TITRE	INSTANCE APPROBATRICE
Politique – Sécurité des actifs informationnels et technologiques	Conseil d'administration
SECTEUR ÉMETTEUR	DATE
PVP Technologies	2022-06-10

LOIS, POLITIQUES ET DIRECTIVES LIÉES

- Lois :
  - Sur les archives
  - Sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
  - Concernant le cadre juridique des technologies de l'information
  - Sur la gouvernance et la gestion des ressources informationnelles des organismes publics
- Code d'éthique et de déontologie à l'intention des dirigeants et des employés
- Politique - Divulgation de l'information financière
- Directives :
  - Utilisation sécuritaire et acceptable des actifs informationnels et technologiques
  - Mesures administratives et disciplinaires en cas de manquement au Code d'éthique et de déontologie
  - Protection des renseignements personnels
  - Gestion de l'information privilégiée
- Guide opérationnel - Sécurité des actifs informationnels et technologiques

OBJECTIFS

- Établir les principes guidant le cadre de gestion de la sécurité des Actifs informationnels et technologiques de la CDPQ
- Promouvoir une saine culture de gestion des risques de cybersécurité à tous les paliers de l'organisation
- Définir les rôles et responsabilités des intervenants et la structure de gouvernance
- Établir l'encadrement des principaux risques de cybersécurité auxquels la CDPQ est exposée

1. Définitions

Les termes commençant par une majuscule sont définis dans la présente *Politique – Sécurité des Actifs informationnels et technologiques* (la « Politique »). Les termes en italique réfèrent à des documents officiels de la CDPQ.

- Actif informationnel : Toute ressource apportant des éléments d'Information qui est utilisée par la CDPQ. Cela comprend notamment les Informations, les Documents, les bases de données et les progiciels métiers, ou un ensemble de ces éléments acquis ou constitués au sein de la CDPQ, qu'ils soient hébergés à la CDPQ ou non.
- Actif technologique : L'ensemble du matériel informatique, des logiciels et des services utilisés pour la collecte, le traitement et la transmission des Actifs informationnels. Cela comprend notamment les postes de travail, téléphones, tablettes, claviers et autres périphériques d'entrée ou de sortie des données. Les logiciels incluent notamment les logiciels de traitement de texte, systèmes

d'exploitation des postes de travail, serveurs et équipement informatiques, progiciels métiers, outils de gestion réseaux, outils de développement, didacticiels et pilotes de périphériques.

- 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.
- Cybersécurité : Ensemble des processus et moyens utilisés pour assurer la sécurité des Actifs informationnels et technologiques de la CDPQ face aux acteurs malveillants, internes ou externes à la CDPQ. Elle vise la protection contre le risque de perte ou de divulgation d'informations sensibles de la CDPQ, ainsi que le risque de dégradation ou d'interruption des fonctions d'affaires critiques de la CDPQ découlant d'un incident de cybersécurité.
- 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.
- Information : Données, indications, ensemble de renseignements, incluant des Renseignements personnels, consignés par la CDPQ sur un Document ou détenus par la CDPQ, y compris une Information provenant d'un tiers.
- Personne : Tout individu travaillant pour la CDPQ, à temps plein ou partiel, ou qui dispose d'un accès (sur site ou à distance) à un Actif informationnel ou technologique de la CDPQ. Ceci inclut, sans s'y limiter, les employés réguliers et occasionnels, les entrepreneurs, les consultants, les étudiants, les stagiaires et tout autre travailleur de la CDPQ.
- Responsable de données : Personne responsable d'un Actif informationnel, tel que défini dans la Politique. Ce rôle est octroyé au producteur d'une donnée et/ou au propriétaire d'un dépôt de données (ex : site SharePoint) œuvrant au sein des lignes d'affaires de la CDPQ. Ses responsabilités sont définies dans la section *Gouvernance* de cette Politique.
- Responsable de produit numérique : Personne responsable d'un Actif technologique de type produit. Ceci inclut les applications-métier et les solutions numériques développées à l'interne ou acquises à l'externe, qui sont mises en place dans l'environnement technologique de la CDPQ pour répondre à ses besoins d'affaires. Ses responsabilités sont définies dans la section *Gouvernance* de cette Politique.
- Responsable de plateforme numérique : Personne responsable d'un Actif technologique, de type plateforme. Ceci inclut les plateformes de cybersécurité, d'infranuagique, de données, d'exploitation et de développement, d'intégration et d'intelligence augmentée. Ses responsabilités sont définies dans la section *Gouvernance* de cette Politique.

