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

Politique de confidentialité

Nous vous remercions de visiter le site web de l'Institut de tourisme et d'hôtellerie du Québec (l' « **ITHQ** »). La présente Politique de protection de la vie privée s'applique au site web accessible au lien https://www.ithq.qc.ca (le « **site web** »).

1. Qui nous sommes

Aux fins de la présente politique de protection de la vie privée (la « **Politique de protection de la vie privée** »), toute référence à l'ITHQ ou à la Fondation est réputée inclure leurs employés, dirigeants, administrateurs, mandataires, sous-traitants et autres représentants respectifs.

Lorsque nous utilisons les expressions « **nous** », « **nos** », ou « **notre** » ci-dessous, nous référons donc spécifiquement à l'ITHQ, à titre de responsable du traitement de vos renseignements personnels.

La présente Politique de protection de la vie privée décrit nos pratiques en matière de collecte, d'utilisation, de communication, de partage et de gestion des renseignements personnels fournis sur le Site web ou autrement colligés dans le contexte des activités de l'ITHQ. Notre Politique de protection de la vie privée décrit également les mesures que nous prenons pour protéger la sécurité de ces renseignements ainsi que la façon dont vous pouvez accéder à vos renseignements personnels, les modifier ou les supprimer. En plus de la présente Politique de protection de la vie privée, votre visite du présent site web est assujettie à (i) nos modalités d'utilisation du site web, et (ii) toutes autres conditions d'utilisation qui pourraient vous être communiquées de temps à autre par l'ITHQ.

Si vous ne consentez pas aux modalités concernant notre collecte, utilisation, communication, partage et gestion de renseignements personnels énoncées dans la présente Politique de protection de la vie privée, veuillez ne pas nous communiquer vos renseignements personnels ou utiliser le site web.

2. Quand et comment nous recueillons vos renseignements personnels

Nous respectons votre vie privée et visons à minimiser la collecte de vos données. Nous visons également la transparence, raison pour laquelle nous détaillons ci-dessous les circonstances limitées dans lesquelles nous pouvons collecter et traiter vos données.

2.1. Par nos échanges directs

Nous procédons à la collecte de vos renseignements personnels dans le cadre d'échanges directs entre vous et l'ITHQ, plus spécifiquement dans les contextes suivants :

- vous déposez une demande d'admission pour un de nos programmes;
- vous déposez une demande d'aide financière auprès de la Fondation;
- vous remplissez volontairement un des formulaires rendus disponibles à partir de notre site web, notamment pour vous inscrire à une formation ou pour nous fournir de la rétroaction sur un de nos produits ou services;
- vous créez un compte « employeur » sur le site web pour y afficher des offres d'emploi ou de stage;
- vous effectuez une réservation à partir du site web ou sur une des plateformes de réservation offertes par nos partenaires technologiques;
- vous communiquez avec nous au sujet des services et des produits que nous offrons, notamment lorsque vous sollicitez une soumission ou demandez de l'information sur l'ITHQ, ou encore lorsque vous vous inscrivez à un atelier, une séance d'information, une rencontre individuelle d'information ou à une journée « portes ouvertes »;
- vous entrez dans une relation contractuelle avec nous pour l'obtention d'un produit ou d'un service, notamment pour exécuter nos obligations envers vous ou pour effectuer des suivis relativement au produit ou au service qui vous est livré;
- vous communiquez avec nous dans le but de poser une question, de soumettre un commentaire ou de formuler une plainte;

- vous complétez votre inscription à nos listes d'envoi, communications par courriel et services de messagerie, et ce, pour recevoir des actualités, des nouvelles, ainsi que des offres promotionnelles;
- vous demandez d'être ajouté au répertoire des entreprises des diplômés;
- vous mettez à jour vos coordonnées auprès du Bureau des diplômés de l'ITHQ;
- vous effectuez une demande d'emploi;
- vous effectuez une donation ou participez à une activité de levée de fonds de la Fondation;
- votre candidature est soumise pour un certificat de mérite professionnel;
- vous effectuez une demande auprès de nos services de bibliothèque, y compris une demande d'information, pour un achat, un emprunt ou une numérisation;
- vous interagissez avec nous à travers les médias sociaux.

2.2. Par des technologies ou interactions automatiques

Lorsque vous utilisez notre site web, nous recueillons certains types d'informations électroniquement via courriels, comptes de médias sociaux, publicité en ligne, ou par l'utilisation de nos technologies ou celles d'un tiers, ce qui inclut des témoins, des balises internet ou pixels invisibles ou moteurs d'analyse. Ces informations nous aident à comprendre les opérations que vous effectuez lorsque vous interagissez avec ces technologies et leur permettent de fonctionner correctement.

Nous pouvons combiner ces informations avec d'autres informations colligées en ligne, telles que votre historique de navigation. Cela nous permet de comprendre comment vous utilisez notre site web et de réaliser des analyses, afin de vous proposer des campagnes de publicité et de marketing plus personnalisées. Ces pratiques incluent la diffusion de publicités basées sur les centres d'intérêt. Pour en savoir plus sur les choix qui s'offrent à vous en matière de protection de la vie privée, veuillez consulter la Section 9 de la présente Politique de protection de la vie privée.

Les technologies que nous utilisons sont les suivantes :

- Témoins qui sont des petits fichiers de données qui sont enregistrés et stockés sur le disque dur de votre ordinateur afin de nous permettre de sauvegarder certaines informations entre les visites au site web, telles que vos données d'accès ou vos

préférences linguistiques. Les témoins vous permettent, entre autres, de vous connecter rapidement lorsque vous visitez notre site web.

- Balises Internet et pixels invisibles qui sont des petits fichiers images contenant certaines de vos informations, telles que votre adresse IP, qui peuvent être téléchargés lorsque vous visitez un site web ou que vous ouvrez un courriel. Cette technologie nous permet de comprendre votre comportement en ligne, de contrôler l'envoi de nos courriels et de vous proposer des publicités basées sur vos centres d'intérêt. Ces fichiers permettent également aux outils de suivi de tiers de recueillir des informations, telles que votre adresse IP, et de nous les renvoyer sous une forme anonyme et agrégée (c'est-à-dire d'une manière qui nous empêche de vous identifier personnellement). Par renseignements agrégés, on entend des renseignements personnels compilés et exprimés sous une forme résumée dans laquelle aucun identifiant personnel n'est inclus.
- Outils d'analyse web (tels que Google Analytics) qui se servent des témoins pour analyser votre utilisation de notre Site web, créer des rapports sur les activités des internautes et fournir d'autres services associés à l'utilisation de notre Site web.
- Moteurs d'analyse qui extraient les données d'utilisation de plusieurs sources et aident à gérer et à collecter ces données pour les utiliser à des fins de personnalisation, pour la publicité basée sur les centres d'intérêt, pour la personnalisation du contenu et pour d'autres méthodes permettant de mieux connaître les besoins et les préférences des visiteurs de notre site web.
- Des outils de protection contre les usages non autorisés, tels que Google Invisible reCAPTCHA qui recueillent des informations sur le matériel informatique et les logiciels, telles que les données relatives aux appareils et aux applications, les résultats des contrôles d'intégrité et les identifications uniques en ligne (l'adresse IP, par exemple) et qui envoie ces données à Google pour analyse.

Vous pouvez supprimer ou désactiver certaines de ces technologies à tout moment via votre navigateur. Toutefois, dans ce cas, il se peut que vous ne puissiez pas utiliser certaines fonctions de nos sites web. Pour en savoir plus sur les choix qui s'offrent à vous en matière de protection de la vie privée, veuillez consulter la Section 9 de la présente Politique de protection de la vie privée.

2.3 Par l'entremise de tiers

Nous pouvons obtenir des informations à votre sujet auprès d'autres sources, y compris de tiers qui fournissent des services à l'ITHQ dans le cadre de leurs activités. La collecte de

renseignements personnels faite par l'ITHQ auprès de ces tiers s'effectue pour les seules fins qui sont décrites à la présente Politique de protection de la vie privée. Plus précisément, l'ITHQ obtient certains de vos renseignements personnels de la part de tiers dans les circonstances suivantes :

- vous déposez une demande d'admission à travers une plateforme technologique opérée par un tiers (par ex. plateformes SRAM ou COBA);
- vous déposez votre candidature pour un emploi à travers une plateforme technologique opérée par un tiers (par ex. plateforme SOFE); ou
- vous effectuez une demande de réservation à travers une plateforme technologique opérée par un tiers (par ex. plateformes LIBRO, OPERA CLOUD, LOUNGE UP ou LUXURY RES).

