Régie de l'assurance maladie Québec
Secrétariat général et Services à la gouvernance

DIRECTIVE
RI-2211

IDENTIFICATION DU DOCUMENT Section obligatoire

Titre	Sécurité de l'accès logique aux actifs informationnels	Date d'entrée en vigueur	2020-11-30
Thème	Ressources informationnelles		
Sous-thème	Protection et sécurité de l'information		
Unité responsable	Direction générale de la planification, de l'intégration, des architectures et de la sécurité		
Approuvée par	Vice-président aux technologies de l'information	Date d'approbation	2020-11-30

ORIGINAL SIGNÉ par : Gaël Ségal
Signature du vice-président

2020-11-30
Date de la signature

INTRODUCTION Section obligatoire

CONTEXTE

L'information est au cœur des services livrés par la Régie à ses clients et partenaires. La valeur et la sensibilité de cette information est considérable, compte tenu du rôle qu'elle joue dans les différents processus de l'organisation. L'encadrement de l'accès à cette information nécessite la mise en œuvre de règles appropriées de gestion des accès afin d'en assurer la disponibilité, l'intégrité et la confidentialité.

Par ailleurs, la *Directive sur la sécurité de l'information gouvernementale* exige que soit mis en œuvre un processus formel de sécurité de l'information permettant d'assurer la gestion de l'accès à l'information. La mise en place d'un tel processus doit s'appuyer sur des règles de gestion des accès formelles, communes et reconnues.

CHAMP D'APPLICATION

La présente directive porte sur l'accès logique aux actifs informationnels détenus par la Régie et ceux dont la gestion lui a été confiée.

Elle concerne les employés de la Régie et ses fournisseurs de services ainsi que ses clients et ses partenaires d'affaires.

En outre, en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, le dirigeant de l'information du secteur de la santé et des services sociaux a défini des règles particulières en matière de gestion de l'information. Ces règles particulières, établies dans le cadre de la mise en œuvre de la Loi concernant le partage de certains renseignements de santé (LPCRS), sont applicables à l'égard de la sécurité des actifs informationnels définis dans cette loi, incluant le Dossier Santé Québec et, le cas échéant, ont préséance sur la présente directive. À défaut, les règles énoncées ci-après s'appliquent.

ÉNONCÉ DE LA DIRECTIVE Section obligatoire

OBJECTIFS

La présente directive précise les règles concernant la sécurité de l'accès logique aux actifs informationnels de la Régie. Elle vise essentiellement à énoncer les règles générales et spécifiques sur lesquelles doivent s'appuyer les processus opérationnels de gestion des accès et à définir les rôles et responsabilités des intervenants impliqués.

RÈGLES GÉNÉRALES

1. Les mesures de sécurité à mettre en œuvre pour assurer la sécurité de l'accès sont déterminées en considérant la valeur et la sensibilité des actifs à protéger ainsi que la probabilité d'occurrence et les effets et conséquences anticipés de tout événement pouvant affecter la sécurité de ces actifs.
2. La personne à qui un identifiant est attribué en est responsable et est présumée être l'auteur des actions effectuées avec cet identifiant.

   La personne responsable d'un identifiant attribué à une entité administrative ou technologique, assume, au regard de cet identifiant et de son authentifiant, les responsabilités définies dans ce document comme étant celles de l'utilisateur. Elle est alors présumée être l'auteur des actions effectuées avec cet identifiant.
3. L'accès, par une personne ou une entité, à un document technologique renfermant des renseignements confidentiels doit pouvoir être imputé à cette personne ou au responsable de l'identifiant de cette entité administrative ou technologique.

   L'identification de la personne ou de l'entité, le document technologique accédé ainsi que le moment et le type d'action réalisée doivent faire l'objet d'une inscription dans un registre protégé.
4. Il est jugé répréhensible de chercher à rendre inopérant un mécanisme de contrôle de l'accès ainsi que d'accéder ou de tenter d'accéder à un actif informationnel en cherchant à contourner ou éluder un tel mécanisme.

   Sont exclus de l'application de cette règle, les essais réalisés par des personnes spécifiquement mandatées aux fins de vérification de l'efficacité des mesures de sécurité en place.

RÈGLES SPÉCIFIQUES

1. Gestion des identifiants

Création et attribution

1.1 La forme des identifiants, leurs modes de création, de modification et de communication ainsi que leur délai de réattribution à un autre utilisateur doivent être formellement établis.