2. Mise en contexte

Les menaces de cybersécurité sont en croissance, en constante évolution et de plus en plus complexes. L'adoption de la Politique s'inscrit dans ce contexte et tient compte de l'importance pour la CDPQ de protéger ses Actifs informationnels et technologiques (les « Actifs ») et de mitiger les risques d'incidents de cybersécurité auxquels elle peut faire face.

La Politique concerne toute Personne qui se voit accorder un accès autorisé aux Actifs de la CDPQ, et couvre tous les aspects de ses opérations commerciales, de ses activités et de ses fonctions.

La Politique s'applique à tous les Actifs de la CDPQ, qu'ils soient accessibles et utilisés de façon permanente ou occasionnelle, qu'ils soient fournis par la CDPQ à l'interne ou dans le cadre d'engagements contractuels ou qu'ils soient commercialisés ou accessibles via l'Internet.

3. Principes directeurs

3.1 Propriété et responsabilité des Actifs informationnels et technologiques

La CDPQ est l'unique propriétaire de tout Actif produit ou géré par une Personne, ou auquel une Personne a accès dans le cadre de ses fonctions. Ceci inclut tout Document et toute Information produite ou reçue, ainsi que tout équipement technologique fourni à une Personne.

Ceci exclut les Informations provenant de l'externe qui, bien qu'elles doivent être protégées adéquatement par les Personnes qui y accèdent, demeurent la propriété de leur émetteur initial.

En matière de gestion des Actifs, un responsable désigné (Responsable de donnée, Responsable de produit numérique ou Responsable de plateforme numérique) est associé à chaque Actif. Ce responsable est assigné lors de la création ou de l'introduction d'un Actif. Cette assignation est mise à jour lorsqu'un responsable désigné change de fonction.

Le responsable désigné s'assure, pour les Actifs qui lui sont associés, de faire respecter et d'appliquer les mesures de sécurité énoncées dans la présente Politique et dans les encadrements qui en découlent, tout au long de leur cycle de vie, afin de les sécuriser et de mitiger les risques de cybersécurité.

3.2 Modèle de référence et d'encadrement

La PVP Technologies s'inspire de deux cadres de référence reconnus pour assurer l'exhaustivité, le bien-fondé et la cohérence des encadrements présentés dans la présente Politique, ainsi que dans la Directive et le Guide opérationnel qui en découlent. Ces cadres de référence sont celui du *National Institute of Standards and Technology Cybersecurity Framework* (NIST-CSF) applicable à la cybersécurité et celui du ISO 27001.

Le NIST-CSF, illustré ci-contre, guide la PVP Technologies dans la conception de son programme et dans sa volonté de définir, encadrer et faire évoluer les comportements et pratiques de la CDPQ en matière de sécurité des Actifs. Il se base sur les cinq piliers suivants:

1. **IDENTIFIER**, catégoriser et prioriser les risques de cybersécurité liés aux Actifs. Ce pilier vise à brosser un portrait global des risques liés à la cybersécurité, à prioriser les actions à prendre en fonction de leur évolution et à intégrer les actions priorisées de mitigation de risque dans le programme. Il structure la gouvernance du programme de cybersécurité en se basant sur une approche intégrée de gestion des risques, en lien avec l'appétit pour le risque suivi et entériné au comité de direction.

2. **PROTÉGER** les Actifs face aux risques et menaces. Ce pilier vise à mettre en œuvre des mesures de protection appropriées pour sécuriser les Actifs informationnels et les différentes couches de l'environnement technologique (ex : donnée, application, point de terminaison, réseau) afin de mitiger la probabilité et les risques d'incident de cybersécurité.

3. **DÉTECTER** les événements affectant la sécurité des Actifs. Ce pilier vise à développer et mettre en œuvre des activités appropriées dans l'objectif d'identifier l'occurrence d'un incident, potentiel ou avéré, de cybersécurité. Il inclut les mécanismes de surveillance déployés par la CDPQ afin de vérifier l'efficacité des mesures de protection.