3. Quels renseignements personnels nous colligeons

Aux fins de la présente Politique de protection de la vie privée, l'expression « **renseignements personnels** » désigne toute information concernant un individu à partir de laquelle cette personne peut être identifiée. Cela n'inclut pas les renseignements dont l'identité a été retirée (données anonymes).

Nous pouvons recueillir, utiliser, stocker et transférer différents types de renseignements personnels à votre sujet. Le type de renseignements personnels que nous pouvons recueillir est décrit dans le tableau ci-dessous, avec une indication du caractère obligatoire ou facultatif de ces renseignements dans le cadre des activités de l'ITHQ.

Type de renseignement personnel	Obligatoire ou facultatif
Les coordonnées de communication incluent le nom, le prénom, pronom, l'adresse courriel, le titre, le numéro de téléphone, l'adresse postale et les préférences de contact	Obligatoire : pour répondre à vos demandes, pour traiter votre demande d'admission, de stage, de bénévolat, ou d'emploi ou encore pour vous fournir les produits ou services que vous avez demandés

	Facultatif : à toutes autres fins
Les données démographiques, qui incluent la date de naissance ou le sexe	Obligatoire : la date de naissance sera utilisée pour traiter votre demande de bourse ou pour mettre à jour le profil des diplômés Facultatif : à toutes autres fins
Les données géographiques, qui incluent le pays, la province, la région administrative, la ville ou le code postal	Obligatoire : pour répondre à vos demandes, pour traiter votre demande d'admission, de stage ou de bénévolat, ou encore vous fournir les produits ou services que vous avez demandés Facultatif : à toutes autres fins
Les données relatives à l'emploi ou aux activités professionnelles, qui incluent tous les renseignements personnels pouvant être présentés dans une lettre de présentation, un curriculum vitae ou autre document similaire déposé au soutien d'une demande d'emploi, d'une demande de stage ou d'offre de bénévolat	Obligatoire : pour traiter votre candidature et gérer toute relation de travail ou relation contractuelle subséquente Facultatif : à toutes autres fins
Les données des médias sociaux comprennent des informations associées à tout compte de médias sociaux dont vous êtes titulaire et au profil y associé, telles que le nom, le nom d'utilisateur, l'adresse de messagerie, la photo de profil, la date de naissance et le genre	Facultatif
Les données techniques incluent l'adresse IP (protocole Internet), vos données de connexion, le nombre de clics et d'autres informations connexes, telles que les sites web que vous avez visités immédiatement avant et après votre visite sur notre site web, vos réglages concernant le fuseau horaire et la zone géographique, le fournisseur de services Internet que vous utilisez et les autres technologies sur les appareils que vous utilisez pour accéder à notre site web	Facultatif

Les données d'utilisation incluent le nombre de visites sur nos sites web, la date et le temps moyen passé sur nos sites web, ainsi que des informations sur la manière dont vous utilisez nos produits et services	Facultatif
Les données de marketing et de communication incluent vos préférences pour recevoir du marketing de notre part et des tiers qui nous sont reliés et vos préférences de communication.	Obligatoire : afin de vous communiquer des messages de marketing que vous avez accepté de recevoir ou qui sont permis par les lois applicables Facultatif : à toutes autres fins

Nous recueillons, utilisons, stockons et partageons également des **Renseignements Agrégés**, tels que des renseignements statistiques ou démographiques. Les Renseignements Agrégés peuvent être dérivés de vos renseignements personnels, mais ne sont pas considérés comme des renseignements personnels s'ils ne révèlent pas directement ou indirectement votre identité. Par exemple, nous pouvons regrouper vos données d'utilisation pour calculer le pourcentage d'utilisateurs accédant à une fonctionnalité spécifique de notre site web. Toutefois, si nous combinons ou connectons des Renseignements Agrégés avec vos renseignements personnels afin de vous identifier directement ou indirectement, nous les traitons comme des renseignements personnels qui seront utilisés conformément à la présente Politique de protection de la vie privée.

Nous ne recueillons aucun renseignement personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ni aucune donnée génétique, aucune donnée biométrique aux fins d'identifier une personne physique de manière unique, aucune donnée concernant la santé ni aucune donnée concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

<u>Conséquences d'un refus de fournir certains renseignements personnels</u>

Lorsque nous devons colliger des renseignements personnels en vertu de la loi ou d'un contrat que nous avons conclu avec vous, si vous ne fournissez pas ces renseignements sur demande, il se peut que nous ne puissions pas exécuter le contrat en cause. Dans ce cas, il se peut que nous devions annuler la livraison d'un produit ou l'exécution d'un service que vous avez requis de nous dans la mesure où votre refus rend impossible l'exécution de nos obligations, mais nous vous en informerons si tel est le cas au moment opportun.

4. Comment nous utilisons les renseignements personnels recueillis

Nous limitons la collecte de renseignements personnels à ceux qui sont raisonnablement requis pour atteindre les objectifs pour lesquels ils sont recueillis. Le plus souvent, nous utiliserons vos renseignements personnels dans les circonstances décrites ci-dessous.

- **Avec votre consentement:** par exemple, nous obtiendrons votre consentement avant de vous envoyer des communications marketing;
- **Pour des raisons conformes aux motifs pour lesquels les renseignements personnels ont été collectés :** par exemple, le traitement de vos renseignements personnels lorsque cela est nécessaire pour répondre à vos demandes, exécuter un contrat auquel vous êtes partie ou encore pour entreprendre des démarches en votre nom et à votre demande avant de conclure un tel contrat;
- **À des fins strictement avantageuses pour vous :** par exemple, pour exécuter une obligation contractuelle ou toute autre obligation que nous avons envers vous;
- **Dans la mesure où la loi l'autorise et lorsque nous devons respecter une obligation légale:** respecter une obligation légale signifie traiter vos renseignements personnels lorsque cela est expressément autorisé par les lois applicables en matière de la protection de la vie privée ou nécessaire au respect d'une obligation légale à laquelle nous sommes soumis.

De temps à autre, nous pouvons utiliser vos renseignements personnels afin de mener des sondages dans le but d'améliorer nos produits et services. Dans de tels cas, nous ne colligerons pas de renseignements personnels sensibles et les résultats du sondage seront anonymes. Nous n'utilisons pas vos renseignements personnels dans le cadre d'une prise de décision automatisée. Dans le cas où nous effectuerions un sondage à des fins autres que celles identifiées ci-dessus ou prendrions une décision automatisée, un énoncé sur la protection de la vie privée vous serait communiqué avant que ces activités n'aient lieu.

Vos renseignements personnels peuvent, selon le cas, être accessibles par nos employés, consultants, sous-traitants, étudiants et bénévoles en fonction du critère de nécessité, c'est-

à-dire lorsque l'accès aux renseignements est requis pour les fins qui sont décrites dans la présente Politique, et toujours en fonction de notre processus de gestion des accès.

5. Comment nous divulguons vos renseignements personnels

5.1 Principe

Sauf si expressément énoncé dans la présente Politique de protection de la vie privée, nous ne procédons pas à la vente, la location, le transfert ou la communication de vos renseignements personnels à des tiers pour des fins non divulguées sans votre consentement.

5.2. Exceptions

Nous pouvons transférer les renseignements personnels dans les cas suivants :

- **Fournisseurs tiers** : nous pouvons partager tous les types de renseignements personnels identifiés dans la Section 3 ci-dessus avec des tiers qui fournissent des services à l'ITHQ, tels que des services de réservation en ligne, services comptable, services de traitement de paiement, services de communications électroniques (marketing), services publicitaires ou services d'analyse (par exemple, le suivi de l'efficacité de nos campagnes marketing et l'analyse de l'utilisation de notre site web), services de formation en ligne. Ces tiers ne sont autorisés à utiliser vos renseignements personnels que dans le but de fournir ces services à l'ITHQ et ne sont pas autorisés à utiliser vos renseignements personnels à leurs propres fins internes.

