Titre	Approbation	Date de première approbation
Politique de gestion et sécurité de l'information	Conseil d'administration	11 novembre 2020
	Dates de révision • Modifiée le 21 décembre 2023 • Modifiée le 13 décembre 2024 avec entrée en vigueur au 1er janvier 2025	
Vice-présidence responsable Transformation numérique et systèmes d'information	**Commentaires** S.O.	

Table des matières

1 Préambule

Fondaction, le Fonds de développement de la Confédération des syndicats nationaux pour la coopération et l'emploi (« **Fondaction** »), dans le cadre de ses opérations d'affaires, recueille, détient, traite, utilise, communique et détruit de l'Information sous plusieurs formes et ce, que ce soit directement ou par l'entremise de 9525-9495 Québec inc., aussi connue comme étant « Le Regroupement entre Bâtirente et Fondaction », personne morale régie par la *Loi sur les sociétés par actions*, immatriculée au registre des entreprises sous le numéro 1180227242 ainsi que ses successeurs ou ayants cause (aux présentes, le « **Regroupement** ») ou avec des Tiers.

Comme toute autre organisation dans le même domaine d'affaires au Québec et au Canada, Fondaction fait face à une multitude de menaces pouvant porter atteinte à la Confidentialité, l'Intégrité et la Disponibilité des Informations qu'il détient directement ou indirectement via le Regroupement ou des Tiers. Ces menaces, en constante évolution, peuvent provenir de plusieurs sources tant de l'externe que de l'interne.

Fondaction directement ou par l'entremise du Regroupement surveille de manière constante les principaux risques liés aux Actifs informationnels et met en place divers mesures et contrôles de sécurité pour atténuer ces risques à des niveaux acceptables pour Fondaction. De ce fait, Fondaction vise à avoir des contrôles efficaces dans l'identification, la protection, la détection, la réponse et le recouvrement des Actifs informationnels qui sont proportionnels en fonction des évaluations de risque de ces menaces (probabilité d'occurrence et impact potentiel) et du seuil de tolérance énoncé.

La saine gestion et la sécurité de l'Information visent à être un levier essentiel pour la réalisation des ambitions commerciales et stratégiques de Fondaction. Tout en soutenant la mission de Fondaction, elles favorisent la création de valeur. Par conséquent, la gestion et la sécurité de l'Information sont intégrées de manière fluide dans les processus, optimisant ainsi la performance, la fiabilité et la conformité des opérations.

2 Objectif

La *Politique de Gestion et Sécurité de l'Information* (« **Politique** ») fournie des principes généraux qui sont alignés sur les mêmes principes en place pour gérer les autres risques auxquels Fondaction assure la gestion. La Politique vise à :

- Permettre un alignement de la gestion et la sécurité de l'Information aux obligations légales applicables;
- Compléter l'encadrement découlant des documents suivants:
    - Code d'éthique et de conduite applicables;
    - *Politique sur la confidentialité et la protection des renseignements personnels*;
    - *Politique de gestion intégrée des risques.*
- Permettre l'établissement des priorités d'entreprise en termes de transformation organisationnelle, d'évolution technologique et du seuil de tolérance aux risques de sécurité de l'information énoncé;

- Consacrer une structure de gouvernance basée sur le modèle des trois lignes de défense établissant, entre autres, les mécanismes de reddition de comptes sur les indicateurs d'efficacité de contrôle et de risques de sécurité, des prises de décisions face aux risques et de suivi des actions de remédiation selon les cas.

3 Champ d'application

Cette Politique s'applique à toutes les personnes visées à la section 6.

Cette Politique chapeaute un cadre normatif de sécurité qui inclut les directives, procédures et instructions portant sur des points précis de gestion et de sécurité de l'Information.