1.2 Un identifiant est créé et attribué uniquement sur réception d'une demande autorisée par un gestionnaire (utilisateur interne) ou par un représentant désigné d'un organisme externe (utilisateur externe).

1.3 Un identifiant nouvellement créé est remis ou communiqué à son utilisateur légitime en appliquant un processus établi permettant de certifier l'identité de l'utilisateur.

L'identifiant destiné à une entité administrative ou technologique est communiqué à une personne qui doit se rendre responsable de sa bonne garde et utilisation.

1.4 Un identifiant qui n'est plus utilisé ne peut être réattribué à une autre personne avant un certain délai établi afin de préserver l'imputabilité des actions réalisées par l'entremise de cet identifiant.

1.5 L'attribution d'un identifiant doit s'accompagner d'une information relative au respect des règles en vigueur à la Régie visant à assurer la sécurité de ses actifs informationnels.

1.6 Pour répondre à des impératifs opérationnels, requérant alors obligatoirement l'approbation du détenteur de l'information concerné et du responsable organisationnel de la sécurité de l'information (ROSI), un identifiant de type partagé peut être créé et attribué. Des mesures spécifiques sont mises en place pour assurer l'imputabilité des actions réalisées par l'entremise de cet identifiant.

1.7 Un identifiant dont l'identité de l'utilisateur n'est pas déterminée peut être inscrit dans un système de contrôle de l'accès à la condition qu'il ne puisse être utilisé pour accéder à des actifs informationnels (identifiant suspendu ou aucun privilège d'accès attribué).

1.8 La forme d'un identifiant, dans la mesure où les moyens disponibles le permettent, ne doit donner aucune indication quant aux privilèges d'accès particuliers pouvant lui être octroyés.

1.9 L'information relative à l'identité de l'utilisateur d'un identifiant ainsi qu'aux privilèges d'accès qui lui sont associés ne doit être révélée à l'extérieur de l'organisation sans l'autorisation du ROSI.

Utilisation

1.10 Seule la personne à qui un identifiant a été personnellement attribué est autorisée à en faire usage. Elle n'accède aux actifs informationnels et ne les utilise que dans le cadre de l'exercice de ses fonctions et que pour les fins permises.

1.11 Sauf circonstances exceptionnelles (ex. : départ définitif précipité, absence prolongée imprévisible), il est interdit d'utiliser l'identifiant attribué à une autre personne ou entité administrative ou technologique pour accéder à un actif informationnel.

Si le besoin survient, le gestionnaire de la personne responsable de l'identifiant doit en faire la justification et obtenir au préalable l'approbation du ROSI. Selon le contexte (personne concernée, nature des accès possibles, sensibilité de l'information, etc.), d'autres autorisations pourraient être requises (ex. : détenteur, Responsable du bureau de l'accès à l'information et à la protection des renseignements personnels). L'usage qui sera alors fait de l'identifiant doit être d'une durée limitée. L'utilisateur dont on désire ainsi emprunter l'identité doit, tant que possible, en être informé et pouvoir préserver la confidentialité de son authentifiant.

1.12 Aux fins de validation, une liste des identifiants et de leur responsable (utilisateur), attribués en réponse aux besoins de son unité administrative, est transmise périodiquement au gestionnaire.

Suspension d'un identifiant

1.13 La suspension d'un identifiant peut être requise lors des événements suivants :

- N'est plus requis pour une période supérieure à 10 jours ouvrables (ex. : congé de maternité, maladie) excluant les vacances;
- N'est plus requis conséquemment à un départ précipité, sans date de retour raisonnablement envisageable;
- Lorsqu'il n'est pas utilisé au cours d'une période déterminée;
- Lorsque son usage peut compromettre la sécurité de l'information (exemple : usurpation d'identité appréhendée, soupçons de comportement malveillant).

Au regard de ces événements, le gestionnaire doit obligatoirement, dès qu'il en est informé, s'assurer qu'une requête d'absence prolongée est complétée et transmise à la DGSCE afin que celle-ci porte action. La suspension ou non de l'identifiant est sous la prérogative du gestionnaire de la personne responsable de l'identifiant.

1.14 Un identifiant ayant été suspendu sans avoir été révoqué peut être réactivé au besoin, à la demande du gestionnaire de la personne responsable de l'identifiant.

