Institut de tourisme et d'hôtellerie Québec

POLITIQUE
SUR LA SÉCURITÉ DE L'INFORMATION

Numéro du document	POL- 2400-01-V03	
Préparée par	Welly Augustin, directeur Direction des technologies de l'information	
Instance consultée	- Comité sur l'accès à l'information et de la protection des renseignements personnels - Comité de gestion	
Recommandée par	Dany Gauthier, directeur Direction principale des finances et de l'administration	
Adoptée par	Liza Frulla, directrice générale Direction générale	
Entrée en vigueur	Le 15 juin 2023	
Responsable de l'application	Welly Augustin, directeur Chef de la sécurité de l'information organisationnelle (CSIO)	
Historique des mises à jour	**Numéro**	**Date de mise à jour**
	Version originale	2010-01-09
	Révision 1	2013-06-27
	Révision 2	2019-08-14

Table des matières

1. PRÉAMBULE

Dans l'accomplissement de sa mission, l'Institut de tourisme et d'hôtellerie du Québec (ITHQ) traite de l'information disponible sur plusieurs supports à l'aide de différents systèmes d'information. Les informations détenues par l'ITHQ, lui permettant de soutenir ses activités, possèdent une valeur administrative, légale, financière ou patrimoniale et doivent, par conséquent, faire l'objet d'une utilisation appropriée et d'une protection adéquate tout au long de leur cycle de vie.

À ces fins, la mise en œuvre d'un ensemble de mesures de sécurité est nécessaire. Ces mesures sont déterminées par une approche de gestion des risques basée sur des principes, des rôles et des responsabilités.

2. OBJET

L'ITHQ reconnaît expressément son devoir de protéger les renseignements personnels qu'il détient, que leur conservation soit assurée par ce dernier ou par un tiers. La présente politique vise à affirmer l'engagement de l'ITHQ à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information.

Elle s'appuie sur l'engagement de tous les utilisateurs à protéger l'information détenue par l'ITHQ en vue d'en assurer la disponibilité, l'intégrité et la confidentialité, quel que soit le support sur lequel elle est conservée (numérique, papier ou autre).

L'ITHQ met en œuvre une approche de gestion intégrée de la sécurité, laquelle comprend celle des personnes, des lieux, des biens et de l'information. Les activités visées impliquent la manipulation ou l'utilisation de l'information, sous toutes ses formes, et qu'elles aient lieu dans les locaux de l'ITHQ ou ailleurs (télétravail, réunions externes, etc.).

3. CHAMP D'APPLICATION

La politique vise l'ensemble des utilisateurs qui conçoivent, développent ou utilisent des actifs informationnels à l'ITHQ. Elle s'applique à l'ensemble des actifs informationnels de l'ITHQ.

4. CADRE NORMATIF

Cette politique fait référence aux exigences des lois et documents normatifs suivants :

a) la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* R.L.R.Q., c. A-2.1;

b) la *Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03);

c) la *Directive sur la sécurité de l'information gouvernementale*, C.T. 203560 du 11 avril 2006.

5. DÉFINITIONS

Les définitions à considérer pour l'application de la présente politique sont les suivantes, et peuvent être complétées par tout autre règlement, politique, directive ou procédure y faisant référence.

Actif informationnel : Information ainsi que son support, qu'il soit tangible ou intangible, permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue.

Catégorisation de l'information : Processus permettant de déterminer le degré de sensibilité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité des dits actifs.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

Incident de sécurité : Événement de sécurité qui compromet, ou pourrait compromettre la confidentialité, la disponibilité ou l'intégrité d'un actif informationnel, ou la continuité de service d'une organisation. Il peut s'agir, par exemple, d'une tentative de cyberattaque, de la découverte d'une vulnérabilité, d'un vol de documents dans un bureau ou d'une perte d'un ordinateur portable.

Intégrité : Propriété d'une information intacte, entière, qui n'a pas été altérée, volontairement ou accidentellement, lors de son traitement, de sa conservation ou de sa transmission.

Responsable d'actif informationnel : Membre du personnel détenant la plus haute autorité au sein d'une unité administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité.

Ressource informationnelle : Ressource utilisée par une organisation dans le cadre de ses activités de traitement de l'information pour mener à bien sa mission, pour l'aider dans sa prise de décision, ou encore pour résoudre des problèmes.

Renseignement personnel : Information qui concerne une personne physique et qui permet de l'identifier ou de la distinguer d'une autre ou qui permet de faire connaître quelque chose sur quelqu'un par exemple : le nom, l'adresse, le numéro de téléphone, le statut de fréquentation, le code permanent, le numéro d'employé, la date de naissance, les informations médicales et les numéros de carte de paiement.

Unité administrative : Regroupement d'employées et employés sous l'autorité d'une même supérieure ou d'un même supérieur immédiat.

