Rapport d’exemple — InfoSécurité Express PME

EXEMPLE — organisation fictive

Organisation : Votre organisation
Juridiction : QC
Version : 1.0
Date d’entrée en vigueur : 1 janvier 2026
Responsable : Personne désignée par la direction — Responsable de la sécurité de l’information

---

Diagnostic synthétique

Accès et authentification

Maturité : Intermédiaire

Priorité : Moyenne

Certaines mesures de protection des accès sont en place, mais le dispositif peut encore être renforcé, notamment par une généralisation du MFA et des exigences homogènes.

Gestion des données

Sensibilité : Élevée

Priorité : Élevée

L’organisation traite des données sensibles ou variées, ce qui augmente les exigences de protection, de contrôle d’accès, de conservation et de gestion des incidents.

Fournisseurs et services externes

Exposition : Élevée

Priorité : Élevée

Le recours à plusieurs tiers, notamment avec des accès techniques ou administratifs, accroît la surface d’exposition et justifie un meilleur encadrement.

Télétravail

Maturité : Faible

Priorité : Élevée

Le télétravail est pratiqué de manière partielle, mais sans politique claire identifiée, ce qui crée une hétérogénéité de pratiques.

Gestion des incidents

Maturité : Intermédiaire

Priorité : Moyenne

Un certain cadre existe pour les incidents, mais son niveau de formalisation ou d’opérationnalisation peut encore être amélioré.

Sauvegardes

Maturité : Intermédiaire

Priorité : Moyenne

Des sauvegardes régulières existent, mais leur gestion pourrait être davantage encadrée, testée ou documentée.

Recommandations prioritaires

Accès et authentification

Priorité : Moyenne

Action : Étendre l’authentification multifacteur aux accès les plus sensibles.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Ajoute une barrière importante contre les accès non autorisés.

Gestion des données

Priorité : Élevée

Action : Identifier clairement les catégories de données sensibles traitées par l’organisation.

Urgence : Immédiat — **Effort :** Moyen

Bénéfice : Permet d’adapter les mesures de protection aux données réellement en jeu.

Action : Limiter l’accès aux données sensibles selon le besoin d’en connaître.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Réduit l’exposition interne et les accès excessifs.

Action : Définir des règles minimales de conservation, de partage et de suppression.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Encadre mieux le cycle de vie des données sensibles.

Fournisseurs et services externes

Priorité : Élevée

Action : Identifier les fournisseurs ayant un accès technique, administratif ou hébergeant des données importantes.

Urgence : Immédiat — **Effort :** Faible

Bénéfice : Clarifie les dépendances externes les plus critiques.

Action : Encadrer les accès des tiers par des attentes minimales de sécurité et de confidentialité.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Réduit le risque lié aux accès externes.

Action : Prévoir une revue périodique des fournisseurs les plus sensibles.

Urgence : À structurer — **Effort :** Moyen

Bénéfice : Aide à maintenir le contrôle dans le temps.

Télétravail

Priorité : Élevée

Action : Formaliser des règles minimales de télétravail pour les accès, les appareils et la protection des informations.

Urgence : Immédiat — **Effort :** Moyen

Bénéfice : Réduit rapidement l'hétérogénéité des pratiques à distance.

Action : Préciser les attentes concernant les connexions distantes, les équipements et la confidentialité hors site.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Encadre les risques propres au travail à distance.

Gestion des incidents

Priorité : Moyenne

Action : Formaliser davantage les rôles, les étapes de traitement et les mécanismes d'escalade.

Urgence : Court terme — **Effort :** Moyen

Bénéfice : Améliore la cohérence de traitement des incidents.

Action : Prévoir un point de contact ou un mode de signalement clair.

Urgence : Immédiat — **Effort :** Faible

Bénéfice : Facilite la remontée rapide des incidents.

Sauvegardes

Priorité : Moyenne

Action : Documenter la fréquence, la portée et la responsabilité des sauvegardes existantes.

Urgence : Immédiat — **Effort :** Faible

Bénéfice : Rend les pratiques de sauvegarde plus fiables et vérifiables.

Action : Tester au moins une procédure de restauration.