Révocation d'un identifiant

1.15 La révocation d'un identifiant est requise conséquemment aux événements suivants :

- Lorsque sa période de validité est expirée (exemple : fin de contrat);
- Lors d'un départ définitif d'une personne de la Régie (ex. : départ à la retraite, départ pour un autre ministère ou organisme gouvernemental, démission);
- Après une période déterminée de suspension, ou bien après un délai prescrit lorsqu'il n'a jamais été attribué.

Au regard de ces événements, le gestionnaire doit, dès qu'il en est informé, s'assurer qu'une requête visant la révocation de l'identifiant et de ses privilèges d'accès est transmise à la DGSCE. La révocation de l'identifiant doit prendre effet à la date de départ de la personne responsable de l'identifiant ou avec effet immédiat.

1.16 Les informations colligées concernant l'attribution d'un identifiant révoqué, ses privilèges d'accès et les actions réalisées lors d'accès obtenus sont conservées suivant la période prévue au calendrier de conservation des documents.

2. Gestion des authentifiants

Création et communication

2.1 La longueur des authentifiants, leur complexité, leur durée de vie (changement périodique) et leur réutilisation (historique) doivent être formellement établies.

2.2 Un authentifiant associé à un identifiant est remis ou communiqué de façon confidentielle à son utilisateur légitime en appliquant un processus établi.

Lorsqu'un authentifiant doit être révélé à une personne autre que l'utilisateur légitime, des instructions demandant à ce dernier de le changer le plus rapidement possible suivant sa réception doivent lui être communiquées. Préférablement, des automatismes obligeront ce changement à la première utilisation.

2.3 Une personne ne doit en aucune circonstance remettre ou communiquer à qui que ce soit, incluant le personnel de soutien technique, l'authentifiant qu'elle utilise.

2.4 Des mesures sont établies pour assurer la confidentialité d'un authentifiant lorsqu'il est inscrit sur un support quelle que soit sa forme, incluant les codes sources applicatifs.

Modification

2.5 Un authentifiant ne doit pouvoir être modifié que par l'utilisateur légitime de l'identifiant associé. Toutefois, si la confidentialité d'un authentifiant est ou peut être compromise, une modification peut alors être effectuée par une personne affectée à des tâches d'administration de la sécurité.

2.6 La réinitialisation d'un authentifiant par un administrateur de la sécurité, suite à une demande d'un utilisateur, ne doit être réalisée qu'après avoir dûment vérifié que le demandeur est bien l'utilisateur légitime de cet identifiant. L'authentifiant alors attribué doit être modifié à sa première utilisation lors d'une authentification de l'utilisateur. Dans le cas d'un identifiant d'une entité administrative ou technologique, ce changement doit être autorisé par la personne responsable de cet identifiant ou une personne qu'elle désigne à cette fin.

2.7 Des informations concernant le moment où la modification d'un authentifiant a été réalisée ainsi que l'identité de la personne ou de l'entité administrative ou technologique l'ayant effectuée sont enregistrées. Ces informations ne sont rendues accessibles qu'aux personnes autorisées.

3. Gestion de l'habilitation d'accès

Privilèges d'accès

3.1 Un privilège d'accès est octroyé à l'utilisateur désigné d'un identifiant en considérant la nature et la durée des tâches attribuées à l'utilisateur. Les principes de nécessité de faire ou de connaître, de séparation des tâches et d'attribution du minimum requis de privilèges d'accès doivent orienter les décisions prises à cet égard.

3.2 Une personne, œuvrant au sein d'une organisation cliente ou partenaire de la Régie pour laquelle des accès doivent être octroyés, doit être formellement désignée à titre de représentant auprès de la Régie. Conformément aux ententes, lois et règlements, ce représentant établit et maintient à jour les besoins d'accès de son organisation. De plus, il certifie l'identité des personnes (utilisateurs externes) à qui un identifiant et des privilèges d'accès sont attribués.

3.3 Les privilèges d'accès octroyés à un identifiant d'une entité administrative ou technologique correspondent à ceux offerts à cette entité pour réaliser le rôle ou mandat qui lui est confié. Aucune personne ne peut, du seul fait qu'elle détient ou utilise cet identifiant, prétendre à l'octroi pour elle-même des privilèges d'accès.

3.4 L'octroi de privilèges d'accès se réalise conformément à des processus approuvés qui sont appropriés à la valeur des actifs auxquels l'accès est octroyé ainsi qu'aux risques encourus.

