Pratique recommandée en sécurité de l'information

PR-077

Guide de gestion des accès logiques

ENSEMBLE on fait avancer le Québec

Québec

Guide de gestion des accès logiques

Version 1.0

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – Novembre 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71120-9

Table des matières

Table des figures

Acronymes

COSI : conseiller organisationnel de la sécurité de l’information

COGI : coordonnateur organisationnel de gestion des incidents

DIC : disponibilité, intégrité, confidentialité

ROSI : responsable organisationnel de la sécurité de l’information

Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel de leur participation et du travail accompli.

Équipe de réalisation

Roza Lami, chargée de projet
Secrétariat du Conseil du trésor

Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

Groupe de travail interministériel

Chantal Périé
Ministère des Relations internationales
et de la Francophonie

Christian Marcotte
Société de l'assurance automobile
du Québec

Daniel Guimont
Tribunal administratif du travail

Jacques Blouin
Régie de l'assurance maladie du Québec

Yassine Maghlout
Ministère des Finances

Makram-Mourad Laribi
Ministère de la Santé
et des Services sociaux

Mohamed-Cherif Ben Abderrahmane
Régie du bâtiment du Québec

Samuel Morin
Ministère de la Sécurité publique

Souleymane Ndoye
Secrétariat du Conseil du trésor

Notes à l'intention du lecteur

Note 1 : Le terme « organisme public » ou « organisme » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur ou du réseau de la santé et des services sociaux. [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].

Note 2 : Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chaque organisme public de les adapter à son contexte et aux risques qui lui sont propres.

Note 3 : Pour ne pas alourdir le texte, le terme « gestion des accès » est employé pour désigner la gestion des droits d'accès logiques.

Note 4 : Le guide ne couvre pas la gestion des accès physiques ainsi que la gestion des identités et des accès des utilisateurs externes aux prestations de services des organismes publics.

Note 5 : Le contenu du guide peut être considéré comme une boîte à outils en matière de gestion des accès. Celle-ci regroupe plusieurs éléments d'intérêt qui pourraient être employés séparément, à la convenance de chaque organisme public.

1. Introduction

Le recours aux technologies de l'information et des communications (TIC) s'avère incontournable dans un contexte caractérisé par une évolution croissante des besoins d'affaires et la production de données volumineuses et parfois sensibles.

Cette situation fait constamment apparaître de nouvelles menaces et de nouvelles situations de vulnérabilité susceptibles de mettre en péril la sécurité de l'information gouvernementale. De ce fait, l'information est exposée à de nombreux risques qu'il faut réduire à un niveau acceptable par la mise en place de mesures de sécurité, dont la gestion des droits et des privilèges d'accès.

À noter que la gestion des accès est un processus complexe qui intègre différentes règles, procédures et technologies. De ce fait, elle nécessite la contribution de l'ensemble des entités administratives de l'organisme. Fondamentalement, la gestion des accès est basée sur les principes de privilège minimal et de séparation des tâches et elle répond à quatre questions :

1. Qui a accès à quelle information?
2. Qui a approuvé l'accès?
3. L'accès est-il adapté aux tâches à accomplir?
4. L'accès et les opérations en découlant sont-ils correctement surveillés, consignés et enregistrés?

Le présent guide permet de répondre à ces préoccupations et sert de référence pour la mise en œuvre des pratiques de gestion des accès logiques à l'information. Il est basé sur le modèle RBAC (*Role Based Access Control*) et inclut, notamment, les rôles et responsabilités des intervenants, le processus de gestion des accès, les éléments d'encadrement de la gestion des accès et un exemple de directive sur la gestion des accès logiques.

Ce guide ne couvre pas la gestion des accès physiques ainsi que la gestion de l'identité et des accès des utilisateurs externes aux prestations de services des organismes publics.

1.1 Mise en contexte

Le présent guide s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information gouvernementale. Celle-ci est appuyée par :

- ✓ la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
- ✓ la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- ✓ les documents structurants[1] définissant le cadre de gouvernance de la sécurité de l'information dans l'administration québécoise.

1.2 Public cible

Ce guide est notamment à l'usage des personnes suivantes :

- ✓ détenteurs de l'information;
- ✓ pilotes de systèmes ou d'applications;
- ✓ gestionnaires des unités administratives de l'organisme;
- ✓ utilisateurs des ressources informationnelles;
- ✓ principaux intervenants en sécurité de l'information (ROSI[2], COSI[3], COGI[4]);
- ✓ spécialistes dans divers domaines – accès logiques, technologies de l'information, gestion des risques de sécurité de l'information, vérification interne.

1.3 Risques associés à la gestion des accès

À défaut d'un encadrement adéquat de la gestion des accès, un organisme peut s'exposer à plusieurs risques de sécurité de l'information.

- ✓ **Accès non autorisé**

  Un accès non autorisé peut mettre en péril la disponibilité, l'intégrité ou la confidentialité de l'information qu'une organisation détient dans l'exercice de ses fonctions. Il pourra ainsi causer des dommages importants, voire irréversibles, à l'organisation.

- ✓ **Altération ou destruction de données**

1. **Les documents structurants** sont la Directive sur la sécurité de l'information gouvernementale, le Cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents à portée gouvernementale et l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information.
2. **ROSI** : responsable organisationnel de la sécurité de l'information
3. **COSI** : conseiller organisationnel en sécurité de l'information
4. **COGI** : coordonnateur organisationnel de gestion des incidents

L'altération ou la destruction de données peut engendrer des résultats inexacts ou incomplets, voire un ralentissement ou une interruption des services offerts. À titre d'exemple : une altération avec intention de fraude.

- ✓ **Divulgation de l'information ou vol de données**

  La divulgation de l'information ou le vol de données est susceptible d'avoir des impacts de diverses natures : atteinte à l'image de marque de l'organisation, atteinte au droit des citoyens à la protection des renseignements personnels qui les concernent et à leur vie privée, baisse de confiance à l'égard de l'État, pertes financières, etc.

- ✓ **Augmentation du niveau de privilège**

  L'usurpation de privilèges permet à une personne non autorisée d'accéder à de l'information sensible, voire de prendre le contrôle d'applications critiques pour l'organisation. Elle pourra ainsi causer des dommages importants, voire irréversibles, à l'organisation.

