**Modèle de gestion de la confidentialité des données et de la cybersécurité**

**Pratique de référence** : S0.1 & 2 - Gestion de la confidentialité des données et de la cybersécurité

**Classes d'actifs applicables** : Bureaux, Centres commerciaux fermés et à aire ouverte, Industriel léger, Soins de santé, Universel et IRLM

|  |
| --- |
| ***Instructions :****Tous les textes en italique gris avec des bordures sont des instructions qui vous aideront à préparer la pratique de base requise pour le modèle de confidentialité des données de votre bâtiment.* 1. *Remplacer tous les* [textes bleus entre parenthèses] *du document par des informations sur la confidentialité des données du bâtiment.*
2. *Le cas échéant, accomplissez les tâches nécessaires, ou engagez un consultant tiers pour les accomplir, afin d'être en mesure de remplir les sections pertinentes du modèle.*
3. *Supprimez tout le texte en italique gris lorsque vous avez rempli toutes les sections pertinentes avec des informations spécifiques au bâtiment.*
 |

***Remarque !***

***L'élaboration d'une politique globale de cybersécurité est essentielle pour les organisations informatiques au Canada afin de protéger leurs actifs informationnels et de se conformer aux lois et réglementations nationales. Vous trouverez ci-dessous un guide structuré pour l'élaboration d'une telle politique.***

**Politique de confidentialité des données**

[Insérer le nom et l'adresse du bâtiment]

[Insérer le nom de l'organisation]

[Insérer les coordonnées]

# Objectif de la politique de confidentialité des données

[Insérer l'objectif de la politique de confidentialité des données]

La présente politique de cybersécurité a pour objet d'établir un cadre global permettant de protéger les actifs informationnels de [Nom de l'organisation] contre les cybermenaces, en garantissant la confidentialité, l'intégrité et la disponibilité des données. Cette politique vise à

* **Protéger les actifs informationnels :** Mettre en œuvre des mesures de défense contre l'accès non autorisé, la divulgation, l'altération et la destruction des données de l'organisation.
* **Assurer la conformité réglementaire :** Respecter les lois et réglementations applicables des autorités compétentes, y compris la protection des informations personnelles et les documents électroniques, afin de maintenir des normes juridiques et éthiques.
* **Définir les responsabilités en matière de sécurité :** Délimiter clairement les rôles et les responsabilités en matière de cybersécurité à tous les niveaux de l'organisation afin de favoriser la responsabilisation et la gestion proactive des risques.
* **Promouvoir la sensibilisation à la sécurité :** Cultiver une culture de la sensibilisation à la sécurité par des formations régulières, en donnant aux employés les moyens de reconnaître les cybermenaces potentielles et d'y répondre efficacement.
* **Faciliter la réponse aux incidents :** Établir des protocoles pour la détection, le signalement et la réponse rapide aux incidents de cybersécurité afin de minimiser l'impact et de favoriser un rétablissement rapide.

En atteignant ces objectifs, [Nom de l'organisation] vise à protéger son infrastructure numérique, à soutenir la continuité des activités et à préserver la confiance des clients, des partenaires et des parties prenantes.

***Cette section doit définir l'applicabilité de la politique, en précisant les systèmes d'information, les données, les employés, les sous-traitants et les tiers soumis à la politique.***

# Champ d'application de la politique de confidentialité des données

[Insérer le champ d'application de la politique de confidentialité des données]

Le champ d'application de la présente politique de cybersécurité englobe toutes les personnes et tous les systèmes qui interagissent avec les actifs informationnels de [Nom de l'organisation]. Plus précisément, elle s'applique à:

* Le personnel : Tous les employés, contractants, consultants, personnel temporaire, bénévoles et toute autre personne autorisée à accéder aux systèmes d'information et aux données de [Nom de l'organisation].
* Actifs informationnels : Toutes les données, électroniques ou physiques, détenues, gérées ou traitées par [Nom de l'organisation], y compris les informations confidentielles, sensibles et personnelles.
* Systèmes d'information : L'ensemble du matériel, des logiciels, des réseaux, des applications et des dispositifs (appartenant à l'organisation ou personnels) qui accèdent aux données de [Nom de l'organisation] ou les traitent.

Cette politique s'applique à tous les environnements opérationnels, y compris les sites sur place, les environnements de travail à distance et tout autre scénario dans lequel les ressources d'information de [Nom de l'organisation] sont accessibles ou utilisées. L'adhésion à cette politique est obligatoire pour toutes les parties susmentionnées afin de garantir la sécurité et l'intégrité des ressources d'information de [Nom de l'organisation].