Urgence : Court terme — **Effort :** Faible

Bénéfice : Vérifie que les sauvegardes sont réellement exploitables.

Politique

Objet

La présente politique établit les principes, règles et responsabilités applicables afin d’assurer la confidentialité, l’intégrité et la disponibilité des informations traitées par l’organisation.

Elle vise également à réduire les risques liés aux accès non autorisés, aux erreurs humaines, aux incidents de sécurité, aux pertes de données et aux interruptions de services pouvant affecter les activités de l’organisation.

Portée

Elle couvre les employés travaillant à distance, incluant le télétravail.

Les fournisseurs et sous-traitants ayant accès aux informations sont soumis aux mêmes exigences.

La présente politique s’applique à l’ensemble des actifs informationnels de l’organisation, incluant notamment les données, systèmes, comptes, équipements, supports de stockage et services numériques utilisés dans le cadre des activités.

Elle s’applique à toute personne qui accède aux informations ou aux ressources technologiques de l’organisation, y compris les employés, gestionnaires, consultants, stagiaires et toute autre personne autorisée.

Toute personne visée par la présente politique doit adopter un comportement prudent, respecter les règles établies et signaler sans délai toute situation susceptible de compromettre la sécurité de l’information.

Principes généraux

L’organisation applique des mesures de sécurité de l’information proportionnelles à la sensibilité des informations qu’elle traite, aux risques identifiés et aux contraintes opérationnelles propres à ses activités.

L’accès à l’information doit être accordé selon le principe du besoin d’en connaître et limité aux usages autorisés dans le cadre des fonctions exercées.

Toute personne visée par la présente politique doit faire preuve de vigilance dans l’utilisation des ressources informationnelles et adopter des comportements compatibles avec la protection des informations et des systèmes.

Gouvernance

Un responsable désigné supervise l’application des mesures de sécurité de l’information, coordonne les actions pertinentes et veille à ce que les pratiques en vigueur demeurent cohérentes avec les besoins de l’organisation.

L’organisation reconnaît que la sécurité de l’information constitue une responsabilité partagée qui doit être soutenue par des orientations claires, des mesures adaptées aux risques et une application cohérente dans les activités courantes.

Les gestionnaires doivent veiller à la diffusion de la présente politique, à sa compréhension par les personnes sous leur responsabilité et à l’application des mesures requises dans leur secteur d’activités.

Toute personne autorisée à utiliser les ressources informationnelles de l’organisation est responsable de protéger les accès qui lui sont confiés, d’utiliser les outils de manière conforme et de contribuer à la prévention des incidents de sécurité.

Gestion des données

Les données administratives internes doivent être gérées de manière ordonnée et protégées contre les accès non autorisés, les pertes accidentelles et les usages incompatibles avec les besoins de l’organisation.

Les renseignements personnels doivent être traités avec un niveau de confidentialité approprié. Leur accès doit être limité aux seules personnes autorisées dans le cadre de leurs fonctions, et leur utilisation doit être restreinte aux fins légitimes de l’organisation.

Les dossiers employés et les renseignements liés aux ressources humaines doivent être protégés avec un niveau élevé de confidentialité. Leur consultation et leur traitement doivent être réservés aux personnes ayant un besoin fonctionnel légitime.

Gestion des actifs informationnels

Les actifs informationnels de l’organisation, incluant les équipements, comptes, systèmes, applications, supports et informations, doivent être identifiés, utilisés avec précaution et protégés selon leur niveau de sensibilité et leur importance pour les opérations.

Les personnes à qui des actifs informationnels sont confiés doivent en assurer un usage approprié, en préserver la sécurité et signaler rapidement toute perte, anomalie, détérioration ou utilisation non autorisée.

Lorsque cela s’applique, les équipements, comptes d’accès et supports appartenant à l’organisation doivent être restitués, désactivés ou pris en charge conformément aux procédures établies lors d’un départ, d’un remplacement ou d’un changement de fonction.

Contrôle des accès

Les accès aux systèmes et aux ressources informationnelles doivent être protégés par des mécanismes d’authentification appropriés, adaptés à la sensibilité des informations, aux risques associés et au contexte d’utilisation.