3.5 Les décisions prises au regard de l'octroi de privilèges d'accès sont documentées dans un niveau de langage approprié aux intervenants concernés, notamment les gestionnaires et les conseillers organisationnels en sécurité de l'information.

3.6 La justesse de la définition et de l'octroi des privilèges d'accès est examinée périodiquement selon un processus établi.

3.7 Sauf circonstances exceptionnelles et requérant obligatoirement l'approbation du détenteur de l'information concernée, un privilège d'accès à des données confidentielles ne doit être attribué à un identifiant de type partagé.

3.8 Un privilège d'accès à des données confidentielles ne doit pas être attribué à un identifiant créé pour répondre à des besoins de formation. Pour répondre à ces besoins, des données fictives doivent alors être employées.

Profils d'accès

3.9 Un profil d'accès est défini en considérant la nature et la durée des tâches à accomplir. Les principes de nécessité, de séparation des tâches et d'attribution du minimum requis de privilèges d'accès doivent orienter les décisions prises à cet égard.

3.10 Un profil d'accès doit être documenté dans un niveau de langage approprié aux intervenants concernés, notamment les gestionnaires et les conseillers organisationnels en sécurité de l'information.

3.11 Un profil d'accès demeure en tout temps sous la responsabilité d'une seule unité administrative.

3.12 Tout utilisateur interne nécessitant un accès logique à un actif informationnel doit être assigné à un profil d'accès.

4. Autorisation et contrôle d'accès

Autorisation d'accès

4.1 Avant qu'il n'obtienne l'autorisation d'accès, l'utilisateur est informé que les actifs qui lui seront rendus disponibles ne doivent être utilisés que pour l'exercice de ses fonctions et que toute dérogation à cette règle peut faire l'objet de sanctions.

4.2 Un utilisateur ne devrait voir que les choix d'accès aux actifs informationnels auxquels il est autorisé.

4.3 Au moment de l'ouverture d'une session, dans la mesure du possible, l'utilisateur est informé du dernier moment où un accès a été réalisé au moyen de son identifiant ou de toute suspension de cet identifiant s'étant produite depuis ce dernier accès.

4.4 Les mécanismes d'identification et d'authentification de l'utilisateur sont sélectionnés en considérant la valeur et la sensibilité des actifs faisant l'objet du contrôle d'accès.

4.5 Une autorisation d'accès peut être accordée en se basant sur des données d'identification et d'authentification détenues par une entité administrative externe (ex. : ClicSÉQUR). La fiabilité et la sécurité des mécanismes mis en place pour assurer la collecte, le traitement, la conservation, la communication, la protection et la disposition de ces informations doivent être assurées.

4.6 L'enregistrement de données d'authentification, si requis, doit s'effectuer en utilisant un procédé permettant d'en garantir la confidentialité.

4.7 Des mesures doivent être prises pour assurer la confidentialité des données d'authentification lors de leur transmission sur un réseau.

4.8 Un authentifiant affiché à l'écran doit être illisible. Toutefois, lors de sa saisie ou de sa modification, un mécanisme peut permettre momentanément à l'utilisateur de l'afficher lisiblement pour en vérifier la composition.

4.9 Une donnée relative à l'identification ou à l'authentification du dernier utilisateur ne doit pas s'afficher automatiquement à l'écran. Cette règle ne s'applique pas pour une donnée d'identification suite à la réactivation d'une session de travail consécutive à une mise en veille (continuité d'opération par le même utilisateur).

Contrôle d'accès

4.10 Suite à une tentative d'accès refusée, aucune information précise ne doit être communiquée au requérant lui permettant de découvrir lequel des éléments d'authentification (identifiant ou authentifiant) n'est pas valide.

4.11 L'autorisation d'accès d'un utilisateur doit être suspendue après un nombre déterminé de tentatives successives et infructueuses d'authentification réalisées au moyen de son identifiant.

4.12 Un identifiant suspendu par suite de tentatives d'accès infructueuses est réactivé en appliquant une procédure ou un mécanisme préétabli qui tient compte du risque associé à cette réactivation.

4.13 Une segmentation du contrôle de l'accès est appliquée et tient compte de la valeur de l'actif à protéger et des risques appréhendés de sécurité.

4.14 L'autorisation d'accès à un actif informationnel obtenue lors d'une session de travail est annulée :

- après une certaine période d'inactivité;
- lorsque le poste utilisé pour réaliser l'accès est éteint;
- lorsque l'utilisateur met fin à sa session de travail.