2. Concepts et définitions

2.1 Contrôle d'accès

Le contrôle d'accès représente une composante essentielle de la gestion des accès. Il consiste à vérifier si un sujet (personne ou dispositif) qui demande l'accès à un objet (fichier, base de données ou dispositif) possède, à cet égard, les autorisations nécessaires [20].

Le contrôle d'accès a pour objectifs :

- ✓ de gérer et contrôler les accès logiques aux ressources informationnelles par des personnes ou des dispositifs;
- ✓ de détecter les accès non autorisés;
- ✓ de préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs;
- ✓ d'assurer la disponibilité de l'information en réduisant :
  - les attaques de déni de service;
  - les destructions ou les effacements non autorisés;
  - la propagation d'un code malicieux entre systèmes informatiques;
  - les erreurs d'opération ou de configuration des applications.
- ✓ d'assurer l'intégrité de l'information en réduisant :
  - les abus d'utilisation ou de modification;
  - les altérations par des utilisateurs non autorisés;
  - les erreurs d'utilisation;

- la dénégation des modifications.

✓ d'assurer la confidentialité de l'information en réduisant :

- les accès non autorisés;
- les divulgations involontaires;
- les diffusions non autorisées.

✓ d'assurer la traçabilité[5] des accès et des tentatives d'accès.

2.2 Droit d'accès logique

Le droit d'accès logique désigne l'effet recherché lorsqu'un sujet accède à un objet, c'est-à-dire lire, écrire, modifier, supprimer, imprimer, créer, copier, transmettre et approuver. [20]

2.3 Règle de contrôle d'accès

Une règle de contrôle d'accès définit les paramètres permettant d'évaluer l'autorisation d'accès à un objet. L'application des règles de contrôle d'accès permet d'assurer que les sujets emploient uniquement les droits d'accès qui leur sont octroyés sur les objets. [20]

Exemple de règle : Le sujet « S1 » a le droit de lire, écrire, modifier « Ob2 » de 8 h 30 à 13 h, le lundi et le mercredi.

Certaines anomalies, comme celles indiquées ci-dessous, peuvent apparaître dans un ensemble de règles de contrôle d'accès.

✓ **L'incohérence**

L'incohérence se traduit par la possibilité de dériver de l'ensemble des règles deux décisions opposées concernant un accès donné : une permission et une interdiction.

✓ **L'incomplétude**

Un système de règles de contrôle d'accès est incomplet s'il ne permet pas d'arriver à une permission ou une interdiction à propos d'une demande d'accès donnée. Il peut être rendu complet en appliquant une politique d'accès ouverte[6] ou une politique d'accès fermée[7].

✓ **La fuite d'information**

Une fuite d'information se produit lorsqu'on permet la lecture d'un fichier « F1 » à une personne qui n'a pas le droit de lire un fichier « F2 », sachant que l'information contenue dans « F1 » peut provenir en partie de « F2 ». Contrairement au cas où la fuite

---

5. **Traçabilité** : la traçabilité garantit que les accès et tentatives d'accès aux éléments considérés sont enregistrés et que ces renseignements sont normalement conservés et exploitables.
6. **Politique d'accès ouverte :** politique qui considère qu'un accès est permis, à moins qu'il ne soit explicitement interdit. [21]
7. **Politique d'accès fermée :** politique qui considère qu'un accès est refusé, à moins qu'il ne soit explicitement permis. [21]

d'information est causée par un accès non autorisé, dans cette situation, l'accès est autorisé. C'est plus un problème touchant la consistance des règles de contrôle.

- ✓ **La redondance**

  Une redondance se produit lorsque la même réponse à une demande d'accès est définie dans plusieurs règles.

2.4 Rôle

Un rôle définit les autorisations nécessaires à l'utilisation des objets (applications ou ressources). Un rôle applicatif est un ensemble de droits d'accès propres à une seule tâche dans une application. [5] Exemples :

- ✓ le rôle « Serveradmin » regroupe les permissions nécessaires pour configurer les paramètres au niveau serveur dans SQL Server;
- ✓ le rôle « Db_accessadmin » regroupe les permissions nécessaires pour ajouter et supprimer des utilisateurs de bases de données;
- ✓ le rôle « Ajouter dossier étudiant » regroupe les autorisations nécessaires pour ajouter un nouveau dossier étudiant à la base de données.

2.5 Principe du privilège minimal

Le principe du privilège minimal exige que l'utilisateur ne dispose pas de plus de droits que nécessaire pour accomplir ses tâches. Cela implique que les autorisations accordées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches associées à ce rôle. [15]. À cet effet, la politique d'accès fermé semble la plus appropriée.

2.6 Profil d'accès général

Un profil d'accès général décrit les accès standards nécessaires pour un utilisateur ou un groupe d'utilisateurs aux ressources, autres que les systèmes de mission. Il concerne les accès aux messageries, plateformes de collaboration, boîtes aux lettres partagées, listes de distribution, répertoires de données, intranet, extranet, etc. [5]. À titre d'exemple, le profil d'accès général des utilisateurs « Groupe_Usagers1 » pourrait être :

- ✓ les répertoires (K/securite, L/App, R/Log, U/Usager),
- ✓ Internet, extranet, intranet,
- ✓ plateforme de collaboration (CODD),
- ✓ liste de distribution (LD1), messagerie.

2.7 Profil d'accès applicatif

Un profil d'accès applicatif regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction sur un système de mission ou une application (exemples de profil : pilote d'application, enquêteur, analyste, DBA). Un utilisateur peut avoir un ou plusieurs profils. [5]. À titre d'exemple, le profil d'accès applicatif « Enquêteur » de l'application « AAA » regroupe les rôles (modifier dossier enquête, consulter dossier enquête) de cette application.

2.8 Matrice de profils d'accès général

Une matrice de profils d'accès général est une grille associée à une entité administrative et contenant les profils d'accès général définis pour ses utilisateurs ou groupes d'utilisateurs. Un exemple de matrice de profils d'accès général est présenté à l'annexe II « Exemple de matrice de profils d'accès général ».