Des mots de passe robustes doivent être exigés lorsque ce mode d’authentification est utilisé, et leur gestion doit respecter des pratiques raisonnables en matière de complexité, de confidentialité et de renouvellement selon les règles internes applicables.

Lorsque l’authentification multifactorielle est disponible ou requise, elle doit être utilisée pour renforcer la protection des accès, particulièrement dans les contextes présentant un niveau de risque accru.

Les droits d’accès aux systèmes et aux informations doivent être accordés selon les fonctions exercées et limités à ce qui est nécessaire à l’accomplissement des tâches autorisées.

Les accès doivent être attribués à des utilisateurs identifiés individuellement. Le partage d’identifiants, l’utilisation de comptes génériques non contrôlés ou l’utilisation du compte d’une autre personne sont interdits, sauf exception formellement autorisée.

Les droits d’accès doivent être révisés périodiquement et ajustés lors de tout changement de rôle, de responsabilités ou de statut d’une personne, afin d’éviter le maintien d’autorisations devenues inutiles.

Lorsqu’une personne quitte l’organisation ou n’a plus besoin d’un accès, les comptes, privilèges et autorisations qui lui sont associés doivent être retirés ou désactivés dans les meilleurs délais.

Postes de travail

Les équipements fournis ou gérés par l’organisation doivent être configurés et maintenus selon des paramètres de sécurité appropriés, de manière à réduire les risques d’accès non autorisé, de compromission ou d’utilisation non conforme.

Lorsqu’un équipement personnel est autorisé pour des activités professionnelles, son utilisation doit respecter les exigences minimales de sécurité définies par l’organisation afin de limiter les risques pour les informations et les systèmes.

Les postes de travail utilisés pour accéder aux informations de l’organisation doivent être configurés, utilisés et protégés de manière à réduire les risques d’accès non autorisé, de perte de données, d’infection logicielle ou d’utilisation inappropriée.

Les utilisateurs doivent verrouiller leur session lorsqu’ils s’absentent de leur poste et s’assurer que les informations affichées à l’écran ne soient pas accessibles à des personnes non autorisées.

Les postes de travail doivent, dans la mesure du possible, être maintenus à jour, protégés par des mécanismes appropriés contre les logiciels malveillants et utilisés conformément aux paramètres de sécurité établis par l’organisation.

Lorsqu’un appareil personnel est utilisé dans le cadre des activités de l’organisation, son usage doit demeurer encadré afin de limiter les risques liés au mélange des environnements personnels et professionnels ainsi qu’à la protection insuffisante des informations.

Le stockage local d’informations sensibles sur les postes de travail doit être limité au strict nécessaire et faire l’objet de précautions raisonnables, notamment en matière de protection d’accès, de sauvegarde et de confidentialité physique.

Utilisation acceptable

Les ressources informationnelles mises à la disposition des utilisateurs doivent être utilisées principalement à des fins professionnelles autorisées et conformément aux règles, procédures et directives applicables dans l'organisation.

Il est interdit d'utiliser les systèmes, comptes, équipements ou réseaux de l'organisation d'une manière susceptible de compromettre leur sécurité, leur disponibilité, leur intégrité ou leur bon fonctionnement.

L'installation de logiciels, l'usage d'outils non autorisés, le contournement de mécanismes de sécurité ou le recours à des services externes non approuvés doivent être évités ou faire l'objet d'une autorisation préalable, selon les règles internes en vigueur.

Les utilisateurs doivent faire preuve de prudence lorsqu'ils reçoivent des courriels, liens, pièces jointes ou demandes inhabituelles, et éviter toute action pouvant favoriser l'hameçonnage, la fraude ou l'introduction de code malveillant.

Télétravail

Lorsque le télétravail est autorisé, les activités réalisées à distance doivent être effectuées dans un environnement permettant de préserver la confidentialité des informations, la sécurité des accès et le respect des pratiques internes de l'organisation.

Les personnes en télétravail doivent porter une attention particulière à la confidentialité physique des informations, notamment en évitant l'exposition des écrans, des documents ou des conversations à des tiers non autorisés.