Utilisateur : Membre du personnel de l'ITHQ et toute personne physique ou morale qui, à titre d'employé, d'étudiant, de consultant, de bénévole, de partenaire, de fournisseur ou autres, est dûment autorisé à utiliser un actif informationnel de l'ITHQ.

6. GESTION DES ACTIFS INFORMATIONNELS

La politique s'articule autour de trois axes fondamentals de gestion, soit la gestion des accès, la gestion des risques et la gestion des incidents, lesquelles font l'objet de directives distinctes.

6.1. Gestion des accès

La sécurité de l'information est assurée par des mesures d'encadrement et de contrôle adéquat de l'accès, de la divulgation et de l'utilisation des actifs informationnels par les personnes autorisées afin de protéger leur confidentialité et leur intégrité.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des utilisateurs, à tous les niveaux.

Cette gestion est encadrée par la *Directive de gestion des identités et des accès*.

6.2. Gestion des risques

Une catégorisation à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

Chaque unité administrative doit, en collaboration avec le Chef de la sécurité de l'information organisationnelle (CSIO), inventorier les actifs informationnels les plus critiques de son unité, évaluer leur degré de sensibilité, identifier les impacts qu'entraîneraient un incident de sécurité pour son unité ou pour l'ITHQ, et évaluer le degré de protection nécessaire pour minimiser ce risque.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de l'ITHQ.

6.3. Gestion des incidents

L'ITHQ déploie des mesures de sécurité de l'information afin d'éviter toute situation pouvant mener à des bris de confidentialité ou de disponibilité des services.

À cet égard, elle met en place les mesures nécessaires afin de :

a) limiter l'occurrence des incidents en matière de sécurité de l'information;

b) gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Cette gestion est encadrée par la *Directive de protection contre les incidents de sécurité.*

7. RÔLES ET RESPONSABILITÉS

7.1. Direction générale

Être la première personne responsable de la sécurité de l'information, de l'accès aux documents et de la protection des renseignements personnels.

Être la personne responsable d'établir la composition et le mandat du Comité sur l'accès à l'information et de la protection des renseignements personnels (CAIPRP). Elle est également responsable du bon fonctionnement de celui-ci, notamment en s'assurant que des séances ont lieu régulièrement.

Nommer un chef de la sécurité de l'information organisationnelle (CSIO) pour la représenter en matière de coordination de la sécurité de l'information.

Nommer, s'il y a lieu, une personne responsable de l'accès aux documents et de la protection des renseignements personnels (RADPRP).

7.2. Direction des ressources humaines

Élaborer une procédure applicable lors des arrivées et départs des membres du personnel afin de prévoir des mécanismes assurant la sécurité des biens et de l'information institutionnelle.

Informer et obtenir de tout nouveau membre du personnel son engagement au respect de la présente politique.

7.3. Direction de l'immeuble et de la sécurité

Soutenir les gestionnaires dans le processus d'identification et de mise en place des mesures adéquates de protection physique des locaux et de sécurisation de leurs accès.

Assurer la mise en application du plan des mesures d'urgence.

7.4. Gestionnaires

Être les personnes responsables des actifs informationnels de son unité administrative.

Effectuer, en collaboration avec le CSIO, la catégorisation des actifs informationnels de sa direction en faisant une analyse des risques, une évaluation des besoins et des mesures à mettre en œuvre pour limiter les risques en matière de sécurité de l'information.

Mettre en place les moyens pour assurer adéquatement la confidentialité, l'intégrité et la destruction sécuritaire des actifs informationnels par tout utilisateur sous sa responsabilité.

Transmettre au RADPRP les formulaires requis par le CAIPRP pour les projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, communique ou détruit des renseignements personnels.

Informer promptement le RADPRP de toute perte, vol ou divulgation de renseignements personnels ou de tout incident afférant à la confidentialité de l'information.

Rapporter au CSIO tout problème lié à l'application de la présente politique et à la sécurité de l'information, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de cette politique.

Sensibiliser les utilisateurs sous sa responsabilité à protéger l'information de toute divulgation, altération, perte ou vol.

S'assurer que les personnes sous sa responsabilité participent à toute formation en matière de sécurité de l'information et de protection des renseignements personnels requise.

Informer tout utilisateur externe, appelés à utiliser les actifs informationnels de l'ITHQ, avec qui ils transigent de la présente politique afin qu'ils s'y conforment.

7.5. Direction des technologies de l'information (DTI)

Assurer la coordination et la cohérence des actions menées au sein de l'ITHQ en matière de sécurité de l'information en conseillant ou en formant les gestionnaires, le cas échéant.

S'assurer de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information et dans la réalisation de projets de développement ou d'acquisition de systèmes d'information.

Mettre en œuvre un plan de relève informatique qui assurera la continuité des services essentiels, selon un délai prévu.

Réaliser des audits de sécurité, des tests d'intrusion et de vulnérabilité du réseau interne et externe.

S'assurer que la disposition des matériels et des équipements informatiques respecte les règles de destruction sécuritaire de l'information.