***Cette section doit présenter les objectifs de la politique de cybersécurité, notamment la protection des actifs informationnels, le respect des exigences légales et l'établissement des responsabilités en matière de sécurité au sein de l'organisation.***

# Définitions

[Insérer les définitions]

Dans le cadre de la politique de cybersécurité de [Nom de l'organisation], les définitions suivantes clarifient les termes clés :

* Contrôle d'accès : Mécanismes qui limitent l'accès aux systèmes d'information et aux données aux utilisateurs, processus ou dispositifs autorisés, en veillant à ce que seules les activités permises soient exécutées.
* Informations confidentielles : Données dont l'accès est limité aux personnes autorisées en raison de leur caractère sensible, y compris les données personnelles, les informations commerciales exclusives et toute autre information classée comme confidentielle par [Nom de l'organisation].
* Incident de cybersécurité : Un événement qui compromet la confidentialité, l'intégrité ou la disponibilité des systèmes d'information ou des données, tel qu'un accès non autorisé, une violation des données ou une attaque de logiciels malveillants.
* Cryptage des données : Le processus de conversion des données dans un format codé pour empêcher l'accès non autorisé pendant la transmission ou le stockage.
* Actifs informationnels : Toutes les données, le matériel, les logiciels et les autres composants que [Nom de l'organisation] utilise pour mener à bien ses activités.
* Données personnelles : Informations concernant une personne identifiable, y compris, mais sans s'y limiter, les coordonnées, les numéros d'identification et toute donnée permettant d'identifier une personne de manière unique.
* Évaluation des risques : Le processus systématique d'identification, d'évaluation et de hiérarchisation des risques pour les opérations et les actifs de l'organisation.
* Contrôles de sécurité : Les garanties ou contre-mesures employées pour protéger les systèmes d'information et les données contre les menaces à la sécurité.
* Tiers : Entités externes, y compris les fournisseurs, les partenaires et les prestataires de services, qui interagissent avec les systèmes d'information ou les données de [Nom de l'organisation].

Ces définitions ont pour but de clarifier la présente politique. Pour un glossaire complet des termes relatifs à la cybersécurité, voir le glossaire de l’autorité compétente.

***Cette section doit définir clairement les termes clés utilisés dans la politique, tels que "incident de cybersécurité", "informations confidentielles" et "données à caractère personnel".***

# Conformité juridique et réglementaire

[Insérer la conformité réglementaire]

La politique de cybersécurité de [Nom de l'organisation] repose sur le respect des cadres juridiques et réglementaires des autorités compétentes. Cet engagement englobe le respect des principaux cadres juridiques et réglementaires suivants :

1. Protection des informations personnelles et documents électroniques au sein de l’autorité compétente.

2. Loi relative à la cybersécurité au sein de l’autorité compétente

3. Code pénal de l’autorité compétente

4. Législation de l’autorité compétente

***Fournir des détails supplémentaires concernant l'engagement de l'organisation à se conformer aux lois et réglementations pertinentes de l’autorité compétente.***

# Rôles et responsabilités

[Insérer les rôles et responsabilités]

Il est essentiel de définir clairement les rôles et les responsabilités pour une mise en œuvre efficace de la politique de cybersécurité de [Nom de l'organisation]. Les paragraphes suivants décrivent les principales parties prenantes et leurs fonctions respectives :

1. Conseil d'administration
* Supervision de la gouvernance : Veiller à ce que les stratégies de cybersécurité soient conformes aux objectifs de l'organisation et aux exigences réglementaires.
* Allocation des ressources : Approuver les ressources nécessaires au développement et au maintien des programmes de cybersécurité.

2. Directeur général (DG)

* Leadership stratégique : Se faire le champion des initiatives en matière de cybersécurité et les intégrer dans la stratégie globale de l'organisation.
* Application des politiques : Veiller au respect des politiques de cybersécurité dans tous les services.

3. Responsable de la sécurité de l'information (CISO)

* Élaboration de politiques : Rédiger, mettre en œuvre et actualiser les politiques et procédures en matière de cybersécurité.
* Gestion des risques : Identifier, évaluer et atténuer les risques liés à la cybersécurité.
* Réponse aux incidents : Diriger la réponse aux incidents de cybersécurité et coordonner les efforts de rétablissement.

4. Département des technologies de l'information (TI)

* Sécurité de l'infrastructure : Mettre en œuvre et maintenir des contrôles de sécurité pour le matériel, les logiciels et les réseaux.
* Surveillance et maintenance : Contrôler régulièrement les systèmes pour détecter les vulnérabilités et appliquer les mises à jour nécessaires.