2.9 Matrice de profils d'accès applicatif

Une matrice de profils d'accès applicatifs est une grille associée à un système de mission (application) et contenant les profils d'accès applicatifs supportés par ce système ainsi que les exigences de sécurité correspondantes. Un exemple de matrice de profils d'accès applicatifs est présenté à l'annexe III « Exemple de matrice de profils d'accès applicatif ».

2.10 Référentiel des profils d'accès à l'information

Répertoire dans lequel sont consignées les matrices de profils d'accès applicatifs de chaque système de mission et les matrices de profils d'accès général de chaque entité administrative.

2.11 Principe de séparation des tâches

Principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible sont réparties entre plusieurs entités (personnes, processus, etc.) afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité. Il vise à limiter les possibilités d'abus et d'infraction par une seule personne.

Exemple : une personne ne doit pas avoir la possibilité de commander une fourniture ou une prestation et celle de valider sa réception.

2.12 Habilitation

L'habilitation[8] est l'ensemble des droits d'accès autorisés à une entité par une autorité de l'organisme, généralement la hiérarchie immédiate.

L'habilitation est associée à une fonction organisationnelle et elle est constituée de l'ensemble des profils d'accès nécessaires à l'accomplissement des tâches associées à la fonction considérée. Ainsi, toutes les personnes qui exercent la même fonction organisationnelle bénéficient, théoriquement, d'une même habilitation. [5]

De plus, selon la sensibilité des données traitées par les profils d'accès composant une habilitation, des critères d'habilitation répondant à des exigences de sécurité pourraient être imposés aux personnes appelées à occuper la fonction correspondante.

Exemple : L'habilitation de la fonction « Comptable » est composée : du profil d'accès applicatif « agent de saisie » de l'application « A1 », du profil d'accès applicatif « analyste » de l'application « A2 », du profil d'accès applicatif « vérificateur » de l'application « A3 » et du profil d'accès général « utilisateurs_G1 ». Comme les données de l'application « A2 » sont des données financières avec un niveau d'intégrité « 3 » et un niveau de confidentialité « 4 » alors l'habilitation de la fonction « Comptable » est assortie des critères d'habilitation (exigences de sécurité) « vérification des antécédents judiciaires » et « enquête de crédit ».

2.13 Référentiel des habilitations

Le référentiel est le répertoire dans lequel sont consignés, pour chaque fonction organisationnelle, les profils d'accès applicatif et les profils d'accès général nécessaires pour accomplir les tâches associées à la fonction ainsi que les critères d'habilitation requis. Un exemple de référentiel des habilitations est présenté à l'annexe IV « Exemple de référentiel des habilitations ».

Il est à noter qu'un organisme peut avoir un ou plusieurs référentiels des habilitations associés à chacun de ses grands secteurs d'activité.

2.14 Comptes à privilèges spéciaux

Les comptes à privilèges spéciaux comprennent les comptes d'administrateur, les comptes intégrés[9] et les comptes utilisés pour exécuter des programmes de services[10]. Ce sont des comptes hautement sensibles qu'il faut entourer de mesures de sécurité supplémentaires et contrôler périodiquement.

---

8. **L'habilitation** est appelée également dans certains organismes « profil métier ». Il est important de ne pas la confondre avec l'habilitation sécuritaire au sens de filtrage de sécurité, lequel consiste à réaliser des enquêtes sur les bonnes mœurs des candidats devant occuper des postes évalués comme sensibles dans l'appareil gouvernemental québécois.

9. **Comptes intégrés :** comptes utilisés par un système pour se connecter à un autre système.

10. **Programmes de services :** programmes faisant généralement partie de la bibliothèque de programmes et destinés à augmenter les possibilités de base du système d'exploitation en permettant l'exécution d'opérations courantes telles que la conversion de supports de fichiers, le tri, la fusion, le diagnostic [OQLF, 2002].

3. Partage des responsabilités

Cette section décrit succinctement les responsabilités attribuées en matière de gestion des accès. Il est important de souligner qu'il revient à chaque organisme de les adapter en fonction de son propre contexte organisationnel.

3.1 Détenteur de l'information

Le détenteur[11] de l'information s'assure de la protection de l'information et des processus d'affaires relevant de sa responsabilité compte tenu du niveau de sensibilité de l'information et des risques de sécurité encourus. À ce titre, il :

- ✓ participe à l'élaboration de la directive de gestion des accès à l'information;
- ✓ établit les règles d'attribution des droits d'accès et s'assure de leur application;
- ✓ catégorise l'information relevant de sa responsabilité en vue d'en déterminer la sensibilité en termes de disponibilité, d'intégrité et de confidentialité;
- ✓ valide les critères d'habilitation requis pour autoriser l'accès à l'information;
- ✓ autorise l'accès aux seuls utilisateurs disposant des habilitations nécessaires;
- ✓ s'assure de la mise en place des mécanismes de sécurité indispensables au contrôle des accès;
- ✓ s'assure de la conformité des règles d'attribution des droits d'accès aux contextes juridique et organisationnel;
- ✓ approuve les matrices de profils d'accès applicatifs définies pour les systèmes sous sa responsabilité;
- ✓ s'assure de la conformité des exigences de sécurité associées aux profils d'accès applicatif par rapport au degré de sensibilité de l'information;
- ✓ révise périodiquement les autorisations d'accès accordées aux utilisateurs de ses applications;
- ✓ signale au détenteur du référentiel des profils d'accès à l'information toute modification apportée aux matrices des profils d'accès applicatifs;
- ✓ s'assure de l'intégration dans les ententes et contrats de clauses garantissant le respect des exigences de sécurité de l'information, dont celles sur la gestion des accès.

11. **Détenteur de l'information :** employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé. [Directive sur la sécurité de l'information gouvernementale, 2014]

3.2 Pilote d'application

Le pilote d'application :

- ✓ définit et met à jour les profils d'accès applicatifs supportés par les applications relevant de sa responsabilité;
- ✓ définit et met à jour les exigences de sécurité nécessaires à chaque profil d'accès applicatif en tenant compte du degré de sensibilité des données manipulées;
- ✓ soumet à la validation du détenteur les matrices des profils d'accès applicatifs définies ou mises à jour;
- ✓ soumet périodiquement au détenteur de l'information un état des autorisations d'accès accordées aux applications sous sa responsabilité.