4.15 Tout poste de travail présent sur un réseau interne de la Régie doit posséder un système de verrouillage requérant de l'utilisateur qu'il s'authentifie à nouveau pour reprendre une session de travail qu'il a abandonné temporairement (système de mise en veille). Ce système devrait pouvoir être activé manuellement par l'utilisateur ou se mettre en marche automatiquement après une certaine période d'inactivité.

4.16 Un utilisateur désirant accéder à un réseau interne de la Régie à partir d'un réseau externe (Internet) doit s'authentifier deux fois. Une première fois au niveau d'une interface agissant entre le réseau interne et le réseau externe. Une seconde fois, pour accéder aux actifs présents sur le réseau interne.

4.17 L'autorisation d'accès à un réseau interne accordée lors d'une session de travail à partir d'un poste situé sur un réseau externe est annulée :

- après une certaine période d'inactivité fixée;
- lorsque la quantité d'information échangée atteint un seuil maximal prédéterminé;
- lorsque des échanges sont tentés ou effectués en faisant appel à des protocoles non autorisés.

4.18 Les actions réalisées sur les actifs informationnels présents sur les réseaux internes au moyen d'un identifiant devraient être consignées dans un registre auquel l'utilisateur de l'identifiant ne peut accéder. Ces informations ne seront rendues accessibles qu'aux personnes autorisées.

4.19 Une surveillance constante de l'ensemble des activités d'accès aux actifs informationnels présents sur les réseaux internes de la Régie doit être réalisée.

5. Gestion des privilèges spéciaux

Désignation et attribution

5.1 Les identifiants créés ou utilisés pour accéder aux actifs informationnels et qui possèdent des privilèges spéciaux, notamment les identifiants de système et d'administrateur de système, doivent être formellement répertoriés.

Un registre des personnes, groupes de personnes et entités technologiques autorisées à utiliser ces identifiants doit être constitué et continuellement maintenu à jour.

5.2 La justesse de la définition et de l'octroi des privilèges spéciaux doit être revue périodiquement.

5.3 Un identifiant de système doit être détruit ou renommé à la première opportunité suivant l'installation du produit l'ayant créé; une préférence étant accordée à la destruction. L'identifiant ainsi renommé est soumis à l'ensemble des règles de la présente section.

5.4 Les circonstances menant à l'utilisation des identifiants de système doivent être limitées le plus possible. Si possible, on créera et attribuera des identifiants non partagés (identifiants de type alias) auxquels on attribuera uniquement les privilèges requis pour accomplir les tâches confiées.

Utilisations autorisées

5.5 Un identifiant de système ne doit être utilisé par une personne que pour réaliser des tâches d'administration, de vérification, d'installation, de modification ou d'entretien sur le produit l'ayant créé.

5.6 Un identifiant d'administrateur de système ne devrait être utilisé que pour réaliser des tâches d'administration, de vérification, d'installation, de modification ou d'entretien sur un produit particulier. Il ne doit permettre d'accéder à un système, réseau ou appareil autre.

5.7 Les tâches d'administration de la sécurité sont réservées aux personnes habilitées dans le cadre de leurs fonctions.

5.8 Sauf circonstances exceptionnelles, un identifiant de système ou d'administrateur de système ne doit pas être utilisé pour accéder à des renseignements confidentiels.

Le fait d'accéder à un fichier informatique contenant de tels renseignements (le contenant), sans accéder au contenu, n'est pas considéré, au regard de l'application de cet article, comme constituant un accès à des renseignements confidentiels.

Authentifiants associés aux identifiants de système et d'administrateur de système

5.9 Les règles de constitution, de modification et de communication des authentifiants associés à des identifiants de système et d'administrateur de système doivent être élaborées en considérant les risques d'atteinte à la sécurité de l'information.

5.10 L'authentifiant associé à un identifiant de système devrait être modifié immédiatement après l'installation du produit ayant créé l'identifiant ou lors d'un changement de version du produit logiciel.

5.11 L'authentifiant associé à un identifiant de système ou d'administrateur de système devrait être modifié aussitôt que possible après le départ ou le changement d'affectation d'un individu l'ayant à sa connaissance ou à sa disposition, ou en cas de doute sur l'usurpation d'un tel identifiant.