5. Responsables de service

* Mise en œuvre des politiques : Veiller à ce que leurs équipes respectent les politiques et les procédures en matière de cybersécurité.
* Facilitation de la formation : Coordonner les formations de sensibilisation à la cybersécurité pour les membres de l'équipe.

6. Employés et contractants

* Respect des politiques : Respecter les politiques de cybersécurité établies et signaler toute activité suspecte.
* Pratiques de sécurité : Protéger les données de l'organisation en utilisant des mots de passe forts et en sauvegardant les informations sensibles.

7. Partenaires tiers

* Assurance de conformité : Adhérer aux normes de cybersécurité de [Nom de l'organisation] et se soumettre à des évaluations de sécurité régulières.
* Signalement des incidents : Signaler rapidement tout incident de sécurité susceptible d'avoir un impact sur [Nom de l'organisation].

En définissant clairement ces rôles et responsabilités, [Nom de l'organisation] vise à promouvoir une culture de la sécurité et à assurer la protection de son patrimoine informationnel.

***Cette section doit permettre d'attribuer des responsabilités spécifiques en matière de cybersécurité aux différents rôles au sein de l'organisation.***

# Gestion des risques

[Insérer la stratégie de gestion des risques]

Une gestion efficace des risques est essentielle pour protéger les actifs informationnels de [Nom de l'organisation] et garantir la conformité aux normes canadiennes en matière de cybersécurité. Notre approche s'aligne sur les lignes directrices de l’autorité compétente en matière de cybersécurité, en particulier la gestion des risques liés à la sécurité des TI.

1. Cadre de gestion des risques

Nous adoptons un cadre structuré de gestion des risques qui s'intègre dans nos processus organisationnels et qui englobe les éléments suivants :

* Identification des risques : Identifier systématiquement les menaces et les vulnérabilités potentielles qui pourraient avoir un impact sur les systèmes d'information.
* Évaluation des risques : Évaluer les risques identifiés afin de déterminer leur impact potentiel et leur probabilité.
* Atténuation des risques : Mettre en œuvre des contrôles appropriés pour ramener les risques à des niveaux acceptables.
* Surveillance des risques : Contrôler en permanence l'environnement de risque et l'efficacité des contrôles.

2. Rôles et responsabilités

* L'encadrement supérieur : Assurer la surveillance et veiller à ce que des ressources soient allouées aux activités de gestion des risques.
* L'équipe de gestion des risques : Évaluer les risques, élaborer des stratégies d'atténuation et surveiller les niveaux de risque.
* Tous les employés : Respecter les politiques de sécurité et signaler tout risque ou incident observé.

3. Processus d'évaluation des risques

Notre processus d'évaluation des risques comprend

* Identification des actifs : Cataloguer les actifs informationnels et leur importance pour les opérations de l'organisation.
* Analyse des menaces : Identifier les menaces potentielles, y compris les cyber-attaques, les catastrophes naturelles et les erreurs humaines.
* Évaluation de la vulnérabilité : Déterminer les faiblesses qui pourraient être exploitées par des menaces.
* Analyse d'impact : Évaluer les conséquences potentielles des événements à risque sur les opérations et les actifs.
* Évaluation des risques : Classer les risques par ordre de priorité en fonction de leur impact et de leur probabilité.

4. Stratégies d'atténuation des risques

Pour faire face aux risques identifiés, nous mettons en œuvre

* Contrôles préventifs : Mesures telles que les pare-feu, les contrôles d'accès et le cryptage pour prévenir les incidents.
* Contrôles de détection : Systèmes tels que la détection d'intrusion pour identifier et alerter sur les incidents.
* Contrôles correctifs : Procédures de restauration des systèmes et des données après un incident.

5. Contrôle et révision continus

Conscients de la nature dynamique des cybermenaces, nous :

* Mettre régulièrement à jour les évaluations des risques : Refléter les changements dans le paysage des menaces et les opérations de l'organisation.
* Auditer les contrôles : S'assurer que les contrôles mis en œuvre sont efficaces et conformes aux politiques.

En adhérant à cette approche de gestion des risques, [Nom de l'organisation] s'engage à protéger ses actifs informationnels et à maintenir sa résilience face à l'évolution des cybermenaces.