- **Partenaires externes** : nous pouvons divulguer vos renseignements personnels à un partenaire externe lorsque vous effectuez une demande d'information, d'inscription ou de participation pour un stage ou une autre activité offerte en collaboration entre l'ITHQ et ce partenaire externe. Dans tous les cas, le nom du partenaire à qui vos renseignements personnels seront divulgués sera mentionné dans l'information qui vous sera fournie relativement à l'activité en question.

- **La Fondation** : nous pouvons divulguer vos renseignements personnels à la Fondation, une personne morale sans but lucratif avec comme mandat d'obtenir du financement

pour soutenir l'ITHQ dans la réalisation de son mandat et de sa mission. Certains renseignements personnels colligés à travers le site web sont communiqués à la Fondation, à savoir :

- lorsque vous effectuez une demande de bourse provenant de la Fondation;
- lorsque vous créez un compte « donateur » sur le site web;
- lorsque vous effectuez une donation à la Fondation;
- lorsque vous vous inscrivez pour une activité de levée de fonds organisée par la Fondation; ou
- lorsque vous déposez votre candidature pour effectuer du bénévolat auprès de la Fondation.

- Les renseignements décrits ci-haut sont utilisés par la Fondation conformément à sa politique de protection de la vie privée pour les fins suivantes :
  - évaluer la demande de bourse;
  - évaluer la candidature d'une personne qui veut effectuer du bénévolat auprès de la Fondation;
  - administrer la donation effectuée auprès de la Fondation;
  - administrer les activités de levées de fonds auxquelles vous avez demandé de participer;
  - vous envoyer des communications électroniques lorsque vous y avez consenti ou autrement en conformité avec les lois applicables.

- **Étudiants et bénévoles :** nous pouvons divulguer vos renseignements personnels aux étudiants de l'ITHQ ou à certains bénévoles lorsque cette communication est nécessaire pour les fins décrites à la présente Politique de protection de la vie privée. Ces tiers ne sont autorisés à utiliser vos renseignements personnels que pour les fins prévues à cette Politique de protection de la vie privée et ne sont pas autorisés à utiliser vos renseignements personnels à leurs propres fins.

- **Fins judiciaires :** nous pouvons divulguer vos renseignements personnels lorsque cela est demandé ou requis à des fins judiciaires. Plus précisément l'ITHQ et ses fournisseurs tiers peuvent communiquer vos renseignements personnels pour donner suite à un mandat de perquisition ou à une autre demande ou ordonnance conforme à la loi, ou pour répondre à un organisme d'enquête en cas de violation d'une entente ou de manquement à la loi, ou

comme autrement requis ou autorisé par la loi. Nous pouvons également communiquer des renseignements personnels au besoin en vue de faire valoir ou d'exercer des réclamations en justice ou de faire valoir un moyen de défense contre de telles réclamations, ou dans le but de prévenir des pertes réelles ou présumées ou d'éviter des blessures corporelles ou des dommages matériels.

- **Vente, transfert d'activités ou autres transactions** : nous pouvons partager vos renseignements personnels avec une autre entité si nous vendons ou transférons des actifs dans le cadre d'une transaction commerciale ou bien dans le cadre d'une fusion, d'un changement à notre régime constitutif ou notre structure organisationnelle, ou toute autre opération juridique relativement à la forme juridique de l'ITHQ. Dans le cas où la transaction est réalisée, vos renseignements personnels resteront protégés par les lois applicables en matière de protection de la vie privée. Dans le cas où la transaction n'est pas réalisée, nous exigerons de l'autre partie qu'elle n'utilise pas ou ne communique pas vos renseignements personnels de quelque manière que ce soit et qu'elle supprime complètement ces informations, conformément aux lois applicables.

- **Autres raisons autorisées** : les lois applicables peuvent permettre ou exiger l'utilisation, le partage ou la divulgation de renseignements personnels sans consentement dans des circonstances spécifiques (par exemple, lors d'enquêtes et de mesures de prévention d'activités illégales, y compris la fraude, ou pour aider le gouvernement et les organismes d'application de la loi). Ces circonstances incluent des situations autorisées ou requises par la loi ou nécessaires pour protéger nos entreprises, nos employés, nos clients ou d'autres personnes. Dans un tel cas, nous ne partagerons que les renseignements personnels raisonnablement nécessaires.

Notre site web peut contenir des **liens vers d'autres sites** qui ne nous appartiennent ou qui ne sont pas exploités par nous. De plus, des liens vers notre site web peuvent apparaître sur des sites Internet de tiers sur lesquels nous faisons de la publicité. Sauf dans les limites prévues aux présentes, nous ne communiquerons pas vos renseignements personnels à ces tiers sans votre consentement. Nous offrons à l'utilisateur des liens vers des sites Internet de tiers à des fins de commodité. Ces liens ne se veulent pas une approbation ni une recommandation des sites liés. Les sites Internet liés comportent des énoncés sur la protection de la vie privée, des avis et des conditions d'utilisation qui sont distincts et indépendants et que nous vous recommandons de lire attentivement. Nous n'exerçons aucun contrôle sur ces sites Internet et par conséquent, nous ne saurions engager notre responsabilité quant à la façon dont les

organisations qui exploitent ces sites Internet liés peuvent recueillir, utiliser, communiquer, obtenir ou autrement traiter vos renseignements personnels.

6. Transferts de renseignements personnels vers d'autres pays

Vos renseignements personnels seront accessibles à partir du Canada. Dans certains cas, vos renseignements personnels peuvent être transférés ou stockés à l'extérieur du Canada. Nous prendrons toutes les mesures raisonnablement nécessaires, pour nous assurer que tout renseignement personnel transféré à l'extérieur du Canada soit traité de manière sécurisée et bénéficie d'un niveau de protection adéquat et conforme aux lois sur la protection des données applicables. Toutefois, il est possible que les lois du pays de destination n'offrent pas le même niveau de protection que les lois sur la protection de la vie privée en vigueur au Canada.

7. Protection et traitement de vos renseignements personnels

7.1. Comment nous protégeons vos renseignements personnels

Nous avons établi et appliquons des mesures de sécurité administratives, techniques et matérielles visant à protéger vos renseignements personnels dont nous avons la garde et le contrôle, contre l'accès, l'utilisation, la modification et la communication non autorisés, entre autres :

- Nous limitons l'accès technologique et physique de nos employés à vos renseignements personnels en mettant en œuvre un processus de gestion des accès;
- Nous réalisons des audits de sécurité, des tests d'intrusion et des tests de vulnérabilité des réseaux interne et externe en vue d'identifier toute faille et de les corriger;
- Nous offrons régulièrement des formations à nos employés quant aux enjeux de sécurité des renseignements personnels;
- Nous avons mis sur pied un Comité sur l'accès à l'information et la protection des renseignements personnels qui fait une veille constante quant aux enjeux relatifs à la

protection des renseignements personnels;

- Nous avons adopté une *Politique de sécurité de l'information* et une *Directive de protection contre les cybermenaces et déclaration des incidents de cybersécurité* qui sont communiquées à tous nos employés.

Des mesures de sécurité s'appliquent également lorsque nous disposons ou détruisons vos renseignements personnels, et ce, afin que le tout se fasse d'une façon confidentielle et sécuritaire. Par ailleurs, nous utilisons des mesures raisonnables pour veiller à ce que nos fournisseurs de services protègent vos renseignements personnels, quel que soit le lieu où ils sont utilisés ou stockés.

7.2. Accès et traitement des renseignements personnels

Nous donnons accès à vos renseignements personnels à nos employés, sous-traitants et fournisseurs tiers (chacun étant un « **Représentant** ») dans la mesure où ils ont besoin d'y avoir accès pour remplir les rôles spécifiques que nous leur avons assignés. Pendant la période de conservation de vos données personnelles, nos Représentants sont tenus de maintenir la confidentialité de vos renseignements personnels. Ils ont également la responsabilité d'adhérer aux mesures de protection administratives, techniques et physiques exigées afin de protéger vos renseignements personnels. Ils doivent par ailleurs se conformer aux politiques et pratiques désignées dans la présente Politique de protection de la vie privée.