Limiter les accès au local des serveurs uniquement aux personnes autorisées.

7.6. Chef de la sécurité de l'information organisationnelle (CSIO)

Assurer la gestion de la sécurité des actifs informationnels et représenter la direction générale en cette matière à l'ITHQ et auprès des autorités gouvernementales.

S'assurer de l'application de la présente politique.

Effectuer annuellement des rappels de la présente politique, ainsi que des directives y afférant; aux utilisateurs afin qu'ils s'y conforment.

Encadrer l'analyse des risques de sécurité et contribuer à la mise en œuvre des solutions appropriées avec les responsables des actifs informationnels.

Collaborer à l'élaboration du plan de continuité des services, veiller à sa mise en œuvre et en assurer la mise à jour.

Formuler des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information.

Assurer le suivi des décisions du CAIPRP.

S'assurer des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

7.7. Responsable de l'accès aux documents et de la protection des renseignements personnels (RADPRP)

Exposer les obligations législatives, administratives et réglementaires en matière de protection des renseignements personnels afin que celles-ci soient respectées.

Mettre en œuvre les mesures nécessaires au sein de l'ITHQ pour assurer la protection des renseignements personnels tout au long de leur cycle de gestion, soit de la collecte à leur destruction (ex. : politique, directive, etc.).

Présider et coordonner les travaux du CAIPRP.

Prendre part à toute question relative à la protection des renseignements personnels.

Communiquer au CAIPRP les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible.

7.8. Utilisateurs

Protéger les actifs informationnels mis à sa disposition dans tout leur cycle de vie.

Respecter les mesures de sécurité mises en place sans les contourner.

Faire usage des actifs informationnels dans le respect de la présente politique, de même qu'en harmonie avec la réglementation en vigueur, notamment dans le respect des droits

d'auteur, des droits de propriété intellectuelle, de la protection des renseignements personnels.

Utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés.

Sauvegarder toute information institutionnelle seulement sur les supports approuvés par l'ITHQ.

Signaler immédiatement au CSIO, et à son gestionnaire s'il y a lieu, tout acte dont il a connaissance susceptible de constituer une violation réelle ou présumée des règles de sécurité, comme un vol ou la perte d'informations confidentielles, l'intrusion dans un réseau ou un système ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de l'ITHQ.

8. COMITÉ SUR L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (CAIPRP)

Est institué par la présente politique un Comité sur l'accès à l'information et de la protection des renseignements personnels (CAIPRP).

8.1. Composition

Le CAIPRP est composé :

a) du RADPRP;
b) du CSIO;
c) du directeur des technologies de l'information;
d) du directeur du registrariat, du recrutement et de l'organisation scolaire;
e) d'un représentant de la Direction principale des études universitaires et de la recherche;
f) du responsable de la gestion documentaire;
g) d'un représentant de la direction des ressources humaines;
h) du directeur de la direction des communications et du marketing.

Le RADPRP peut inviter, de façon permanente ou ponctuelle, toute personne à participer au CAIPRP dont l'expertise est requise.

8.2. Mandat du comité

Soutenir l'ITHQ dans l'exercice de ses responsabilités et dans l'exécution de ses obligations relatives à la protection des renseignements personnels.

Définir et recommander les orientations en matière de protection des renseignements personnels.

Recommander les règles de gouvernance en matière de protection des renseignements personnels, notamment :

a) les rôles et responsabilités des membres du personnel tout au long du cycle de vie de ces renseignements;
b) le processus de traitement des plaintes relatives à la protection des renseignements personnels;
c) les activités de formation et de sensibilisation offertes aux utilisateurs de l'ITHQ en matière de protection des renseignements personnels et de déclaration des incidents de sécurité comportant des renseignements personnels;
d) les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage.

Formuler des recommandations sur les événements significatifs ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'ITHQ.

Rendre un avis et suggérer des mesures de protection sur tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, communique ou détruit des renseignements personnels, sur tout sondage recueillant ou utilisant des renseignements personnels, et sur toute technologie de vidéosurveillance.

Déclarer à la Commission d'accès à l'information tout procédé permettant de saisir des caractéristiques ou des mesures biométriques à des fins d'identification ou d'authentification ou la création d'une banque de caractéristiques ou de mesures biométriques, au moins 60 jours avant sa mise en service.

9. MESURES ADMINISTRATIVES, DISCIPLINAIRES OU LÉGALES

Tout manquement aux dispositions de la présente politique pourrait entrainer des mesures administratives ou disciplinaires ou légales, selon la gravité du manquement.

10. RESPONSABLE DE L'APPLICATION

Le CSIO est responsable de l'application de la présente politique.

11. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de sa signature par la directrice générale.

12. MISE À JOUR

La présente politique doit être mise à jour au plus tard le 1er février 2026.

13. SIGNATURE

Signée à Montréal, le 15 juin 2023

ORIGINAL SIGNÉ
Liza Frulla
Directrice générale