5.12 Lorsqu'un haut niveau de sécurité l'exige, l'authentifiant associé à un identifiant de système ou d'administrateur de système est conservé de façon à prévenir tout usage par une personne non autorisée. Il est remis ou communiqué à une personne dûment autorisée après inscription dans un registre protégé de son identité ainsi que du moment et de la raison de l'utilisation. L'authentifiant est modifié après chacune de ses séquences d'utilisation.

DESCRIPTION DU PROCESSUS — Section facultative

Description du processus

RÔLES ET RESPONSABILITÉS — Section obligatoire

Note : Les rôles et responsabilités définis ci-après excluent ceux relatifs à la sécurité des accès aux actifs informationnels définis dans la Loi concernant le partage de certains renseignements de santé ainsi que dans les règles particulières en découlant.

La Direction générale du soutien à la clientèle et de l'exploitation (DGSCE)

En plus d'agir comme pilote des applications de gestion des accès, la DGSCE établit les processus, mesures et normes relatives à la sécurité de l'accès logique pour les utilisateurs. Plus précisément, elle doit :

à l'égard de la gestion des identifiants :

- établir les normes et processus de gestion des identifiants;
- définir et mettre en place les processus et mesures permettant de certifier l'identité de l'utilisateur légitime lors de la communication d'un identifiant nouvellement créé;
- créer et gérer les identifiants permettant d'accéder de façon logique aux actifs informationnels;
- informer l'utilisateur d'un identifiant des responsabilités à assumer reliées à son utilisation;

à l'égard de la gestion des authentifiants :

- établir les normes et processus de gestion des authentifiants;
- définir et mettre en place les processus et mesures permettant de certifier l'identité de l'utilisateur légitime d'un identifiant lors de la réinitialisation de l'authentifiant associé à cet identifiant;
- définir et mettre en place les processus et mesures permettant l'appropriation sécuritaire d'un authentifiant par son utilisateur légitime;
- établir les mesures à prendre pour assurer la confidentialité d'un authentifiant lorsqu'il est inscrit sur un support informatique;

à l'égard de la gestion de l'habilitation d'accès :

- établir et mettre en œuvre des processus et mécanismes de gestion et de révision des privilèges et profils d'accès;
- traiter les demandes d'accès qu'elle reçoit;

à l'égard de l'autorisation et du contrôle d'accès :

- établir une norme concernant le nombre de tentatives successives et infructueuses d'authentification avant que l'autorisation d'accès d'un utilisateur soit suspendue;
- établir les procédures et mécanismes permettant la réactivation d'un identifiant suspendu;

à l'égard de la gestion des privilèges spéciaux :

- établir et mettre en œuvre des processus et mécanismes de gestion et de révision des privilèges spéciaux;
- identifier les identifiants qui possèdent des privilèges spéciaux et maintenir un registre des personnes, groupes de personnes et entités technologiques qui les possèdent;
- établir les règles de constitution, de modification et de communication des authentifiants associés à des identifiants de système et d'administrateur de système.

La Direction générale des services infrastructures technologiques (DGSIT)

La DGSIT est, entre autres, responsable de la configuration des réseaux et équipements informatiques en respect des règles de la présente directive.

Elle est aussi responsable de la gestion des répertoires d'accès de la Régie. Enfin, elle assure une surveillance des activités d'accès aux actifs informationnels présents sur les réseaux de la Régie.

Le détenteur

Le détenteur de l'information a droit de regard sur l'attribution des privilèges d'accès à l'information qui lui est confiée. De façon plus générale, il a la responsabilité de la sécurité de cette information. Il autorise, avec le soutien de son conseiller en sécurité de l'information (CSI), et selon les processus établis, les accès à l'information sous sa responsabilité et assure le suivi des privilèges d'accès accordés.

Le gestionnaire

Le gestionnaire joue un rôle essentiel au maintien de la sécurité de l'accès logique. À cet effet, avec le soutien de son CSI, il est responsable :

- d'aviser son CSI des mouvements de personnel de son secteur (entrée en fonction, changement d'unité administrative, changement de tâche, absence prolongée, départ, etc.);

- d'attribuer, de suspendre et de révoquer les identifiants et privilèges d'accès des personnes et entités technologiques qu'il gère;
- d'attribuer, de suspendre et de révoquer les identifiants et privilèges d'accès des personnes et entités externes, découlant de mandats lui étant confiés;
- d'aviser la DGSCE lorsque l'usage d'un identifiant n'est plus requis;
- d'établir et de maintenir à jour les profils d'accès requis à réalisation de la mission de son unité administrative;
- d'assigner les utilisateurs internes sous sa responsabilité aux profils d'accès de son unité administrative et de les retirer lorsque requis;
- d'aviser le coordonnateur organisationnel de gestion des incidents de la Régie lorsqu'il perçoit ou est informé que la sécurité de l'accès à l'information a été compromise ou risque de l'être.