4 Définitions

« Actif informationnel »	Actif composé ou supportant de l'Information. Cela inclut les connaissances, les données ainsi que les documents et les supports tangibles ou intangibles (ex. : papier, matériel, logiciel, réseau, personne) permettant son traitement, son exploitation, sa transmission ou sa conservation aux fins d'utilisation prévue.
« CGRSI »	Le Comité de Gestion des Risques de Sécurité de l'Information (CGRSI) du Regroupement est conçu pour faire une reddition de compte sur la sécurité opérationnelle et gérer efficacement les risques liés à la sécurité de l'information. Il vise à renforcer la posture de sécurité en supervisant la gestion des risques de sécurité de l'information qui est communiqué au Comité de Gestion Intégrée des Risques (CGIR) de Fondaction.
« Dérogation de sécurité »	Écart dans l'application des exigences ou des contrôles de sécurité pouvant changer la posture de risque.
« Disponibilité »	Propriété de l'Information d'assurer ses fonctions sans interruption ou délai au moment où la sollicitation en est faite.
« Information »	Vise, peu importe le support ou la technologie en cause : les Renseignements personnels, l'Information confidentielle, l'Information privilégiée et l'information protégée par le secret professionnel qui sont sous le contrôle de Fondaction ou qui sont confiés au Regroupement ou à un Tiers par Fondaction.
« Information confidentielle »	Désigne toute information qui n'est pas connue du public ayant trait à Fondaction, ses filiales et personnes morales dans lesquelles il détient un investissement ou examine la possibilité d'un investissement, incluant notamment et sans s'y limiter : toute information relative à la propriété intellectuelle, les notes, les droits d'auteur, les marques de commerce, les noms commerciaux et les secrets commerciaux, et toute information de nature stratégique, commerciales, financières, légales ou techniques, y compris mais sans s'y limiter, toute information

	relative à des produits, services, investissements, placements, clients, actionnaires, fournisseurs, employés du Regroupement, méthodologies, plans d'affaires, matériel et logiciels, informatiques, technologies, systèmes, codes source, profits, plans stratégiques, plans de publicité et de marketing, opinions, analyses, rapports, données financières, états financiers, prévisions, négociations, offres, promesses de contracter, contrats et relations commerciales.
« Information privilégiée »	Désigne 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'un émetteur ayant fait un appel public à l'épargne, incluant, sans limiter la généralité de ce qui précède, toute information concernant l'un ou l'autre des événements suivants : une émission de titres, un changement dans les politiques de dividendes, un changement important quant à la propriété des titres qui pourrait avoir un effet sur le contrôle de l'émetteur, un changement important dans la composition de la direction, de même qu'un changement important relatif à la situation financière, aux affaires ou aux clients.
« Intégrité »	Propriété de l'Information de ne subir aucune altération accidentelle ou non autorisée permettant de la maintenir dans son intégralité de façon stable et pérenne.
« Renseignement personnel »	Désigne tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
« Tiers »	Personne physique ou morale, autre qu'un Utilisateur, qui recueille, détient, utilise, communique ou détruit des Informations pour le compte de Fondaction.
« Utilisateur(s) »	Désigne toute personne physique à l'emploi du Regroupement incluant les dirigeants, cadres, gestionnaires, les salariés syndiqués, les stagiaires, les étudiants travaillant à temps plein ou à temps partiel, à titre permanent ou temporaire. Cette expression englobe également tout responsable Fondaction, responsable régional Fondaction, administrateur, membre de comité et toute personne qui est assujettie à la Politique en vertu d'un contrat et dans la mesure prévue à ce contrat (exemple : consultant).

5 Principes directeurs

Les principes suivants guident les mesures prises en matière de sécurité de l'Information :

— Évolution : les pratiques et les solutions retenues en matière de sécurité de l'Information doivent être réévaluées périodiquement et actualisées afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques de sécurité de l'Information sous-jacents ;

— Responsabilité et imputabilité : l'efficacité des mesures de sécurité de l'Information exige l'attribution claire des responsabilités et des mesures claires à l'égard des Tiers, et la mise en place de processus de gestion de la sécurité de l'Information permettant une reddition de comptes adéquate ;

— Universalité : les pratiques et les solutions retenues en matière de sécurité de l'Information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées dans le domaine d'affaires (afin d'en faciliter la gestion, l'opération et la maintenance par exemple).

— Alignement avec les opérations et la transformation organisationnelle : En sécurité de l'Information, la vue holistique des menaces, des scénarios de risques et de l'évaluation de l'efficacité des contrôles de sécurité est primordiale. Fondaction s'assure que la posture de sécurité de l'Information évolue au même rythme que les scénarios de menaces, qu'elle considère la transformation organisationnelle ainsi que l'évolution technologique tout en étant aligné sur le niveau de risque acceptable.