4. **INTERVENIR** en cas d'événement affectant la sécurité des Actifs. Ce pilier vise à développer et mettre en œuvre des processus et activités appropriés pour réagir le plus rapidement et efficacement possible à un incident de cybersécurité détecté, en coordination avec les intervenants internes et externes identifiés. Il vise également à hausser les capacités de la CDPQ à contenir l'impact d'un incident de cybersécurité.

5. **RÉTABLIR** les Actifs et les processus d'affaires critiques de la CDPQ suite à un incident. Ce pilier vise à développer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience de la CDPQ et restaurer les fonctions d'affaires pouvant être dégradées ou interrompues suite à un incident de cybersécurité.

Plus spécifiquement, les principes directeurs à respecter et les mesures à mettre en place en matière de sécurité, inspirés du NIST-CSF et de ISO 27001, sont énoncés dans les documents suivants :

- La *Directive - Utilisation sécuritaire et acceptable des actifs informationnels et technologiques*, qui définit, encadre et précise la manière dont les Personnes doivent faire usage des Actifs.

- Le *Guide opérationnel - Sécurité des actifs informationnels et* technologiques, qui énonce les principes directeurs à respecter et les mesures à mettre en place au sein de la PVP Technologies afin de protéger les Actifs et de mitiger les risques d'incidents de cybersécurité auxquels la CDPQ peut faire face.

3.3 Adoption de comportements sécuritaires et surveillance

Toute Personne est tenue d'utiliser les Actifs de manière responsable et sécuritaire en appliquant les règles énoncées dans la *Directive – Utilisation sécuritaire et acceptable des actifs informationnels et technologiques.*

La direction principale Cybersécurité est responsable du programme de formation et de sensibilisation à la cybersécurité afin de développer une culture CDPQ de cybersécurité. Ce programme vise à renforcer, chez toutes les Personnes, leur responsabilité en matière de cybersécurité et de clarifier le rôle qu'ils doivent jouer pour minimiser ce risque.

La PVP Technologies met en place des mécanismes de surveillance permettant d'identifier des comportements allant à l'encontre des principes directeurs et obligations détaillés dans ses encadrements. Si la PVP Technologies détecte une situation réelle ou potentielle de non-conformité, elle se réserve le droit, avec le soutien et l'accord de la PVP Affaires juridiques et secrétariat et de la PVP Talent et performance, d'enquêter sur l'événement et d'intervenir en fonction des critères énoncés dans la *Directive – Mesures administratives et disciplinaires en cas de manquement au Code d'éthique et de déontologie*.

3.4 Protection des renseignements personnels

La collecte, l'accès, l'utilisation, la conservation, la communication et la destruction 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.

Afin de respecter ses obligations légales en matière de protection des renseignements personnels et de gestion des Documents, découlant notamment de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « loi sur l'accès »), la PVP Technologies se dote d'un Plan de classification[1] et d'un Calendrier de conservation[2]. Tous les Documents doivent être répertoriés selon ce Plan et respecter les règles de conservation établies dans le Calendrier.

4. Sanctions découlant du non-respect de la Politique

Une violation de la Politique peut avoir une incidence importante sur la responsabilité juridique, réputationnelle et sur les opérations de la CDPQ. Conséquemment, le non-respect de la Politique peut entrainer des sanctions, lesquelles sont fonction de la gravité de l'acte commis. Ces sanctions sont imposées en lien avec la *Directive – Mesures administratives et disciplinaires en cas de manquement au Code d'éthique et de déontologie* et peuvent aller jusqu'au congédiement.

[1] Le Plan de classification peut être consulté ici.
[2] Le Calendrier de conservation peut être consulté ici.

5. Gouvernance

- Le Conseil d'administration :
  - Révise et approuve la Politique;
  - S'assure que la direction de la CDPQ alloue les ressources humaines et financières nécessaires à la mise en œuvre de la Politique.

- La PVP Technologies :
  - Définit, maintient et assure le respect de la Politique.