Le responsable organisationnel en sécurité de l'information (ROSI)

Le rôle premier du ROSI est de s'assurer de la définition et la mise en place des processus entourant la gestion des accès et en vérifier l'efficacité. Il doit de plus approuver les processus, mesures et normes relatifs à la sécurité de l'accès logique. Enfin, le ROSI intervient lorsqu'une autorisation de dérogation aux présentes règles est requise.

Le coordonnateur organisationnel de gestion des incidents (COGI)

Le COGI a la responsabilité de coordonner les actions de réponse aux incidents de sécurité de l'information de la Régie.

Le conseiller organisationnel en sécurité de l'information (COSI)

Le COSI est responsable d'apporter un soutien dans la définition des processus, mécanismes et normes relatifs à la sécurité de l'accès logique et de contribuer à leur mise en œuvre.

Le conseiller en sécurité de l'information (CSI)

Le CSI agit principalement en soutien aux gestionnaires et détenteurs de son secteur lors de l'établissement, la modification et la révision des privilèges et profils d'accès à l'information des utilisateurs internes. Ainsi, selon le processus de gestion des privilèges d'accès des utilisateurs internes, il doit assurer:

- la mise à jour des privilèges d'accès rattachés à l'identifiant des utilisateurs en fonction des mouvements de personnel de son secteur;
- le traitement et le suivi des demandes d'accès de son secteur ou d'un autre secteur, à l'égard de l'information détenue par son secteur;
- le traitement et le suivi des demandes d'accès de son secteur à l'égard de l'information détenue par d'autres secteurs;
- la réalisation des exercices de révision des accès (conformité, pertinence, privilèges spéciaux) pour son secteur.

L'utilisateur

L'utilisateur est responsable de l'usage approprié de l'identifiant qui lui a été attribué. À cet égard, il :

- ne permet pas qu'une personne non autorisée accède à un actif informationnel sous sa garde ou son contrôle;
- assure la protection des moyens et données d'identification ou d'authentification mis à sa disposition et qui lui permettent d'accéder à un actif informationnel;
- met fin à un accès en cours de réalisation lorsque les exigences de son travail ne le requièrent plus;
- avise son gestionnaire lorsqu'un privilège d'accès à des données confidentielles n'est plus requis à l'exercice de ses fonctions;
- modifie son authentifiant le plus tôt possible s'il croit que sa confidentialité a été compromise;
- informe son gestionnaire lorsqu'il suspecte une atteinte à la sécurité de l'accès à l'information.

DÉFINITIONS Section facultative

Accès

Fait d'obtenir, intentionnellement ou non, la possibilité de consulter ou agir sur une information, d'utiliser un système ou un service de traitement de l'information.

Accès logique

Accès à un document technologique ou capacité d'exécuter un programme ou jeu d'instructions informatiques dans le but d'effectuer un traitement (lecture, écriture, modification ou suppression) de l'information.

Actif informationnel

Tout document ainsi que tout système d'information, appareil, réseau de télécommunication ou infrastructure technologique employé pour assurer sa conservation, son traitement, sa visualisation, sa transmission et son exploitation. En vertu de la Loi concernant le cadre juridique des technologies de l'information, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Authentifiant

Information qui, lorsque jumelée à l'identifiant d'une personne ou d'une entité administrative ou technologique, permet de valider l'identité déclarée de cette personne ou l'identification de cette entité lors d'un accès informatique. Il peut prendre la forme d'un mot de passe, d'un numéro d'identification personnel (NIP) ou autre, compte tenu de la technologie employée.

Document

En vertu de la Loi concernant le cadre juridique des technologies de l'information, un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. Est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. Les documents sur des supports faisant appel aux technologies de l'information sont qualifiés de documents technologiques.

Entité administrative

Ensemble organisé de personnes chargées de fournir un service administratif déterminé et capable d'interagir auprès d'un système informatique, notamment pour réaliser un accès logique à un actif informationnel.