7.3 Plan d'intervention en cas d'incident informatique

En cas de brèche de sécurité, à savoir si vos renseignements personnels sont perdus, divulgués sans votre autorisation ou deviennent accessibles à une personne non autorisée, nous vous informerons d'une telle brèche si elle entraîne un risque réel de préjudice. Par exemple, un risque réel de préjudice comprend les lésions corporelles, l'humiliation, la perte d'opportunités professionnelles, la perte financière ou le vol d'identité. Si la brèche engendre un risque réel de préjudice, nous vous en informerons directement dans les plus brefs délais. Si nous ne pouvons pas vous informer directement, nous vous informerons de la brèche par le biais d'une communication publique. Nous vous fournirons les informations nécessaires pour comprendre l'importance de la brèche de sécurité et prendre les mesures nécessaires pour réduire les risques de préjudice pouvant en découler. Nous signalerons également la brèche de sécurité au gouvernement et à toute autre organisation qui, selon nous, peuvent réduire le risque de préjudice pouvant résulter de cette brèche. Nous conservons un registre

de toutes les brèches de sécurité. À la suite d'une brèche de sécurité, l'ITHQ enquête sur ses causes et passe en revue les mesures de protection en place pour en prévenir la répétition.

7.4 Conservation des renseignements personnels

Nous ne conservons vos renseignements personnels que le temps nécessaire pour atteindre les objectifs décrits dans la présente Politique de protection de la vie privée ou pour nous conformer aux exigences de la loi.

7.5 Formation interne et programme de sensibilisation à la protection de la vie privée

Nos Représentants sont informés de la présente Politique de protection de la vie privée avant d'avoir accès à vos renseignements personnels et s'engagent à en protéger la confidentialité et à se conformer aux procédures et politiques qui y sont énoncées. En outre, nous proposons des programmes de formation à nos Représentants afin de les sensibiliser à nos obligations découlant des lois applicables en matière de protection de la vie privée et à nos processus internes de gouvernance des données. Ces programmes de formation sont disponibles sur une base continue afin de permettre à nos Représentants de se tenir à jour sur les normes de l'industrie. Plus précisément, l'ITHQ tient des campagnes de sensibilisation régulières dédiées à ce sujet durant lesquelles différentes activités sont offertes, comme le visionnement obligatoire de capsules vidéo éducatives, la diffusion de renseignements instructifs sur des écrans situés dans ses locaux, l'organisation de kiosques informatifs, etc.

7.6 Responsabilités du responsable de la protection de la vie privée

Nous avons désigné un responsable de la protection de la vie privée qui est chargé de superviser les questions relatives à la présente Politique de protection de la vie privée et qui se charge de la protection des renseignements personnels au sein de l'ITHQ. Si vous avez des questions ou des commentaires concernant la manière dont nous traitons vos renseignements personnels, y compris requête pour exercer vos droits, ou si vous souhaitez demander l'accès à vos renseignements personnels en notre possession, les mettre à jour ou les corriger, veuillez communiquer avec notre responsable de la protection de la vie privée comme indiqué ci-après :

Attention : Dewi Collin, Secrétaire générale adjointe
Téléphone : 514 282-5111
Adresse postale : 3535, rue Saint-Denis, Montréal Québec H2X 3P1
Courriel : responsable-adprp@ithq.qc.ca

Notre responsable de la protection de la vie privée est également tenu de gérer toute plainte relative à la protection de la vie privée que vous pourriez avoir en rapport avec la manière dont l'ITHQ traite vos renseignements personnels. Notre responsable de la protection de la vie privée traitera chaque plainte de la manière suivante :

- contacter le plaignant par écrit pour accuser réception de la plainte;
- enquêter sur la plainte et en évaluer le bien-fondé lorsque le responsable de la protection de la vie privée dispose d'informations suffisantes; et
- répondre à la plainte par écrit en précisant les pratiques de l'ITHQ en matière de protection de la vie privée en rapport avec la plainte.

8. Vos droits à l'égard de vos renseignements personnels

Vous disposez des droits détaillés ci-dessous à l'égard de vos renseignements personnels :

- **Demander l'accès à vos renseignements personnels :** cela vous permet de recevoir une copie des renseignements personnels que nous détenons sur vous.
- **Demander la correction ou la mise à jour des renseignements personnels que nous possédons sur vous :** ceci vous permet de corriger ou de mettre à jour les données incomplètes, inexactes ou périmées que nous détenons à votre sujet. Toutefois, nous pourrions être amenés à vérifier l'exactitude des nouvelles données que vous nous fournissez.
- **Demander l'effacement de vos renseignements personnels :** cela vous permet de nous demander de supprimer ou de retirer des renseignements personnels lorsqu'il n'y a pas de bonne raison pour que nous continuions à les traiter. Notez cependant que nous ne pourrons peut-être pas toujours donner suite à votre demande d'effacement pour des raisons juridiques spécifiques qui vous seront notifiées, le cas échéant, au moment de votre demande.
- **Demande de transfert de vos renseignements personnels à vous-même ou à un tiers :** nous vous fournirons, ou à un tiers de votre choix, vos renseignements personnels dans un format structuré, lisible par une machine, couramment utilisé. Notez que ce droit s'applique uniquement aux informations automatisées.

Si vous souhaitez exercer l'un des droits énoncés ci-dessus, veuillez contacter notre responsable de la protection de la vie privée en utilisant les coordonnées indiquées à la Section 7.6 de la présente Politique de protection de la vie privée.

Vous n'aurez pas à payer de frais pour accéder à vos renseignements personnels (ou pour exercer l'un des autres droits).

Si vous voulez exercer un des droits susmentionnés, il se peut que nous ayons besoin de vous demander des informations spécifiques afin de nous permettre de confirmer votre identité et ainsi vous permettre d'accéder à vos renseignements personnels (ou d'exercer vos autres droits). Il s'agit d'une mesure de sécurité visant à garantir que les renseignements personnels ne sont pas divulgués à une personne qui n'a pas le droit de les recevoir. Nous pouvons également vous contacter pour vous demander des informations complémentaires concernant votre demande afin d'accélérer notre réponse.

Nous répondrons à toutes les demandes légitimes dans les vingt (20) jours.

9. Changements aux paramètres de confidentialité

Communications électroniques : Vous pouvez à tout moment demander que votre nom soit retiré de nos listes d'envoi pour les communications électroniques promotionnelles ou commerciales en vous désabonnant de nos courriels.

Témoins : Vous pouvez bloquer l'utilisation des témoins en activant le paramètre correspondant dans votre navigateur.

Publicité ciblée : Vous pouvez choisir de ne pas recevoir de publicité personnalisée de la part d'annonceurs et de réseaux publicitaires tiers membres de L'Alliance de la publicité numérique du Canada (DAAC) en consultant le lien suivant : https://youradchoices.ca/fr/en-savoir-plus/.

10. Changements à la politique de protection de la vie privée

La présente Politique de protection de la vie privée est régulièrement révisée et peut être mise à jour de temps à autre pour tenir compte des changements apportés aux lois applicables ou à nos pratiques en matière de renseignements personnels. La Politique de protection de la vie privée modifiée sera affichée sur le site web. Nous traiterons vos renseignements personnels conformément à la Politique de protection de la vie privée dans sa version la plus récente.

11. Pour communiquer avec nous

Pour toute question relative à la présente Politique de protection de la vie privée, vous pouvez contacter notre responsable de la protection de la vie privée en utilisant les coordonnées indiquées à la Section 7.6 ci-dessus.

3535, rue Saint-Denis
Montréal, QC H2X 3P1

Institut de tourisme et d'hôtellerie Québec

DIRECTIVE SUR LA GESTION DES IDENTITÉS ET DES ACCÈS

Numéro du document	DIR-2400-03-V01	
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 direction - Comité de gestion	
Recommandée par	S. O.	
Adoptée par	Liza Frulla, directrice générale, Direction générale	
Entrée en vigueur	30 janvier 2024	
Responsable de l'application	Welly Augustin, Chef de la sécurité de l'information organisationnelle	
Historique des mises à jour	Numéro	Date de mise à jour
	S. O.	S. O.

Table des matières

1. PRÉAMBULE

La gestion des identités, des autorisations et des accès informatiques (GIA) est un contrôle de première importance en matière de sécurité de l'information. Il s'agit de déterminer qui a accès à quelle information pendant une période donnée.

Comme les membres du personnel peuvent accumuler des autorisations d'accès logiques avec le temps, des pratiques rigoureuses de gestion des autorisations et des accès informatiques des utilisatrices, des utilisateurs sont nécessaires pour gérer l'ensemble du cycle de vie de ses autorisations et ainsi protéger l'information. La GIA est basée sur les principes du droit d'accès minimal et de séparation des tâches.