3.3 Détenteur du référentiel des profils d'accès à l'information

Le détenteur du référentiel des profils d'accès à l'information est chargé :

- ✓ d'y consigner les matrices de profils d'accès applicatifs approuvées par les détenteurs de l'information et les matrices de profils d'accès général approuvées par la direction des technologies de l'information;
- ✓ de tenir à jour le référentiel et de s'assurer de la cohérence de son contenu avec la structure organisationnelle;
- ✓ de s'assurer de la sécurité et de la validité du référentiel;
- ✓ de s'assurer périodiquement auprès des détenteurs de l'information et du responsable des technologies de l'information que les profils d'accès consignés au référentiel sont conformes à toute modification de la structure organisationnelle ou modification de la description des tâches associées aux processus;
- ✓ d'attribuer les autorisations d'accès au référentiel.

3.4 Responsable organisationnel de la sécurité de l'information (ROSI)

Le ROSI :

- ✓ élabore et met à jour la directive de gestion des accès et la soumet pour validation au comité chargé de la sécurité de l'information;
- ✓ soumet à l'approbation du sous-ministre ou du dirigeant d'organisme la directive de gestion des accès et assure le suivi de sa mise en œuvre; il lui soumet également toute dérogation à l'application de la directive;
- ✓ définit le processus de gestion des accès;

- ✓ s’assure de la documentation et de la mise à jour des procédures nécessaires à la mise en place du processus formel de gestion des accès;
- ✓ s’assure de la mise en œuvre du processus de gestion des accès.

3.5 Conseiller organisationnel de la sécurité de l’information (COSI)

Le COSI :

- ✓ soutient le ROSI dans l’élaboration et la mise à jour de la directive de gestion des accès;
- ✓ soutient le ROSI dans la définition du processus de gestion des accès;
- ✓ élabore et met à jour la documentation des procédures nécessaires à la mise en place du processus formel de gestion des accès;
- ✓ met en œuvre le processus de gestion des accès;
- ✓ organise des séances de sensibilisation des utilisateurs des dispositifs mobiles aux risques de sécurité encourus par l'information à laquelle ils ont accès au moyen de ces dispositifs;
- ✓ s’assure qu’un audit des mécanismes de contrôle d’accès est effectué périodiquement.

3.6 Coordonnateur organisationnel de gestion des incidents (COGI)

Le COGI collabore étroitement avec le ROSI et le COSI et leur fournit le soutien technique nécessaire à l’exercice de leurs responsabilités en matière de gestion des accès. À ce titre, il :

- ✓ contribue à l’élaboration, la mise en œuvre et la révision de la directive de gestion des accès;
- ✓ détermine les menaces et les situations de vulnérabilité liées à la gestion des accès et, si requis, propose des mesures de renforcement des contrôles d’accès;
- ✓ formule des avis de pertinence sur les mécanismes de gestion des accès mis en place.

3.7 Sous-ministre ou dirigeant d’organisme

Le sous-ministre ou le dirigeant d’organisme :

- ✓ approuve la directive de gestion des accès et en assure la diffusion;
- ✓ approuve toute dérogation aux dispositions de la directive de gestion des accès;
- ✓ s’assure que les gestionnaires des unités administratives définissent et mettent à jour les habilitations et les critères d’habilitation associés aux fonctions organisationnelles relevant de leur autorité;
- ✓ s’assure que les détenteurs de l’information sont désignés et assument pleinement leur responsabilité en matière de gestion des accès;

- ✓ s’assure que les détenteurs de processus d’affaires documentent clairement les processus relevant de leur autorité, et particulièrement les règles de séparation des tâches;
- ✓ s’assure que les gestionnaires révisent périodiquement les autorisations d’accès octroyées à leurs employés et veillent à leur conformité aux habilitations associées.

3.8 Gestionnaire d’unité administrative

Le gestionnaire d’une unité administrative :

- ✓ contribue à l’élaboration, la mise en œuvre et la révision de la directive de gestion des accès;
- ✓ définit les habilitations et les critères d’habilitation des fonctions organisationnelles relevant de son autorité et en assure la mise à jour;
- ✓ définit, en collaboration avec la direction des technologies de l’information, les profils d’accès général associés aux groupes d’utilisateurs relevant de son autorité;
- ✓ s’assure que les processus relevant de son autorité sont bien documentés et que les règles de séparation des tâches associées sont clairement définies et appliquées;
- ✓ s’assure de la conformité des qualifications de son personnel aux critères d’habilitation associés aux fonctions occupées;
- ✓ s’assure de la compréhension et de l’application de la directive de gestion des accès par ses employés;
- ✓ remplit les formulaires nécessaires à la gestion des identifiants et des autorisations d’accès lors de l’entrée en fonction d’un employé, de son affectation, de son départ ou de son absence prolongée;
- ✓ révise périodiquement les autorisations d’accès attribuées à ses employés et veille à leur conformité aux habilitations associées aux fonctions occupées;
- ✓ gère les exceptions d’accès attribuées et s’assure de leur retrait lorsqu'elles ne sont plus requises;
- ✓ s’assure que les habilitations et les critères d’habilitation définis sont conformes aux descriptions de tâches des processus d’affaires et aux profils d’accès définis dans le référentiel des profils d’accès à l’information;
- ✓ signale au détenteur du référentiel des habilitations de son unité administrative toute modification des habilitations ou des critères d’habilitation associés aux fonctions organisationnelles sous sa responsabilité;
- ✓ s’assure de l’intégration dans les ententes et contrats de clauses garantissant le respect des exigences en matière de sécurité de l’information, dont celles sur la gestion des accès.

3.9 Détenteur du référentiel des habilitations

Le détenteur du référentiel des habilitations est chargé :

- ✓ d'y consigner les habilitations et les critères d'habilitation approuvés par les responsables d'unités administratives;
- ✓ de s'assurer périodiquement auprès des gestionnaires que les habilitations consignées au référentiel sont conformes à toute modification de la structure organisationnelle ou de la description de tâches des processus relevant de leur responsabilité;
- ✓ de s'assurer de la sécurité et de la validité du référentiel des habilitations;
- ✓ d'attribuer les autorisations d'accès au référentiel des habilitations.

