



Politique de gestion de l'information

1.1 Aperçu

La gestion des ressources informationnelles est une composante essentielle des activités du Partenariat. Ces ressources composent le capital intellectuel sur lequel le Partenariat s'appuie pour la prestation de services. Leur gestion fait appel à des pratiques exemplaires, à des politiques et à des normes qui mènent à leur utilisation de manière efficace, responsable et rentable. La gestion de l'information garantit que des caractéristiques essentielles, comme l'authenticité, la fiabilité, l'intégrité et la facilité d'utilisation des renseignements sont préservées et protégées tout au long du cycle de vie de l'information.

Le Partenariat doit fournir l'accès à ses ressources informationnelles, les gérer, les préserver et les éliminer convenablement, conformément aux lois, aux politiques et aux normes pertinentes, pour :

- i. assurer la reddition de comptes;
- ii. fournir des preuves de ses activités et de sa structure organisationnelle;
- iii. documenter ses responsabilités, ses privilèges et ses droits;
- iv. préserver les ressources informationnelles de valeur durable.

Cette Politique fournit à l'organisation des conseils de gestion précisant ce qui doit être fait par rapport à la gestion de l'information; elle ne précise pas comment la politique doit être mise en œuvre. Le manuel des normes de la politique de cybersécurité du Partenariat détaille les modalités de mise en œuvre de la présente politique. Le Partenariat pourrait, à sa seule discrétion, imposer des directives supplémentaires en la matière.

1.2 Objet

La présente politique a pour but de définir des règles pour gérer l'information de manière à protéger les renseignements personnels et la sécurité des ressources informationnelles du Partenariat. Les règles :

- i. Attribuer des responsabilités et l'obligation de reddition de comptes pour la gestion des renseignements administrés par le Partenariat ou qui sont sous son contrôle. Afin de faciliter la compréhension et le respect de cette politique, l'ensemble du personnel du Partenariat recevra une formation de sensibilisation à la sécurité et à la protection des renseignements personnels.



- ii. Favoriser la conformité aux lois, aux politiques et aux normes pertinentes.
- iii. Encourager la création et la conservation de dossiers complets et exacts, en consignait les décisions et les mesures prises dans des documents officiels.
- iv. Exiger que des renseignements pertinents soient fournis en temps utile, de matière utilisable, rentable et précise.
- v. Permettre la préservation de l'information du Partenariat d'une façon qui conserve l'authenticité, la fiabilité, l'accessibilité et l'intégrité de l'information aussi longtemps que nécessaire.
- vi. Soutenir un accès transparent et efficace aux ressources informationnelles dans le respect des restrictions légales en matière de vie privée et de confidentialité.

1.3 Portée

Cette politique s'applique à tous les employés, consultants et sous-traitants du Partenariat qui gèrent les ressources informationnelles de l'organisation ou qui élaborent des procédures, des normes et des politiques opérationnelles pour encadrer la gestion des ressources informationnelles du Partenariat.

1.4 Énoncés de politique

1.4.1 Gouvernance de l'information

- i. Le Partenariat doit gérer tous les renseignements créés et reçus dans le cadre de ses activités opérationnelles.
- ii. Il doit établir et maintenir un programme de gestion de l'information pour gérer la conception, l'intégrité, la disponibilité et l'utilisation efficace des systèmes de gestion de l'information.
- iii. Les ressources informationnelles doivent être identifiées, classées, inventoriées, consignées et maintenues pendant tout leur cycle de vie.
- iv. Les documents officiels du Partenariat doivent être gérés et conservés afin qu'ils demeurent authentiques, fiables, dignes de foi, sécurisés, complets et accessibles au fil du temps et des emplacements, peu importe le support ou le format.



1.4.2 Classification et conservation des renseignements du Partenariat

- i. Le Partenariat doit élaborer, mettre en œuvre et maintenir un système de gestion des dossiers, avec des calendriers détaillés et continus de conservation et d'élimination des renseignements, pour gérer tous les documents et renseignements en format électronique.
- ii. Le Partenariat doit élaborer, maintenir et promouvoir un schéma de classification de l'information pour toutes ses ressources informationnelles.
- iii. L'information du Partenariat doit demeurer authentique, fiable et accessible après toute conversion ou migration d'un support, d'un format ou d'un système à un autre.

1.4.3 Stockage et élimination de l'information du Partenariat

- i. L'information du Partenariat doit être éliminée de manière sécurisée, conformément aux calendriers de conservation et d'élimination des renseignements et aux processus de gestion des ressources, comme ils sont définis dans le manuel de cybersécurité du Partenariat.
- ii. L'information du Partenariat dont la conservation dans les archives est prévue doit être conservée de manière à préserver son intégrité et son authenticité jusqu'au transfert aux archives du Partenariat, et pendant celui-ci.
- iii. L'information du Partenariat dont la destruction est prévue doit être détruite d'une manière adaptée au support d'information sur lequel elle est stockée, et de façon à assurer la sécurité de l'information et la protection des renseignements personnels des individus. Les dossiers d'affaires officiels et les communications – comme les documents d'importance historique, les courriels ou les messages instantanés – peuvent être exemptés de la destruction conformément à la présente politique.

1.5 Contrôle de l'application de la politique

En cas de non-respect de cette politique, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

- i. Refuser l'accès à ses ressources informationnelles et à ses technologies de l'information.
- ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.



- iii. Mettre en œuvre, pour les employés, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement, la cessation immédiate de l'emploi ou des poursuites en vertu de la loi.

1.6 Définitions

Terme	Définition
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portables et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou de TI
Dossiers officiels	Les dossiers officiels sont ceux qui fournissent l'information la plus exhaustive et concluante par rapport à une mesure ou un événement en particulier. Le dossier officiel peut être composé de différents supports. Des dossiers électroniques peuvent constituer le dossier officiel. La responsabilité de la conservation du dossier officiel est attribuée dans la structure de classification des dossiers. Les dossiers officiels : <ul style="list-style-type: none"> • Sont nécessaires pour soutenir les activités • Documentent les transactions et fournissent des preuves de celles-ci • Démontrent la conformité aux exigences en matière de responsabilité ou à d'autres exigences • Auront une valeur financière, juridique, informative ou archivistique future

1.7 Documents connexes – [Lien du dossier de gestion des documents](#)

- Énoncé de confidentialité
- Politique de cybersécurité
- Manuel des normes de la Politique de cybersécurité
- Politique de gestion des dossiers

Fin du document