À défaut d'un encadrement adéquat de la GIA, l'Institut de tourisme et d'hôtellerie du Québec (ITHQ) peut s'exposer à des risques de sécurité de l'information tels que :

a) l'utilisation illicite d'un accès à la suite du départ d'un membre du personnel ;
b) la destruction ou la modification de données sans autorisation;
c) la fuite de données confidentielles;
d) l'usurpation des accès par une personne autre que celle autorisée.

Cette directive découle de la *Politique sur la sécurité de l'information* de l'ITHQ.

2. OBJET

La présente directive a pour objectifs de permettre à l'ITHQ de gérer et de contrôler les accès aux ressources informationnelles par les utilisatrices, les utilisateurs. Elle vise également à préciser les règles à observer en matière d'identification, d'authentification et d'autorisation des accès des utilisatrices, des utilisateurs et contribue à assurer la confidentialité, l'intégrité et la disponibilité de l'information.

3. CHAMP D'APPLICATION

La présente directive s'applique à :

a) l'information que détient l'ITHQ, que sa conservation soit assurée par lui-même ou par un tiers;
b) l'information confiée à l'ITHQ en vertu d'une entente et qui est reconnue comme devant faire l'objet d'un contrôle d'accès;
c) l'infrastructure technologique de l'ITHQ;
d) toute utilisatrice, tout utilisateur, incluant l'ensemble du personnel de l'ITHQ, de l'actif informationnel de l'ITHQ.

4. CADRE NORMATIF

La présente directive fait référence aux exigences des lois et des documents normatifs suivants :

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

c) *Politique gouvernementale de cybersécurité;*

d) *Politique sur la sécurité de l'information* de *l'ITHQ;*

e) *Directive gouvernementale sur la sécurité de l'information*.

5. DÉFINITIONS

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

Accès : Possibilité d'utiliser des données ou des ressources informatiques ; moyen ou voie permettant d'obtenir leur utilisation.

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.

Compte : Droit d'accès à un ordinateur, un réseau ou un système informatique. Généralement, un compte est composé d'un identifiant et d'un mot de passe.

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.

Infonuagique : Modèle informatique qui, au moyen de serveurs distants interconnectés par Internet, permet d'accéder, à la demande, à un bassin partagé de ressources informatiques externalisées proposées sous la forme de services évolutifs et facturés à l'utilisation.

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.

Permission : Autorisation d'accès à des ressources partagées.

Pilote d'application : Personne désignée par un gestionnaire pour la gestion opérationnelle d'un système d'information.

Responsables sectoriels pour la gestion des identités et des accès : Personne désignée par le gestionnaire d'une direction et habilitée à effectuer en son nom les demandes d'accès, d'arrivées, de départs, d'acquisitions et d'autorisations pour les employées, les employés de sa direction.

Système d'information : Système constitué de ressources informationnelles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents au fonctionnement d'une organisation.

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

6. PRINCIPES DIRECTEURS

Un compte utilisateur (identifiant et mot de passe), permettant l'accès au réseau de l'ITHQ; est alloué à chaque utilisatrice, chaque utilisateur par l'ITHQ à titre personnel et confidentiel. L'utilisatrice, l'utilisateur est responsable de l'utilisation de son compte et il le protège.

Seule la Direction des technologies de l'information (DTI) procède à la création, la modification et la suppression des comptes des utilisatrices, des utilisateurs. Cependant, la DTI ne peut procéder sans une demande dans le système de billetterie du gestionnaire de l'employée, l'employé, de la Direction des ressources humaines ou du responsable sectoriel de la gestion des identités et des accès.

Seules les personnes dûment autorisées ont accès aux actifs informationnels de l'ITHQ, selon la nécessité de connaître l'information qu'ils renferment pour l'exercice de leurs fonctions. Les gestionnaires sont chargés de s'assurer que les actifs informationnels sous leur responsabilité sont utilisés de façon pertinente, raisonnable, circonspecte et efficace.

Dans l'éventualité où l'un ou l'autre du chef de la sécurité de l'information organisationnelle (CSIO) ou du responsable de l'accès au document et de la protection des renseignements personnels (RADPRP) est avisé qu'un membre du personnel fait une

utilisation non conforme des actifs informationnels, il en informe le gestionnaire concerné qui doit s'assurer que la situation soit corrigée.
La création des comptes aux systèmes d'information (Coba, Colnet, Maitre D, Opéra, Virtuo, etc.) et leurs privilèges sont gérés par les pilotes d'application.

6.1. Nouvel utilisateur

La création d'un compte utilisateur pour accéder au réseau de l'ITHQ est faite lors de l'embauche de l'employée, de l'employé. La Direction des ressources humaines fait parvenir la demande à la DTI qui crée le compte de l'utilisatrice, de l'utilisateur et son adresse de courriel.

Il est de la responsabilité du responsable sectoriel de la GIA d'effectuer la demande d'arrivée du nouveau membre de sa direction dans le système de billetterie afin que les permissions aux différents répertoires lui soient accordées. Dans le cas où l'embauche n'est pas effectuée par la Direction des ressources humaines (voir section 6.6), il est de la responsabilité du responsable sectoriel de la GIA d'informer la DTI.

Si le nouveau membre du personnel prend une place déjà existante, par défaut, les accès accordés sont les mêmes que ceux du prédécesseur au poste. Le gestionnaire peut décider de limiter ou d'augmenter les accès du nouveau membre de sa direction lorsque la demande d'arrivée est complétée.

Le responsable sectoriel de la GIA doit faire aussi parvenir, le cas échéant, aux différents pilotes d'application (Coba, Colnet, Maitre D, Opera, Virtuo, etc.) la demande de création de comptes pour les différents Système d'information.

6.2. Changement de poste

Le responsable sectoriel de la GIA de la direction qui reçoit le membre du personnel qui change de poste doit remplir la demande d'arrivée dans le système de billetterie afin de mettre à jour ses nouvelles permissions.

Par défaut, toutes les anciennes permissions seront supprimées et remplacées par les nouvelles figurant dans la demande d'arrivée.

6.3. Départ d'un membre du personnel

Dans le cas d'une fin d'emploi définitive, à l'exception d'un congédiement, le responsable sectoriel de la GIA doit soumettre une demande de départ à la DTI par le système de billetterie et y préciser la date et l'heure de la désactivation du compte utilisateur et des accès du membre du personnel dont l'emploi prend fin. La demande doit aussi préciser les actions à prendre avec les données (OneDrive) et les messages de la boîte de courriel de ce

membre du personnel, à savoir s'ils doivent être conservés, supprimés ou transférés à un autre utilisateur.

De plus, lorsque le membre du personnel dont l'emploi prend fin avait un ou plusieurs comptes dans les systèmes d'information de l'ITHQ, le responsable sectoriel de la GIA doit, sans délai, requérir la suppression de ces comptes par les pilotes d'application (Coba, Colnet, Maître D, Opéra, Virtuo, etc.).

Dans le cas du congédiement d'un membre du personnel, le gestionnaire doit contacter la directrice, le directeur de la DTI afin de l'informer de la date et de l'heure auxquelles le compte utilisateur et les accès du membre du personnel en question doivent être désactivés. Ainsi, les désactivations requises seront effectuées avant que le membre du personnel concerné ne retourne à son poste de travail à la suite de l'annonce de son congédiement.

Par défaut, lors du départ d'un membre du personnel, les données de son OneDrive sont conservées pendant 30 jours civils à compter de sa date de départ, après quoi elles sont supprimées.

6.4. Absence prolongée

Lors d'une absence sans solde, absence pour un congé de maladie, de maternité, la désactivation du compte et le retrait des accès seront laissés à la discrétion du gestionnaire.

Avant son départ, le membre du personnel dont l'absence prolongée est planifiée à l'avance est responsable :

a) d'acheminer ou de partager à une personne remplaçante, les messages professionnels nécessaires à la poursuite des activités de la direction concernée;

b) d'ajouter comme codétentrice une personne remplaçante qui pourra avoir accès aux documents, aux répertoires et aux groupes d'échanges nécessaires à la poursuite des activités de la direction concernée.