3.10 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information :

- ✓ contribue à l'élaboration, la mise en œuvre et la révision de la directive de gestion des accès;
- ✓ met en place les solutions technologiques répondant aux exigences de la directive de gestion des accès;
- ✓ s'assure du bon fonctionnement des mécanismes de contrôle des accès mis en place;
- ✓ approuve les matrices de profils d'accès général;
- ✓ signale au détenteur du référentiel des profils d'accès à l'information toute modification apportée aux matrices des profils d'accès général;
- ✓ approuve les habilitations et les critères d'habilitation correspondant aux comptes à privilèges spéciaux tels que ceux associés aux postes d'administrateur réseau, d'administrateur de bases de données, d'administrateur système ou d'administrateur d'application;
- ✓ révise périodiquement les autorisations d'accès accordées aux comptes à privilèges spéciaux et s'assure de leur conformité aux habilitations;
- ✓ met en place les mesures correctives concernant les contrôles d'accès compte tenu des recommandations des rapports d'audit et des tests d'intrusion.

3.11 Administrateur des accès

L'administrateur des accès :

- ✓ applique la directive de gestion des accès et les procédures afférentes;
- ✓ crée les identifiants et les droits d'accès destinés aux utilisateurs dûment autorisés par les gestionnaires et les détenteurs de l'information;

- ✓ édite à l'intention des détenteurs de l'information et des gestionnaires les rapports périodiques des autorisations d'accès réellement attribuées et s'assure de leur validation.

3.12 Vérificateur interne

Le vérificateur interne :

- ✓ évalue et vérifie l'application, la validité et l'efficacité des règles, des mesures et des moyens technologiques mis en place en matière de gestion des accès;
- ✓ s'assure que les procédures de gestion des accès sont clairement documentées et mises en œuvre de manière efficace;
- ✓ évalue l'efficacité des pratiques de gestion des accès et leur intégration aux systèmes de mission de l'organisation;
- ✓ formule les recommandations nécessaires à l'amélioration du processus de gestion des accès et assure le suivi de leur mise en œuvre.

3.13 Utilisateurs

Dans le cadre de la gestion des accès, l'utilisateur :

- ✓ est responsable de son authentifiant[12] et doit le modifier le plus rapidement possible s'il croit que sa confidentialité est compromise;
- ✓ se conforme aux dispositions de la directive de gestion des accès et à celles des procédures afférentes;
- ✓ s'assure de la confidentialité de son mot de passe;
- ✓ se conforme aux pratiques de gestion des accès le concernant indiquées à la section 6 « Pratiques associées à la gestion des accès »;
- ✓ signale sans délai à son gestionnaire ou aux autorités désignées toute tentative d'accès non autorisée dont il est victime;
- ✓ emploie l'information à laquelle il a accès aux seules tâches qui lui sont assignées;
- ✓ avise son gestionnaire lorsqu'un privilège d'accès qui lui a été octroyé n'est plus nécessaire dans l'exercice de ses fonctions.

12. **Authentifiant :** information confidentielle détenue par une personne et permettant son authentification. Elle peut être sous la forme d'un mot de passe, d'un numéro d'identification personnel (NIP) ou autre, selon la technologie utilisée. [OQLF, 2000]

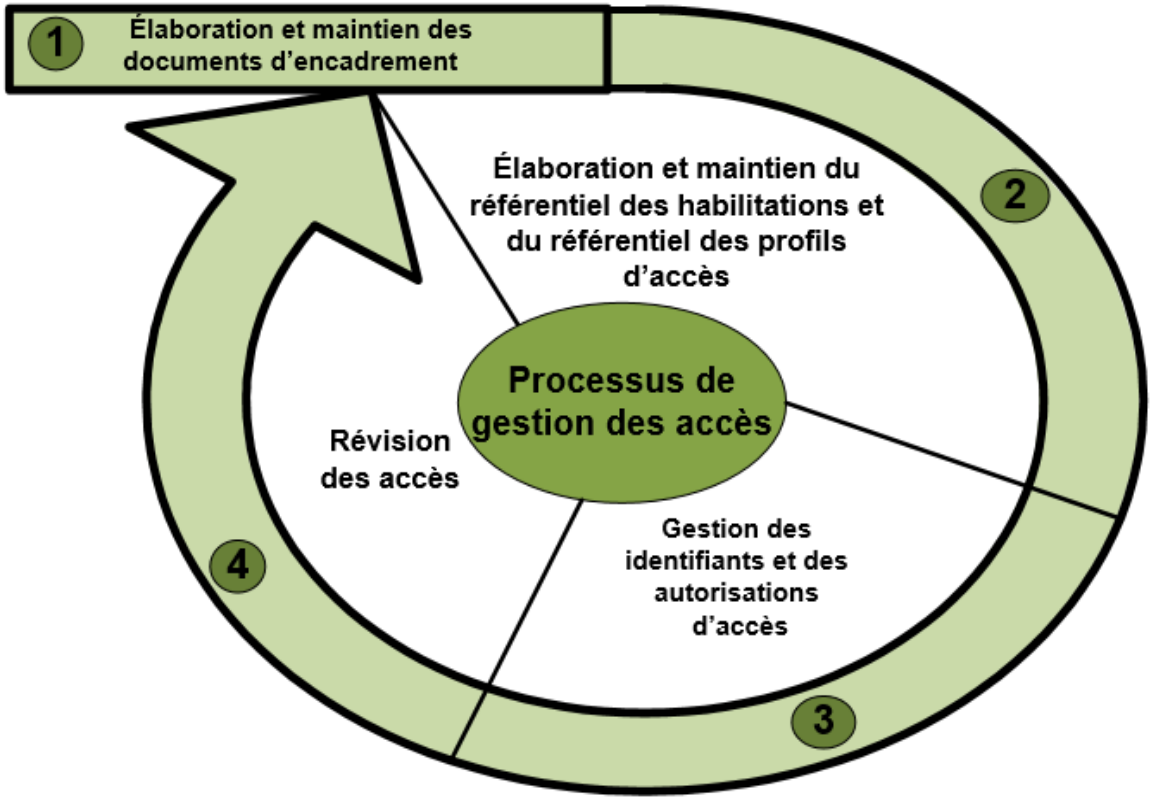
4. Processus de gestion des accès

La mise en place d'un processus de gestion des accès permet à l'organisme d'assurer l'équilibre entre la protection de l'information qu'il détient et l'octroi des accès et des privilèges aux utilisateurs[13] pour qu'ils puissent travailler efficacement.