6 Rôles et responsabilités

Les rôles et responsabilités concernant la gestion et la sécurité de l'Information s'appuient sur le Modèle des Trois Lignes de l'Institut des Auditeurs Internes. De ce fait, plusieurs parties prenantes sont impliquées dans le modèle et le rôle de chacune est présenté ci-dessous :

6.1 Organe de Gouvernance

6.1.1. Conseil d'administration (« CA ») de Fondaction

- Adopte la Politique ainsi que toute modification à celle-ci lorsque requis.
- Approuve la structure et le processus de reddition sur la posture de sécurité de l'Information.
- Sur recommandation du CGIR, définit le niveau de tolérance au risque.
- Est informé, selon le processus de reddition de compte en place, sur la posture de risques de sécurité portant, entre autres, sur les principaux scénarios de risques de sécurité et les indicateurs de risques sous-jacents, les contrôles clés de sécurité et les indicateurs de performance sous-jacents, la portée et l'avancement du programme de sécurité, les incidents de sécurité significatifs, l'état des Dérogations de sécurité et du programme de sensibilisation à la sécurité de l'Information.

6.1.2. Comité de Gestion Intégrée des Risques (« CGIR ») de Fondaction

- Recommande au CA l'approbation de la Politique et de ses modifications, lorsque requis, et surveille sa mise en œuvre.
- Recommande au CA, le niveau de tolérance au risque qui devrait être défini.
- Effectue au CA la reddition de la posture de sécurité de l'Information.
- Recommande au CA la structure et le processus de reddition permettant la prise de décision éclairée à l'égard de la posture de sécurité de l'Information et des risques sous-jacents.

6.1.3. Présidence et direction générale

- S'assure que chacune des vice-présidences du Regroupement exerce les responsabilités inhérentes à sa tâche dans le cadre de la Politique.
- S'assure d'avoir régulièrement, selon le processus de reddition, les Informations requises sur l'environnement de contrôles, les indicateurs d'efficacité des contrôles et les indicateurs de risques de sécurité de l'Information pour être en mesure d'apprécier la posture de risques de sécurité de l'Information et pouvoir à son tour s'assurer de l'alignement versus le niveau de tolérance aux risques de sécurité de l'Information établis par le conseil d'administration.
- Est impliqué plus particulièrement dans le processus de reddition des incidents de sécurité de l'Information et du plan de réponse.

6.2 Première ligne

6.2.1. Vice-présidence, TNSI du Regroupement

- Agit à titre de promoteur du programme de sécurité de l'Information.
- Arrime en continu et de façon transparente les plans stratégiques TI et de la sécurité de l'Information avec les stratégies d'affaires tout en considérant la capacité actuelle et requise dans le futur.
- Établit et maintient une architecture d'entreprise comprenant les processus, Informations, données et couches d'architectures d'applications, de technologies et de sécurité.
- S'assure d'avoir des processus en place pour gérer les Actifs informationnels de nature technologique tout au long de leur cycle de vie.
- S'assure que les objectifs d'affaires, le niveau de tolérance aux risques de sécurité de l'Information, ainsi que son alignement avec celui-ci, sont énoncés, communiqués et respectés.

6.2.2. Direction de la Gouvernance et de la Cybersécurité du Regroupement

- Définit et applique le cadre normatif de sécurité, découlant de la Politique, proportionnellement à la criticité des Actifs informationnels.
- Établit et maintient, en collaboration avec le Comité de Gestion de Risques de Sécurité de l'Information du Regroupement (« CGRSI ») et les propriétaires des Actifs informationnels, le cadre de classification des Actifs informationnels.

- Assure la reddition sur la posture de risque de sécurité de l'information en continu et rapporte celle-ci au Comité de Gestion des Risques de Sécurité de l'Information du Regroupement (« CGRSI ») et autres instances si nécessaire.
- Développe et met en œuvre une pratique de gestion des risques de sécurité de l'information (incluant les Tiers) comprenant l'identification des menaces (internes et externes) et l'amélioration continue des contrôles de sécurité, en fonction du seuil de tolérance aux risques.
- Fournit un accompagnement tout au long du cycle des projets afin d'apporter l'expertise en matière de sécurité de l'Information.
- S'assure qu'un mécanisme de gestion des incidents liés à la sécurité de l'Information est en place et qu'une reddition est faite en fonction de leur sévérité, en harmonie avec le processus de gestion des incidents de confidentialité.
- Établit, opère et rapporte sur le processus et le suivi des Dérogations de sécurité.
- Met en œuvre un programme de sensibilisation et de formation continu à la sécurité de l'Information afin d'amener les Utilisateurs à adopter des comportements qui n'exposent pas Fondaction à des risques de sécurité de l'Information et ainsi instaurer et faire vivre une culture de prudence et diligence.
- Mène une vigie sur les meilleures pratiques et normes dégagées au niveau national et international ainsi qu'une veille des risques émergents.

