politique vise :

- les renseignements personnels;
- l'information confidentielle;
- l'information privilégiée;
- l'information protégée par le secret professionnel;
- la documentation interne stratégique et administrative;
- toute autre information qui constitue une « information confidentielle » au sens du code d'éthique et de conduite de Fondaction.

Information confidentielle : Désigne toute information ayant trait à Fondaction, 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 quelconque ou de compromettre la réalisation d'une opération à laquelle Fondaction participe. La présente définition englobe également toute information relative aux investissements ou aux personnes morales, sociétés et fonds d'investissement dans lesquels Fondaction détient ou examine une participation.

Renseignement personnel : Désigne tout renseignement concernant une personne physique ou qui permet de l'identifier. Tout renseignement personnel constitue une information confidentielle.