Le processus de gestion des accès permet principalement de créer, d'identifier, d'enregistrer et de gérer l'identité des utilisateurs et les droits d'accès à l'information que détient l'organisme. Il permet de coordonner les tâches des différents intervenants afin de mettre en place les structures de contrôle nécessaires pour assurer la conformité aux exigences de sécurité en matière de gestion des accès.

Le processus de gestion des accès peut être représenté comme suit :

Figure 1: Étapes du processus de gestion des accès



13. **Utilisateurs :** dans le cadre de la gestion des accès, les utilisateurs ne se limitent pas forcément aux employés de l'organisme, mais ils peuvent inclure, entre autres, les fournisseurs, les stagiaires, les clients, les partenaires, les comptes administrateurs, les comptes de services, les comptes de machine, les comptes de lots.

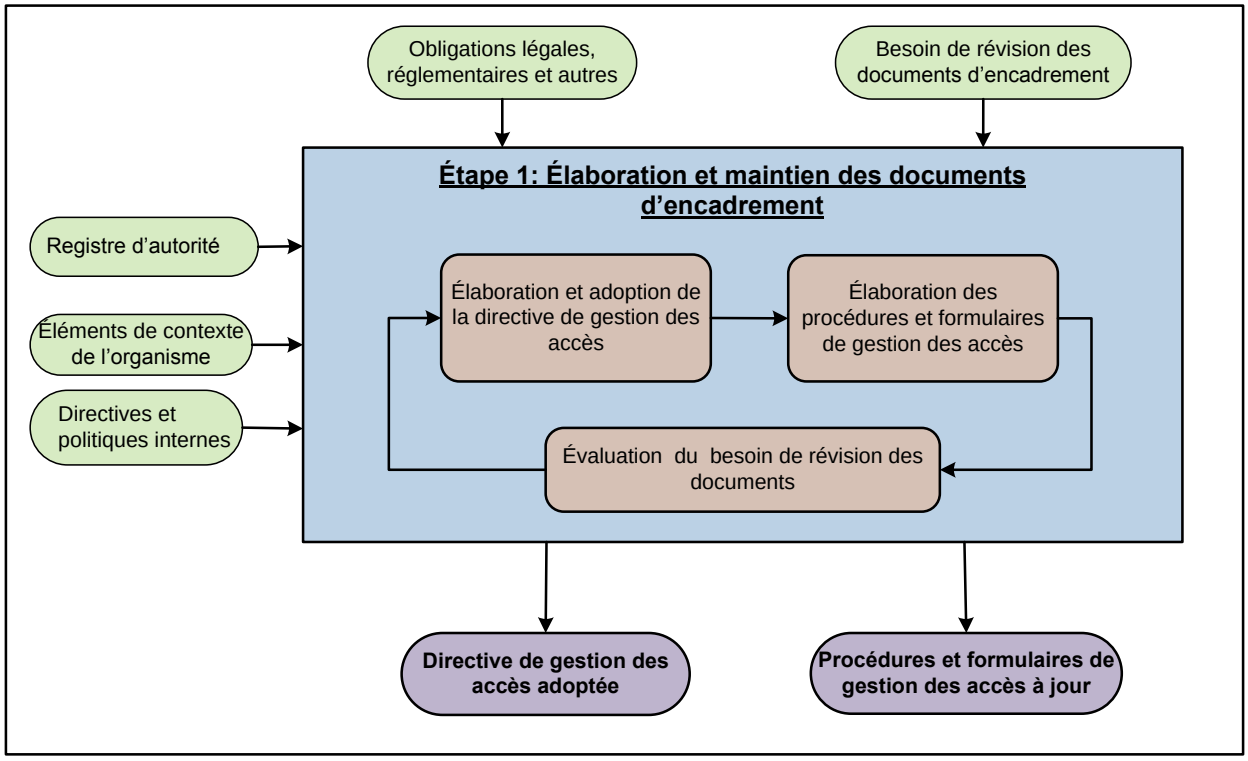
Comme illustré par la figure ci-dessus, le processus de gestion des accès comporte quatre étapes :

- ✓ élaboration et maintien des documents d'encadrement;
- ✓ élaboration et maintien du référentiel des habilitations et du référentiel des profils d'accès;
- ✓ gestion des identifiants et des autorisations d'accès;
- ✓ révision des accès.

4.1 Étape 1 : Élaboration et maintien des documents d'encadrement

Cette étape a pour objectif de s'assurer que tous les documents nécessaires à l'encadrement de la gestion des accès sont bien définis et à jour.

Figure 2: Étape 1 du processus de gestion des accès



Comme illustré ci-dessus, cette étape consiste en :

- ✓ l'élaboration d'une directive ou d'une politique qui précise les exigences de haut niveau et les dispositions à respecter par les principaux intervenants en matière de gestion des accès;

- ✓ l'élaboration des procédures décrivant les étapes à réaliser, les moyens à prendre et les méthodes à appliquer pour mettre en œuvre le processus de gestion des accès. Ces procédures peuvent nécessiter l'élaboration de formulaires tels que :
  - les formulaires de création, suspension, réactivation ou révocation d'un identifiant;
  - les formulaires d'attribution ou de modification des droits d'accès[14].
- ✓ l'évaluation périodique du besoin de révision de la directive, des procédures et formulaires de gestion des accès compte tenu de changements dans les éléments de contexte de l'organisme, tels qu'un changement de structure organisationnelle, un changement de loi, de règlement, etc.

La section 5 « Documents d'encadrement de la gestion des accès » apporte les précisions nécessaires sur l'élaboration de chacun de ces documents.