6.2.3. Vice-présidences du Regroupement

- Communique aux Utilisateurs sous sa responsabilité l'importance de leurs rôles dans les contrôles relatifs aux processus d'affaires et les responsabilités qui s'y rattachent.
- Veille à ce que les Utilisateurs sous sa responsabilité participent au programme de sensibilisation et de formation à la sécurité de l'Information et le mettent en application.
- S'assure que les Utilisateurs sous sa responsabilité respectent la Politique et toutes autres exigences du cadre normatif de sécurité de l'Information qui découle de cette Politique.
- Assume leur rôle de propriétaire d'Actif informationnel pour lesquels ils ont été désignés.

6.2.4. Propriétaire d'Actifs informationnels

- S'assure que les contrôles relatifs à la sécurité de l'Information, qui sont sous sa responsabilité (processus d'affaires), sont mis en œuvre pour atténuer les risques de sécurité au niveau acceptable.
- Soutient l'exécution des contrôles de nature technologique réalisés à la VP TNSI du Regroupement, tout en demeurant responsable et imputable des décisions concernant les stratégies de réponse aux risques qui s'appliquent à ses Actifs informationnels.

- Collabore avec la Direction de la Gouvernance de la Cybersécurité du Regroupement pour classifier les Actifs informationnels sous sa responsabilité, procéder aux évaluations de risques, émettre les indicateurs de risques et établir les actions requises en vue d'améliorer l'efficacité des contrôles de sécurité sous sa responsabilité si requis (exemple : plans de remédiation).
- S'assure que le niveau de risque de sécurité de l'Information relié à ses actifs est aligné avec le niveau de tolérance aux risques approuvé par le conseil d'administration de Fondaction.
- Doit s'assurer de respecter le cadre de gestion documentaire.

6.2.5. Utilisateurs

- Est responsable de se conformer à la Politique et de respecter également toutes les autres exigences du cadre normatif de sécurité de l'Information qui découle de cette Politique.
- Doit participer au programme de sensibilisation et de formation à la sécurité de l'Information et appliquer les bonnes pratiques de sécurité de l'Information dans le cadre de ses fonctions.
- Doit rapidement signaler tout incident de sécurité de l'Information dont il serait témoin selon le processus établi.
- Doit respecter les contrôles de sécurité en place et ne pas tenter de les contourner.

6.2.6. Vice-présidence, GGR (Gouvernance et Gestion des Risque), Direction affaires juridiques du Regroupement

- Établit et maintient le cadre de gestion documentaire permettant une saine gestion de l'Information afin d'assurer la conformité de Fondaction aux lois applicables.

6.2.7. Vice-présidence, Ressources humaines

- Réalise des contrôles adaptés au niveau de risque lié aux fonctions occupées par une personne, ce qui comprend notamment la vérification des antécédents d'Utilisateurs.

6.3 Deuxième ligne

6.3.1. Comité de Gestion des Risques de Sécurité de l'Information (« CGRSI ») du Regroupement

- Assure la reddition auprès du CGIR de Fondaction sur la posture de risques de sécurité de l'Information portant, entre autres, sur les principaux scénarios de risques de sécurité retenus et leurs indicateurs, les contrôles clés et leurs indicateurs, la portée et l'avancement du programme de sécurité, les incidents de sécurité significatifs, l'état des Dérogations de sécurité, le suivi du programme de sensibilisation à la sécurité de l'Information et le suivi des remédiations selon le cas.

- Fournit des orientations sur la manière d'escalader les décisions concernant les risques lorsqu'elles dépassent le niveau d'autorité ou de tolérance pouvant être du ressort du propriétaire de l'Actif informationnel concerné.
- Veille à ce que les décisions prises en matière de gestion des risques soient documentées et communiquées de manière appropriée.

6.4 Troisième ligne

6.4.1. Vice-présidence, GGR, Conformité et gestion des risques du Regroupement

- Assume la fonction d'audit interne et fournit une opinion indépendante et objective sur la suffisance, la conception et l'efficacité de la structure de gouvernance et des contrôles en place et par conséquent, sur la reddition de la posture de risque de sécurité afin de notamment rendre compte au conseil d'administration.

7 Responsable et révision

L'application et la révision de la politique sont sous la responsabilité de la vice-présidence Transformation numérique et systèmes d'information du Regroupement. La fréquence minimale de révision est tous les trois (3) ans ou plus fréquemment si cela s'avère nécessaire.