Les accès à distance doivent être utilisés avec prudence, en privilégiant des réseaux fiables, des mécanismes d'authentification appropriés et des pratiques limitant les risques d'interception, d'usurpation ou d'accès non autorisé.

Fournisseurs et services externes

L’organisation doit identifier les fournisseurs et prestataires externes qui ont accès à ses systèmes, à ses services numériques ou à ses informations, en portant une attention particulière à ceux qui présentent les risques les plus élevés.

Les accès accordés aux tiers doivent être autorisés, limités aux besoins des services rendus et protégés par des mesures appropriées selon la sensibilité des systèmes ou des informations concernés.

Les fournisseurs concernés doivent être informés des attentes minimales de l’organisation en matière de sécurité et de confidentialité et être tenus de protéger les informations auxquelles ils ont accès.

Les comptes, privilèges et autres accès accordés à un fournisseur doivent être retirés ou révoqués dans les meilleurs délais lorsqu’ils ne sont plus nécessaires ou à la fin de la relation de services.

Les fournisseurs les plus sensibles doivent faire l’objet d’une revue périodique afin de confirmer que leurs accès, les services utilisés et les mesures de protection demeurent appropriés.

Gestion des incidents

L’organisation maintient un processus documenté de gestion des incidents visant à encadrer l’identification, l’évaluation, le traitement et le suivi des événements susceptibles d’affecter la sécurité de l’information ou la confidentialité des données.

Toute personne qui constate ou soupçonne un incident de sécurité, une perte d’équipement, une tentative d’hameçonnage, un accès non autorisé ou toute situation anormale pouvant compromettre l’information doit la signaler sans délai selon le mécanisme prévu.

Les incidents doivent être pris en charge de manière structurée afin d’en évaluer la nature, l’étendue, les systèmes touchés, les impacts possibles et les mesures immédiates de limitation à mettre en œuvre.

Dans la mesure du possible, les éléments utiles à l’analyse d’un incident doivent être préservés, notamment les journaux, messages, captures d’écran, fichiers ou autres traces permettant de comprendre la situation et de soutenir les correctifs requis.

À la suite d’un incident, l’organisation met en place les mesures correctives appropriées et révise, au besoin, ses pratiques, procédures ou contrôles afin de réduire les risques de récurrence.

Sauvegardes

Les données jugées importantes pour les activités de l’organisation doivent faire l’objet de sauvegardes régulières afin de réduire les risques de perte, d’altération ou d’indisponibilité.

Lorsque des sauvegardes sont mises en place, leur fréquence et leur portée doivent être adaptées à l’importance des informations concernées, aux besoins opérationnels de l’organisation et aux risques de perte ou d’interruption.

Les copies de sauvegarde doivent être protégées de manière raisonnable contre l’accès non autorisé, l’altération, la suppression accidentelle ou la perte, selon les moyens retenus par l’organisation.

L’organisation devrait, dans la mesure du possible, vérifier périodiquement la possibilité de restaurer les informations sauvegardées, afin de confirmer que les mécanismes de reprise répondent aux besoins réels en cas d’incident ou d’erreur.

Conformité et sanctions

Le respect de la présente politique est requis de toute personne visée. L’organisation peut mettre en place des mécanismes raisonnables de suivi, de vérification ou de contrôle afin d’en soutenir l’application.

Tout manquement à la présente politique peut entraîner des mesures correctives, administratives ou organisationnelles appropriées, selon la nature de la situation, les impacts constatés et le cadre applicable au sein de l’organisation.

Lorsqu’un régime disciplinaire ou des sanctions formelles sont prévus par l’organisation, ceux-ci peuvent être appliqués en cas de non-respect de la présente politique, conformément aux règles internes et aux obligations applicables.

Révision et mise à jour

La présente politique doit être révisée périodiquement afin de s’assurer qu’elle demeure cohérente avec les activités de l’organisation, l’évolution des risques, les changements technologiques et les pratiques de gestion en vigueur.

L’organisation peut mettre à jour la présente politique à la suite d’un incident, d’un changement organisationnel, d’une évolution des outils utilisés ou de tout autre élément justifiant un ajustement des mesures de sécurité applicables.

Document généré via DocuNorme à partir des réponses fournies par l’organisation.