Entité technologique

Élément technologique (ex : dispositif d'accès, serveur, système informatique, application informatique) chargé de fournir un service informatique déterminé et capable d'interagir auprès d'un système d'informatique, notamment pour réaliser un accès logique à un actif informationnel.

Gestionnaire

Employé de classe d'emploi de niveau cadre ou de niveau supérieur responsable d'une unité administrative.

Habilitation

Ensemble des privilèges d'accès d'un utilisateur relatifs à des données ou à des programmes. On utilise aussi le terme habilitation pour désigner l'action d'attribuer des privilèges d'accès.

Identifiant

Information associée à une personne ou entité, connue de celle-ci ou contenue sur un support informatique dont elle est la détentrice, et qui permet son identification.

Personne

Personne humaine (exclut les personnes morales).

Prérogative

Avantage particulier, privilège dû à une fonction, à un état.

Privilège d'accès

Permission d'effectuer une action (lecture, écriture ou mise à jour) sur un actif informationnel.

Privilège spécial

Privilège d'accès étendu (puissant) ou d'administration sur un actif informationnel qui implique des pouvoirs **de création, de modification ou de suppression de cet actif**. Un identifiant de système ainsi qu'un identifiant d'administrateur font notamment partie de cette catégorie. Généralement, ce type de privilège est restreint à un groupe d'employés tels que des administrateurs de réseau, des administrateurs de bases de données ou des administrateurs de la sécurité informatique. Un privilège spécial peut aussi être obtenu par un mécanisme d'élévation des privilèges permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement.

Il est à noter que l'accès en consultation à l'ensemble des données gérées par un système n'est pas automatiquement associé à un privilège spécial. Cependant, l'octroi d'un tel privilège peut conduire à l'accès à l'ensemble des données gérées par un système.

Profil d'accès

Ensemble de privilèges d'accès à des actifs informationnels nécessaires à la réalisation d'une fonction dans l'organisation. Un privilège peut être octroyé par défaut à tous les utilisateurs d'un profil ou octroyé individuellement à chaque utilisateur compte tenu de la nécessité de l'accès, de sa durée et de la valeur de l'actif informationnel concerné.

Révocation d'un identifiant

Retrait d'un identifiant inscrit au système de contrôle d'accès.

Séparation des tâches

Principe voulant qu'une personne ne puisse posséder l'ensemble des privilèges d'accès lui permettant à elle seule de compléter un processus d'affaires.

Suspension d'un identifiant

Action qui a pour conséquence de rendre temporairement l'identifiant inopérant, inactif.

Utilisateur

Personne, entité administrative ou entité technologique qui fait usage d'un identifiant. Les employés de la Régie et les ressources de ses fournisseurs de services sont désignés comme étant des utilisateurs internes tandis que les clients et les ressources relevant des partenaires font partie des utilisateurs externes.

DIRECTIVE
RI-2211

HISTORIQUE Section obligatoire

Description du changement	Instance décisionnelle	Date d'approbation
Mise à jour de la *Directive sur la sécurité de l'accès logique aux actifs informationnels* (RI-2211) par l'ajustement de la définition de « Privilège spécial ».	VPTI	2020-11-30
Mise à jour de la *Directive sur la sécurité de l'accès logique aux actifs informationnels* (RI-2211) par l'ajustement de termes et l'ajout de définition.	VPTI	2020-08-13
Révision de la *Directive sur la sécurité de l'accès logique aux actifs informationnels* (RI-2211) dans le cadre de la révision périodique du cadre normatif en sécurité et de la refonte du cadre normatif de la Régie. La politique administrative devient une directive.	VPTI	2016-10-26
Mise à jour de la *Politique administrative sur la sécurité de l'accès aux actifs informationnels* (2-50000-004) par l'ajustement de termes à la suite de l'entrée en vigueur de la nouvelle *Directive sur la sécurité de l'information gouvernementale* en 2006.	VPTI	2007-06-27
Révision de la *Politique administrative sur la sécurité de l'accès aux actifs informationnels* (2-50000-004). Celle-ci remplace la *Politique administrative sur l'accès aux actifs informationnels* (2-52110-004) du 11 février 1998.	VPTI	2006-03-28
Nouvelle *Politique administrative sur l'accès aux actifs informationnels* (2-52110-004) approuvée par la Direction générale de l'administration.	DGA	1998-02-11

ANNEXE Section facultative

Annexe