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