***Cette section doit décrire le processus d'identification, d'évaluation et d'atténuation des risques de cybersécurité, y compris les évaluations régulières des risques et la mise en œuvre de contrôles appropriés.***

# Contrôles de sécurité

[Insérer les mesures de contrôle de la sécurité]

Pour protéger les informations de [Nom de l'organisation], nous mettons en œuvre les mesures administratives suivantes :

1. Élaboration et mise en œuvre de la politique

* Politiques de sécurité de l'information : Établir des politiques globales décrivant les attentes et les protocoles en matière de sécurité pour l'ensemble du personnel.
* Politique d'utilisation acceptable : Définir l'utilisation appropriée des ressources de l'organisation, y compris l'internet, le courrier électronique et les appareils.
* Politique de classification des données : Classer les données en fonction de leur sensibilité afin de déterminer les niveaux de protection requis.

2. Gestion de l'accès

* Procédures de contrôle d'accès : Mettre en œuvre des processus pour accorder, modifier et révoquer les droits d'accès, afin de s'assurer que seules les personnes autorisées accèdent à des informations spécifiques.
* Principe du moindre privilège : Restreindre l'accès des utilisateurs au minimum nécessaire à l'exercice de leurs fonctions.
* Examens réguliers des accès : Effectuer des audits périodiques pour vérifier les niveaux d'accès appropriés.

3. Sécurité du personnel

Vérification des antécédents : Vérifier les antécédents des employés et des sous-traitants qui traitent des informations sensibles.

* Formation de sensibilisation à la sécurité : Fournir une formation continue sur les politiques de sécurité, la reconnaissance des menaces et les meilleures pratiques.
* Accords de confidentialité : Exiger du personnel qu'il signe des accords pour protéger les informations de l'organisation.

4. Planification de la réponse aux incidents

* Plan d'intervention en cas d'incident : Élaborer et tenir à jour des procédures d'identification, de signalement et de traitement des incidents de sécurité.
* Équipe de réponse aux incidents : Désigner une équipe chargée de gérer et d'atténuer les incidents.
* Analyse post-incident : Effectuer des analyses pour identifier les leçons apprises et améliorer les réponses futures.

5. Gestion des risques

* Évaluations des risques : Évaluer régulièrement les menaces potentielles et les vulnérabilités des actifs informationnels.
* Stratégies d'atténuation des risques : Mettre en œuvre des contrôles pour ramener les risques identifiés à des niveaux acceptables.
* Surveillance continue : Suivre l'évolution de l'environnement de risque et l'efficacité des contrôles.

6. Conformité et audit

* Conformité réglementaire : Assurer le respect des lois et des normes applicables.
* Audits réguliers : Réaliser des audits internes et externes pour évaluer la conformité à la politique et l'efficacité des contrôles.
* Documentation : Conserver les enregistrements des efforts de mise en conformité et des résultats des audits.

7. Gestion par des tiers

* Évaluations de la sécurité des fournisseurs : Évaluer les pratiques de sécurité des partenaires tiers avant de les engager.
* Accords de niveau de service (SLA) : Inclure des exigences de sécurité dans les contrats avec les tiers.
* Contrôle continu : Vérifier régulièrement que les tiers respectent les normes de sécurité. En adhérant à cette approche de gestion des risques, [Nom de l'organisation] s'engage à protéger ses actifs informationnels et à maintenir sa résilience face à l'évolution des cybermenaces.

En mettant en œuvre ces mesures administratives, [Nom de l'organisation] vise à mettre en place un dispositif de sécurité solide, garantissant la protection des actifs informationnels et la conformité avec les réglementations applicables.

***Cette section présente les mesures techniques et administratives mises en place pour protéger les actifs informationnels.***

# Examen et approbation des politiques

La présente politique de confidentialité des données et de cybersécurité est réexaminée chaque année afin de s'assurer qu'elle reste d'actualité, efficace et conforme à l'évolution des menaces de cybersécurité, des exigences légales et des meilleures pratiques. Toute mise à jour nécessaire sera documentée et communiquée à l'ensemble du personnel concerné.

**Calendrier de révision**

- Prochaine date de révision : [Insérer la date]

- Examen effectué par : [Insérer le nom/titre]

**Signatures**

En signant ci-dessous, les soussignés confirment qu'ils ont examiné et approuvé la présente politique de confidentialité des données et de cybersécurité et reconnaissent qu'il leur incombe de veiller au respect de ses dispositions.

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Titre | Signature | Date |
| [Insérer le nom] | [Insérer le titre] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insérer la date] |
| [Insérer le nom] | [Insérer le titre] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insérer la date] |
| [Insérer le nom] | [Insérer le titre] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insérer la date] |