- Le Comité risques opérationnels (CRO) :
  - Révise et approuve la *Directive - Utilisation sécuritaire et acceptable des actifs informationnels et technologiques* et le *Guide opérationnel – Sécurité des actifs informationnels et technologiques*, ainsi que les objectifs et la portée des standards qui détaillent les paramètres, exigences particulières et spécificités de mise en œuvre du Guide opérationnel;
  - Entérine les critères d'évaluation des risques de la CDPQ et l'appétit pour le risque de la CDPQ en matière de cybersécurité;
  - Effectue un suivi de l'évolution de la posture de cybersécurité en lien avec l'appétit pour le risque de la CDPQ en matière de cybersécurité.

- La Direction des risques et relations avec les déposants :
  - Accompagne la direction principale Cybersécurité dans le suivi de ses risques prioritaires;
  - Effectue une revue objective des activités de cybersécurité.

- Le Comité de sécurité globale (CSG) :
  - Donne la vision et les orientations stratégiques en matière de cybersécurité, en plus d'assurer l'alignement des décisions prises en lien avec l'appétit pour le risque de la CDPQ;
  - Confirme les objectifs, les priorités et les orientations du programme de cybersécurité de la CDPQ;
  - Effectue le suivi de l'exécution des initiatives de transformation du programme de cybersécurité de la CDPQ et le suivi de l'évolution de la posture de cybersécurité qui en découle;
  - Entérine les standards de sécurité des Actifs informationnels et technologiques, ainsi que les positionnements de cybersécurité découlant de la Politique;
  - Effectue le suivi des incidents majeurs de cybersécurité, des dérogations et exclusions, des indicateurs de performance et de l'évolution du programme de culture de cybersécurité.

- Le Comité sur l'accès à l'Information et la protection des renseignements personnels:
  - Définit, maintien et assure le respect de la *Directive – Protection des Renseignements personnels;*
  - Approuve les règles encadrant la gouvernance que la CDPQ doit adopter à l'égard des Renseignements personnels.

- La direction principale Cybersécurité :
  - Dresse un portrait global des risques liés à la cybersécurité, priorise les actions à prendre en fonction de leur évolution et intègre les actions de mitigation de risque priorisées dans le programme de cybersécurité de la CDPQ;
  - Planifie et déploie le programme relatif au développement d'une culture de cybersécurité, incluant les formations et activités de sensibilisation qui y sont associées;
  - Développe et met en œuvre :

        - Les mesures de protection requises pour protéger les Actifs informationnels et technologiques de la CDPQ et ainsi limiter les risques d'incident de cybersécurité;
        - Les activités appropriées dans l'objectif d'identifier l'occurrence d'un incident, potentiel ou avéré, de cybersécurité;
        - Les processus et activités appropriées pour réagir le plus rapidement et efficacement possible à un incident de cybersécurité détecté, en coordination avec les intervenants internes et externes identifiés;
    - Définit, maintien et assure le respect de la Directive, du Guide opérationnel et des standards découlant de la Politique.

- Les Responsables de donnée, Responsables de produit numérique et Responsables de plateforme numérique :
    - Appliquent les mesures de sécurité énoncées dans la présente Politique, et dans les Directives qui en découlent, tout au long du cycle de vie des Actifs dont ils sont imputables;
    - Déterminent les exigences de sécurité spécifiques aux Actifs dont ils sont imputables, lesquelles doivent être conformes au cadre normatif;
    - Attribuent la cote de classification ou la catégorisation des Actifs dont ils sont imputables et assurent une revue de ce classement et du niveau de sécurité de manière périodique;
    - Approuvent l'attribution des droits d'accès aux Actifs dont ils sont imputables, en fonction des besoins requis.

6. Vérification et contrôle

Un processus de contrôle spécifique est mis en œuvre par la CDPQ pour surveiller et examiner le rendement et l'efficacité des encadrements et mesures de sécurité et vérifier la conformité aux exigences juridiques et réglementaires. Il comprend des tests et des contrôles adaptés menés par la direction principale Cybersécurité à sa discrétion.

Les leçons tirées de ces contrôles et vérifications sont réutilisées en vue d'un traitement systématique et orientent les actions de la Politique et du cadre de gestion de la sécurité des Actifs informationnels et technologiques.

7. Révision

La présente Politique est révisée au minimum tous les trois ans.