Dans le cas où l'absence prolongée du membre du personnel résulte d'une situation imprévue, son gestionnaire doit alors soumettre une demande à la DTI par le système de billetterie pour que les actions susmentionnées puissent être exécutées.

6.5. Personnel enseignant non permanent

Toute personne enseignant à l'ITHQ possède un compte lui donnant accès à des actifs informationnels.

Lorsque cette personne n'a pas de tâches pendant deux sessions consécutives, son compte

est automatiquement désactivé et après trois sessions consécutives, ce compte est supprimé définitivement.

6.6. Comptes invités (stagiaire, consultant, contractuel)

Un compte invité permet à une personne qui n'est ni une étudiante inscrite, un étudiant inscrit, ni un membre du personnel de l'ITHQ, d'avoir accès temporairement à certains actifs informationnels (dossiers, courriels, SharePoint, etc.) de l'ITHQ. Il est de la responsabilité du responsable sectoriel de la GIA d'effectuer la demande d'arrivée dans le système de billetterie en précisant la nature du poste de la nouvelle personne et la date de fin de contrat. Un compte invité est supprimé automatiquement à la date de fin du contrat de la personne concernée.

6.7. Compte et accès étudiant

L'étudiante, l'étudiant inscrit à l'ITHQ possède un compte lui donnant accès aux actifs informationnels mis à sa disposition et une adresse de courriel pour les communications avec la direction de l'école.

Lorsqu'il n'est plus inscrit depuis deux sessions consécutives à un cours, son compte est désactivé. S'il se réinscrit, son compte sera réactivé.

Une personne diplômée de l'ITHQ conserve son adresse de courriel indéfiniment.

6.8. Attribution des permissions sur les répertoires

Pour toute demande d'ajout ou de retrait d'accès à un actif informationnel, le responsable sectoriel de la GIA doit acheminer une demande à la DTI par le système de billetterie.

Pour les demandes d'accès dans SharePoint, si le site existe, les demandes doivent être adressées aux propriétaires identifiés de ces sites.

6.9. Accès aux systèmes d'information

Pour la création de comptes aux systèmes d'information (Coba, Colnet, Maître D, Opéra, Virtuo, etc.) les demandes doivent être envoyées par courriel aux pilotes d'application identifiés de ces systèmes d'information. Une fois les comptes créés, les pilotes d'application feront parvenir la demande d'installation et d'attribution des accès à la DTI pour le compte de l'utilisatrice, l'utilisateur concerné.

6.10. Enregistrement de données ou de documents

L'ITHQ a fait le choix institutionnel de l'infonuagique publique de Microsoft (OneDrive et SharePoint) pour l'enregistrement de ses données.

Lorsqu'une utilisatrice, un utilisateur souhaite partager des documents contenant des renseignements personnels ou des informations confidentielles à une personne ou un organisme externe à l'ITHQ au moyen de l'infonuagique institutionnelle, une analyse des impacts potentiels en cas de bris de confidentialité doit préalablement être réalisée. Pour ce faire, l'utilisatrice, l'utilisateur souhaitant procéder à ce partage en avise le CSIO qui, par la suite, soumet le résultat de son analyse au gestionnaire responsable des actifs informationnels concernés.

Lors des collaborations externes, seuls les outils de collaboration technologiques d'Office 365 mis à la disposition des utilisateurs par la DTI doivent être utilisés. Le partage avec l'infonuagique publique, telle que Dropbox, Facebook, Google Drive, etc. est interdit et ne doit être utilisé qu'à des fins personnelles.

6.11. Audit et correction

Afin de permettre aux gestionnaires de confirmer la justesse des accès et de corriger les écarts identifiés dans un délai raisonnable, deux audits périodiques sont réalisés par la DTI. Trimestriellement pour les systèmes d'information et annuellement pour les permissions des actifs informationnels. Notamment en vérifiant que :

a) les accès sont toujours pertinents ;
b) les utilisatrices et les utilisateurs autorisés sont les seuls qui ont accès;
c) les permissions spécifiques ou spéciales sont toujours requises;
d) les comptes qui ont des privilèges élevés sont bien protégés.

Trimestriellement, les gestionnaires reçoivent un rapport identifiant les comptes inactifs de leur direction depuis plus de six mois. Les données issues de cet indicateur permettront de détecter les comptes inactifs, notamment ceux qui sont sans justification et, conséquemment, de découvrir de potentielles lacunes dans le traitement des accès.

7. MESURES ADMINISTRATIVES, DISCIPLINAIRES OU LÉGALES

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

8. RÔLES ET RESPONSABILITÉS

8.1. Direction générale

Adopter et approuver la mise en œuvre de la présente directive.

8.2. 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.

S’assurer que les gestionnaires nomment des responsables sectoriels pour la gestion des identités et des accès pour la gestion des actifs informationnels relevant de leur autorité.

S’assurer que les gestionnaires révisent périodiquement les permissions et veillent à leur conformité aux habilitations associées.

Mettre en place et tenir à jour la liste des responsables sectoriels de la gestion des identités et des accès.

S’assurer que les responsables sectoriels de la gestion des identités et des accès assument pleinement leur responsabilité en matière de gestion des accès.

8.3. Direction des technologies de l’information (DTI)

Contribuer à l’élaboration, la mise en œuvre et la révision de la présente directive.

Mettre en place les solutions technologiques répondant aux exigences de la présente directive.

Procéder à la création des comptes et à l’attribution des accès aux utilisatrices, aux utilisateurs dûment autorisés par les gestionnaires et les responsables sectoriels de la gestion des identités et des accès.

Produire à l’intention des gestionnaires et des responsables sectoriels de la gestion des identités et des accès les rapports périodiques des comptes et des accès, conformément à l’article 6.11 de la présente directive, et s’assurer de leur validation.

Mettre en place les mesures correctives concernant le contrôle des accès découlant des recommandations des rapports d’audit et des tests d’intrusion.

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

Élaborer et mettre à jour la *Directive sur la gestion des identités et des accès* puis la soumettre pour validation à la directrice générale.

Définir le processus formel de gestion des accès.

S’assurer de la mise en œuvre et de la révision de la présente directive.
S’assurer de la conformité des règles d’attributions des accès.

S’assurer qu’un audit des contrôles d’accès est effectué périodiquement.

8.5. Gestionnaires

Être la personne responsable des actifs informationnels et des systèmes d'information sous sa responsabilité, notamment en veillant, du point de vue décisionnel, fonctionnel et opérationnel à leur accessibilité, utilisation adéquate, gestion efficiente et sécurité.
Désigner un membre de sa direction et un substitut comme responsable sectoriel de la GIA pour effectuer les demandes d'arrivées et de départs ainsi que les demandes d'attribution des accès aux différents systèmes d'information et les demandes d'accès aux locaux.

Déterminer les règles d'accès aux actifs informationnels sous sa responsabilité, basées sur les rôles des personnes concernées et leurs responsabilités à l'égard de cet actif et s'assurer de leur application.

S'assurer de la compréhension et de l'application de la présente directive par les membres de sa direction.

Réviser trimestriellement les autorisations d'accès applicatifs pour les systèmes sous sa responsabilité.

Gérer les accès aux différents systèmes d'information sous sa responsabilité et informer la DTI du retrait des accès, le cas échéant.

Identifier les actifs informationnels de sa direction qui doivent être protégés, et ce, conformément à la catégorisation des actifs informationnels réalisée en collaboration avec le CSIO, telle que prévue par la *Politique sur la sécurité de l'information.*
S'assurer que chaque membre de sa direction ait accès à l'information nécessaire à la réalisation de ses tâches normales.

Récupérer, lors du départ d'un membre de sa direction, les différentes cartes d'identité et d'accès, les clefs, les actifs informationnels, les documents produits dans le cadre de ses fonctions, ainsi que tout autre bien, équipements électroniques qui ont été mis à sa disposition par l'ITHQ dans le cadre de ses fonctions.

8.6. Responsable sectoriel de la gestion des identités et des accès

Effectuer la demande de création ou de suppression des accès des membres de sa direction lors de leurs arrivées ou leurs départs auprès de la DTI.

Effectuer la demande de création ou de suppression des accès des membres de sa direction lors de leurs arrivées, de leurs affectations, de leurs absences prolongées ou de leurs départs auprès des pilotes d'application pour les différents systèmes d'information.