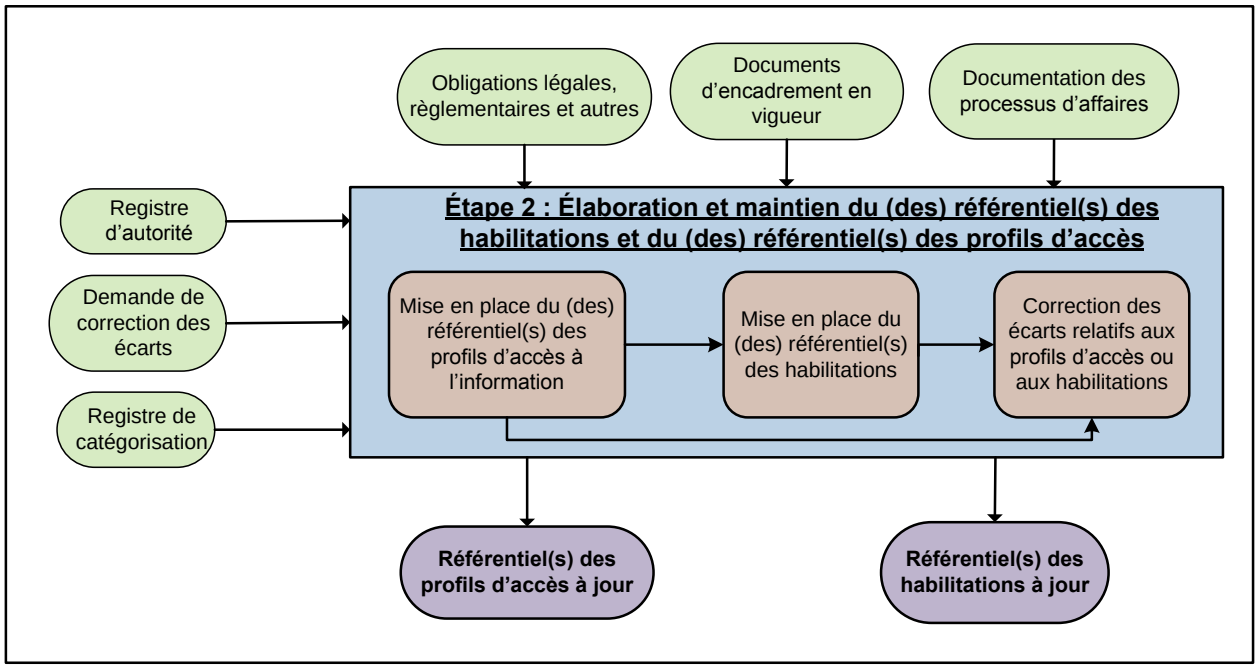
Il est également à noter qu'un exemple de directive de gestion des accès est présenté à l'annexe VI « Exemple de directive de gestion des accès logiques ».

Le responsable organisationnel de la sécurité de l'information (ROSI) et le conseiller organisationnel de la sécurité de l'information (COSI) sont les principaux intervenants à cette étape.

14. **À noter que,** p**our un organisme employant un grand nombre de ressources informationnelles**, la Direction des technologies de l'information peut élaborer un formulaire d'attribution ou de modification des droits d'accès par direction générale pour n'en inclure que les ressources sollicitées par cette direction.

4.2 Étape 2 : Élaboration et maintien du (des) référentiel(s) des habilitations et du (des) référentiel(s) des profils d'accès

Figure 3: Étape 2 du processus de gestion des accès



Comme illustré ci-dessus, les travaux réalisés à cette étape s'appuient sur les obligations légales et réglementaires, sur les documents d'encadrement en vigueur, sur la documentation des processus d'affaires et sur l'information consignée aux registres d'autorité[15] et de catégorisation[16].

Cette étape consiste en :

- ✓ la mise en place du (des) référentiel(s)[17] des profils d'accès à l'information;

15. **Registre d'autorité :** répertoire, recueil ou fichier dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information. Dans ce registre sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leurs sont assignés ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information. [*Guide d'élaboration d'un registre d'autorité de sécurité de l'information*, 2015]

16. **Registre de catégorisation :** répertoire dans lequel sont consignés les niveaux d'impacts, en termes de disponibilité, d'intégrité et de confidentialité, des actifs informationnels [*Guide de catégorisation de l'information*, 2014].

17. **Référentiel des profils d'accès à l'information :** répertoire dans lequel sont consignées les matrices de profils d'accès métiers de chaque application métier de l'organisme et les matrices de profils d'accès général de chaque direction générale.

- ✓ la mise en place du (des) référentiel(s)[18] des habilitations;
- ✓ la correction des écarts constatés relativement aux profils d'accès ou aux habilitations à la suite de la révision des accès.

4.2.1 Mise en place du (des) référentiel(s) des profils d'accès à l'information

Il revient à chaque organisme de décider, selon sa taille ou la diversité de ses plateformes technologiques, du nombre de référentiels des profils d'accès à l'information qui lui convient.

La mise en place du (des) référentiel(s) des profils d'accès à l'information permet à l'organisme de consigner, dans un (des) répertoire(s) commun(s), l'ensemble des profils d'accès à ses ressources (applications et autres). Cette mise en place nécessite :

- ✓ l'élaboration d'une matrice[19] de profils d'accès général[20] par entité administrative. Un exemple de matrice de profils d'accès général est présenté à l'annexe II « Exemple de matrice de profils d'accès général ».
- ✓ l'élaboration d'une matrice[21] de profils d'accès applicatifs[22] par système de mission. La définition de ces profils doit tenir compte du principe de séparation des tâches. Un exemple de matrice de profils d'accès applicatif est présenté à l'annexe III « Exemple de matrice de profils d'accès applicatif »

