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