Gérer les exceptions des accès attribués aux utilisatrices, aux utilisateurs (consultantes, consultants, stagiaires, fournisseurs) et s'assurer de leur retrait lorsqu'elles ne sont plus requises.

Effectuer les demandes d'ajout de matériels ou de logiciels pour les membres de sa direction.

8.7. Pilotes d'application

Définir et mettre à jour les profils d'accès applicatifs supportés par les systèmes d'information dont il assure le pilotage.

Autoriser l'accès aux systèmes d'information sous sa responsabilité seulement aux utilisatrices, aux utilisateurs autorisés.

Effectuer la demande d'installation ou de suppression des applications clientes, sur les postes des utilisatrices, des utilisateurs, des systèmes d'information sous sa responsabilité auprès de la DTI.

Produire trimestriellement à son gestionnaire les rapports des autorisations d'accès pour les systèmes d'information dont il assure le pilotage.

8.8. Utilisateurs

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

Se conformer à la présente directive et à toute autre document normatif en matière de sécurité de l'information et d'utilisation des actifs informationnels.

Gérer ses codes d'accès, mots de passe, jetons numériques et les autres moyens d'authentification de façon confidentielle et choisir les mots de passe selon les règles définies par la DTI.

Respecter les consignes de restriction d'accès. Ne pas divulguer, en tout ou en partie, ni faciliter l'accès à un actif informationnel à des personnes non autorisées.

Aviser son gestionnaire lorsqu'un accès qui lui a été octroyé n'est plus nécessaire dans l'exercice de ses fonctions.

Ne pas conserver des renseignements personnels ou confidentiels dans des endroits ou des environnements qui risquent de compromettre leur confidentialité.

Ne pas usurper l'identité d'une autre personne, d'un groupe ou d'une organisation.

9. RESPONSABLE DE L'APPLICATION

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

10. ENTRÉE EN VIGUEUR

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

11. MISE À JOUR

La présente directive devra être mise à jour tous les trois ans.

12. SIGNATURE

Signée à Montréal, le 30 janvier 2024.

Original signé

Liza Frulla
Directrice générale

Institut de tourisme et d'hôtellerie Québec

DIRECTIVE SUR LA PROTECTION CONTRE LES INCIDENTS DE SÉCURITÉ

Numéro du document	DIR- 2400-02-REV01	
Préparée par	Welly Augustin, directeur, Direction des technologies de l'information Déwi Collin, secrétaire générale adjointe, Secrétariat général	
Instance consultée	- Comité sur l'accès à l'information et de la protection des renseignements personnels - Comité de gestion	
Recommandée par	S.O.	
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	2021-11-30

Table des matières

1. PRÉAMBULE

La transformation numérique amène certes des possibilités aux organisations, mais elle s'accompagne également d'enjeux qui se multiplient en matière de protection de l'information ainsi que des systèmes informatiques et des infrastructures qui assurent les services.

La *Directive de protection contre les incidents de sécurité* découle de *la Politique de sécurité de l'information de* l'Institut de tourisme et d'hôtellerie du Québec (ITHQ). Celle-ci s'appuie sur le cadre de gestion des risques et des incidents à portée gouvernementale du ministère de la Cybersécurité et du Numérique qui présente une approche de gestion des risques et des incidents susceptibles de porter atteinte à la sécurité de l'information, et dont la mise en œuvre exige que des actions de sensibilisation soient menées à tous les échelons de l'organisation.

2. OBJET

L'ITHQ met en œuvre la présente directive afin de promouvoir auprès de ses utilisateurs le développement de comportements et de pratiques exemplaires à adopter devant les incidents de sécurité. Elle vise à mettre en place une organisation résiliente et protégée par la prise en charge des risques de sécurité en anticipant les menaces, puis en adaptant constamment les moyens pour s'en protéger. L'ITHQ mise ainsi sur le développement des compétences et la sensibilisation de ses utilisateurs à l'égard des risques.

De façon plus spécifique, elle indique les rôles et responsabilités des différents intervenants, les mesures à suivre pour contrer les incidents de sécurité et la démarche à suivre lors de la survenance d'un tel incident.

3. CHAMP D'APPLICATION

Cette directive s'adresse à 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 directive fait référence aux exigences des lois et des documents normatifs suivants :

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

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

c) la *Politique gouvernementale de cybersécurité*;

d) la *Politique sur la sécurité de l'information de l'ITHQ*;

e) la *Directive sur la sécurité de l'information gouvernementale.*

5. DÉFINITIONS

Les définitions à considérer pour l'application de la présente directive 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.

Cyberincident : Événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique. Il peut s'agir, par exemple, d'une source de chantage pour avoir accès à nos données, de la revente d'informations personnelles ou d'usurpation d'identité.

Incident de confidentialité : Accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

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 autre, est dûment autorisé à utiliser un actif informationnel de l'ITHQ.

6. RÔLES ET RESPONSABILITÉS

6.1. Direction générale

Adopter la présente directive.

Nommer le directeur des technologies de l'information à agir comme Chef de la sécurité de l'information organisationnelle (CSIO).

Être informé de tout incident de sécurité susceptible de porter atteinte à la réputation de l'ITHQ.

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

S’assurer de la mise en œuvre et de la révision de la présente directive.

Contribuer aux analyses de risques de sécurité de l’information afin d’identifier les menaces et les situations de vulnérabilité et de mettre en place les solutions appropriées.

Contribuer à la mise en place du processus de gestion des incidents de sécurité de l’information.

Être informé de tout incident de sécurité.

Déclarer les risques et les incidents de sécurité de l’information à portée gouvernementale au Centre opérationnel de cyberdéfense (COCD).

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

Collaborer à l’élaboration du contenu d’un plan de communication, d’un programme de sensibilisation et de formation en matière de sécurité de l’information et veiller au déploiement de ceux-ci.

Prescrire des mesures de protection des renseignements personnels, de vérifier l’application de telles mesures, s’il y a lieu, et d’exiger que des correctifs soient apportés, le cas échéant.

Tenir le registre des incidents de confidentialité, s’assurer qu’il soit tenu à jour, que les incidents soient documentés.

Informer la Commission d’accès à l’information advenant un incident de confidentialité, et qu’il y a risque de préjudice sérieux.

6.4. Direction des technologies de l’information (DTI)

Réaliser un plan de communication et des activités de formation et de sensibilisation pour soutenir la mise en œuvre de la directive et évaluer régulièrement ces activités pour procéder aux ajustements nécessaires.

Tenir le registre des incidents de sécurité de l’information et s’assurer qu’il soit tenu à jour, et que les incidents soient documentés.

Élaborer une procédure de gestion des incidents dès leur identification jusqu’à leur traitement, dépendamment de leur sévérité.

Collaborer au processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents.

6.5. Gestionnaires

S'assurer que les utilisateurs sous sa responsabilité soient informés de la présente directive dans le but qu'ils s'y conforment, afin que les exigences en matière de sécurité de l'information soient respectées dans tout processus et dans tout contrat sous sa responsabilité.

Faire signer aux utilisateurs externes sous son autorité, préalablement à l'accès à des renseignements personnels et confidentiels, des engagements au respect de la confidentialité de ces renseignements selon l'Annexe 1 du présent document.

Collaborer à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité, ainsi qu'à toute opération de vérification de la sécurité de l'information.

Rapporter au CSIO tout problème lié à l'application de la présente directive.

6.6. Utilisateurs

Respecter la présente directive.

Collaborer à toute intervention visant à atténuer ou endiguer toute menace à la sécurité de l'information ou tout incident de sécurité.

Suivre les mesures pour contrer les menaces liées à la sécurité de l'information et les mesures pour déclarer les incidents de sécurité.

Protéger de façon adéquate tous les actifs informationnels mis à sa disposition dans le cadre de son mandat (ex. : télétravail, transport, etc.).

Signaler immédiatement à la DTI et à son supérieur immédiat tout événement susceptible de constituer une contravention à la présente directive ou pouvant risquer de porter atteinte à la sécurité de l'information ou à la confidentialité des renseignements personnels ou confidentiels.

Assister aux formations requises.

7. MESURES POUR CONTRER LES INCIDENTS DE SÉCURITÉ

7.1. Mesures pour contrer les incidents de confidentialité

Tout utilisateur doit suivre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité, de leur utilisation, de leur quantité, de leur répartition et de leur support.

Pour cela, il doit notamment :

a) placer tout document confidentiel dans un espace verrouillé;

b) utiliser les renseignements personnels auxquels il a accès uniquement pour la réalisation de ses tâches;

c) ne pas communiquer les renseignements personnels, sans le consentement de la personne concernée ou de la personne titulaire de l'autorité parentale, à qui que ce soit;

d) valider toujours l'identité d'une personne lui demandant des informations sensibles;

e) rendre accessibles les renseignements personnels aux personnes uniquement qui ont la qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions et sont utilisés aux fins pour lesquels ils ont été recueillis ou que la loi autorise leur utilisation;

f) transmettre de façon sécuritaire tous les renseignements personnels ou confidentiels lorsque ceux-ci sont communiqués par courriel ou Internet. Ces renseignements doivent nécessairement faire l'objet d'un chiffrement ou être protégés par un dispositif de sécurité approuvé par la DTI. En cas de communication par courrier, l'utilisateur doit indiquer sur l'enveloppe la mention « personnel et confidentiel »;

g) détruire de façon sécuritaire les renseignements personnels, lorsque les fins pour lesquelles il a été collecté ou utilisé sont accomplies.

7.2. Mesures pour contrer les cyberincidents

Afin de contrer les cyberincidents, tout utilisateur doit :

a) verrouiller en tout temps son poste de travail lorsqu'il le quitte;

b) s'abstenir de donner ses identifiants à une tierce personne;

c) dissocier les mots de passe pour le travail et ceux des services personnels;

d) s'abstenir de télécharger des logiciels ou utilitaires non autorisés sur les équipements fournis par l'ITHQ. En cas de doute, il doit se référer à la DTI;

e) ne pas brancher de clé USB ou tout autre support amovible d'origine inconnue sur un poste de travail de l'ITHQ;

f) éviter d'envoyer des informations personnelles ou financières par courriel;

g) éviter de cliquer sur un lien hypertexte contenu dans un courriel, ou ouvrir un fichier joint provenant de correspondants inconnus;

h) être vigilant,ne pas entreprendre d'action, ni répondre, ni suivre les indications contenues dans un courriel suspect. En cas de doute, l'utilisateur doit informer la DTI en faisant suivre le courriel au besoin;

i) activer un mot de passe et le verrouillage automatique, et faire régulièrement les mises à jour du logiciel d'exploitation pour les appareils électroniques utilisés à des fins professionnelles;

j) bloquer toute connexion automatique à des réseaux sans-fil inconnus sur ses appareils électroniques utilisés à des fins professionnelles.

8. PROCÉDURE ADVENANT UN INCIDENT DE SÉCURITÉ

La procédure suivante doit être respectée par toute personne qui a un motif de croire qu'un incident de sécurité s'est produit.

Tout utilisateur qui a un motif de croire qu'un incident de sécurité s'est produit doit immédiatement en aviser la DTI et son gestionnaire.

L'utilisateur doit recueillir dans la mesure du possible le maximum d'éléments afin de faciliter la documentation de l'incident, comme par exemple, la date et l'heure de l'incident, les circonstances, etc. Il ne doit ni supprimer quelconque élément, ni éteindre son poste de travail s'il y a lieu, afin que les éléments de preuve puissent être sauvegardés.

La DTI informe le CSIO de la situation.

Le CSIO doit évaluer la situation en :

a) établissant les circonstances de l'incident;

b) identifiant les personnes concernées;

c) trouvant le problème, que ce soit une erreur, une vulnérabilité, etc.;

d) déterminant si des renseignements personnels sont impliqués.

S'il s'agit d'un incident de confidentialité, le CSIO doit en informer immédiatement le RADPRP.

Le CSIO doit seul, ou en collaboration avec le RADPRP lorsqu'il s'agit d'un incident de confidentialité, identifier la nature et la sévérité du préjudice. Pour évaluer ce préjudice dans ce dernier cas, la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables doivent être considérées dans cette évaluation :

a) lorsqu'il n'y a pas de risque qu'un préjudice sérieux soit causé, le CSIO, en collaboration avec toute direction concernée, doit prendre toutes les mesures afin de réduire les préjudices et éviter qu'un tel incident ne se reproduise;

b) lorsqu'il existe un risque qu'un préjudice sérieux soit causé, le CSIO doit, sans délai, saisir le comité de gestion de crise afin de gérer les risques à court et moyen terme pour qu'un tel incident ne se reproduise plus et déclencher les plans de mesures d'urgence, le cas échéant. Par la suite, le CSIO doit en aviser le COCD du ministère de l'Enseignement supérieur;

c) lorsqu'il existe un risque qu'un préjudice sérieux soit causé, et qu'il s'agisse d'un incident de confidentialité, le RADPRP :

   i. doit s'associer avec le responsable de l'actif informationnel ainsi que toute autre personne utile selon la nature de l'incident, pour prendre en charge le traitement de l'incident;

   ii. doit aviser la Commission d'accès à l'information, dès que possible et remplir la déclaration prévue à cet effet;

   iii. doit aviser toute personne dont un renseignement personnel est concerné par l'incident, à moins que cet avis ne soit susceptible d'entraver une enquête;

   iv. peut aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne communiquant que les renseignements personnels nécessaires à la poursuite de cet objectif.

Lorsqu'il s'agit d'un incident de confidentialité, le RADPRP doit l'inscrire au registre des incidents de confidentialité.

Dans tous les cas, la DTI doit inscrire l'incident au registre des incidents de sécurité de l'information, que le préjudice soit qualifié de sérieux ou non.

9. REGISTRES DES INCIDENTS

L'ITHQ doit tenir un registre des incidents de sécurité de l'information et un registre des incidents de confidentialité.

9.1. Contenu des registres

Les registres doivent contenir les renseignements suivants :

a) une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

b) une brève description des circonstances de l'incident;

c) la date de l'incident. Si cette information n'est pas connue, une approximation de la période;

d) la date ou la période au cours de laquelle l'ITHQ a pris connaissance de l'incident;

e) le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;

f) s'il s'agit d'un incident de confidentialité, une description des éléments qui amènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, telles que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

g) Si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées, de même qu'une mention indiquant si des avis publics ont été donnés par l'ITHQ;

h) Une brève description des mesures prises par l'ITHQ, à la suite de cet incident, afin de diminuer les risques qu'un préjudice soit causé.

9.2. Durée de conservation des renseignements contenus aux registres

Les renseignements contenus aux registres doivent être tenus à jour et conservés pendant une période minimale de sept ans après la date ou la période au cours de laquelle l'ITHQ a pris connaissance de l'incident.

10. MESURES ADMINISTRATIVES, DISCIPLINAIRES OU LÉGALES

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

11. RESPONSABLE DE L'APPLICATION

Le chef de la sécurité de l'information organisationnelle (CSIO) est responsable de l'application de la présente directive.

12. ENTRÉE EN VIGUEUR

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

13. MISE À JOUR

La directive est mise à jour tous les trois ans.

14. SIGNATURE

Signée à Montréal, le 15 juin 2023

ORIGINAL SIGNÉ

Liza Frulla
Directrice générale

ANNEXE 1 – Engagement de confidentialité

1. Je suis une personne (employée / prestataire de service / autre) de l'ITHQ et, à ce titre, j'ai été affecté(e) à l'exécution du mandat suivant :

   _____

   _____ en date du _____

2. Je m'engage, sans limites de temps, à garder la confidentialité, à ne pas communiquer ou permettre que soit communiqué à quiconque quelque renseignement ou document, quel qu'en soit le support, qui me sera communiqué ou dont je prendrai connaissance dans l'exercice ou à l'occasion de l'exécution de mes fonctions, à moins d'avoir été dûment autorisé à le faire par la personne en autorité.

3. Je m'engage également, sans limites de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre de mon mandat.

4. J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter tout ou partie du présent engagement de confidentialité m'expose à des recours légaux, disciplinaires, administratifs, des réclamations, des poursuites, et toutes autres procédures en raison du préjudice causé pour quiconque est concerné.

5. Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

   ET J'AI SIGNÉ À _____

   CE _____ JOUR DU MOIS DE_____ DE L'AN_____

   _____

   Signature du déclarant ou de la déclarante