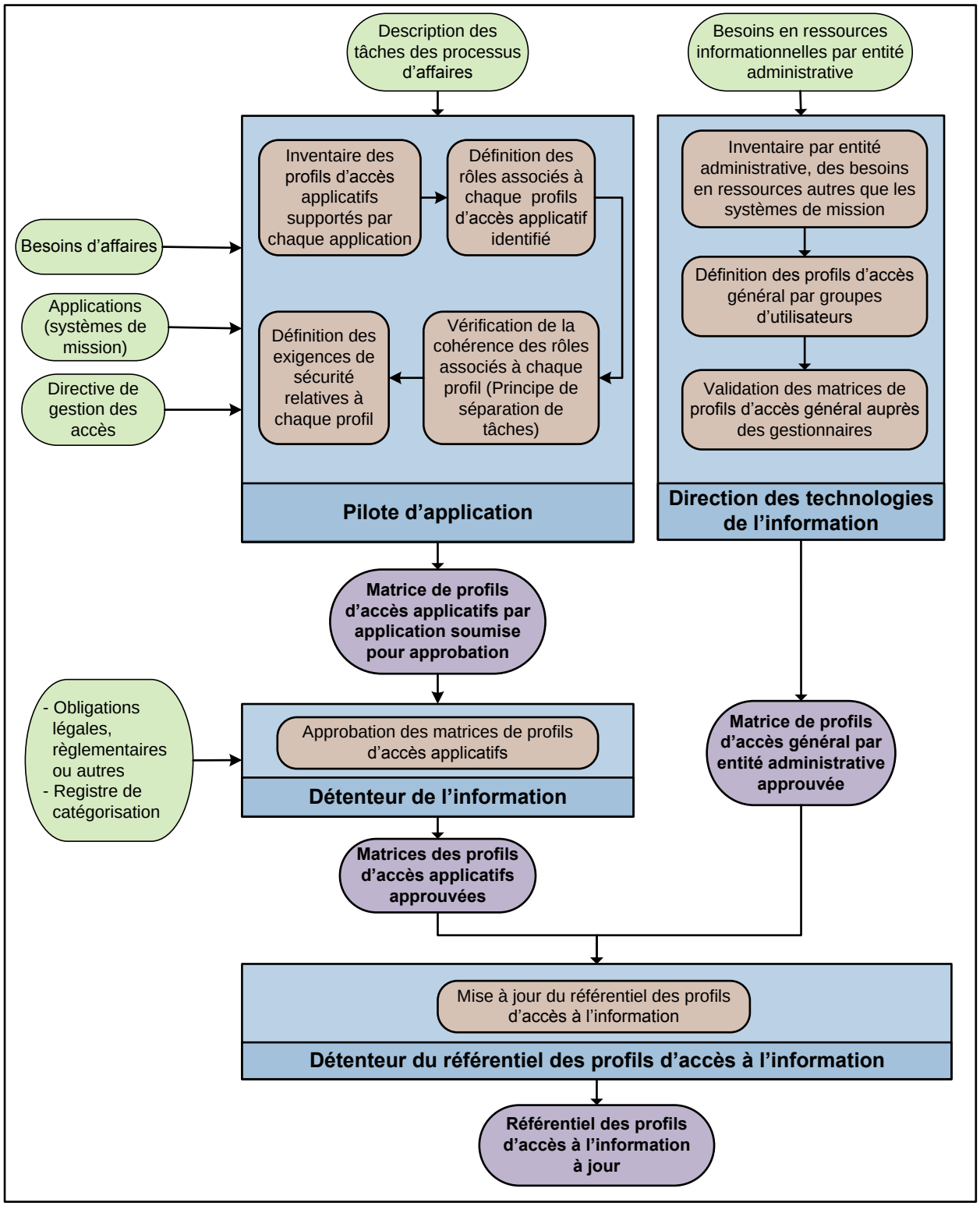
Ainsi, le (les) référentiel(s) de profils d'accès à l'information regroupe (ent) :

- ✓ les matrices de profils d'accès général élaborées par la direction des technologies de l'information;
- ✓ les matrices de profils d'accès applicatif élaborées par les détenteurs de l'information.

La figure ci-dessous illustre le détail de la mise en place du référentiel.

18. **Référentiel des habilitations :** répertoire dans lequel sont consignés pour chaque fonction organisationnelle les profils d'accès applicatifs et les profils d'accès général nécessaires pour accomplir les tâches associées à la fonction ainsi que les critères d'habilitation requis.
19. **Matrice de profils d'accès général :** grille associée à une entité administrative et contenant les profils d'accès général définis pour ses utilisateurs ou groupes d'utilisateurs.
20. **Profil d'accès général :** décrit les accès standards nécessaires pour un utilisateur ou un groupe d'utilisateurs aux ressources autres que les systèmes de mission. Il concerne les accès aux messageries, plateformes de collaboration, boîtes aux lettres de partage, listes de distribution, répertoires de données, serveurs, intranet, extranet, etc. [5]
21. **Matrice de profils d'accès applicatifs :** grille associée à un système de mission (application) et contenant les profils d'accès applicatif supportés par ce système ainsi que les exigences de sécurité correspondantes.
22. **Profil d'accès applicatif :** profil d'accès qui regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction sur un système de mission ou une application. [5]

Figure 4: Mise en place du référentiel des profils d'accès à l'information



Comme illustré par la figure 4, les principaux intervenants dans la mise en place du (des) référentiel(s) des profils d'accès à l'information sont les suivants.

1. **La direction des technologies de l'information :**
   - établit un inventaire des besoins en ressources informatiques pour chaque entité administrative. Ces ressources excluent les systèmes de mission et regroupent généralement les répertoires de données, la messagerie, les listes de distribution, les plateformes de collaboration, les boîtes aux lettres de partage, réseau privé virtuel (VPN), serveurs, Internet, etc.
   - recense les utilisateurs de chaque entité administrative et les répartit en groupes d'utilisateurs selon leurs besoins en ressources informatiques;
   - définit les profils d'accès général pour chaque groupe d'utilisateurs reconnu et en constitue une matrice par entité administrative;
   - fait valider la matrice des profils d'accès général de chaque entité administrative par les gestionnaires concernés;
   - transmet au détenteur du référentiel des profils d'accès à l'information les matrices de profils d'accès général approuvées.
2. **Le pilote d'application :**
   - établit l'inventaire des profils d'accès applicatifs supportés par chaque application (système de mission) relevant de sa responsabilité en tenant compte des besoins d'affaires et des descriptions de tâches des processus qu'elle soutient;
   - définit les rôles associés à chaque profil d'accès applicatif et s'assure de la cohérence de leur cohabitation en se basant sur le principe de la séparation des tâches;
   - définit les exigences de sécurité relatives à chaque profil d'accès applicatif en tenant compte du degré de sensibilité de l'information manipulée et des obligations légales, réglementaires et autres;
   - construit une matrice de profils d'accès applicatif pour chaque application relevant de sa responsabilité et la soumet à l'approbation du détenteur de l'information.
3. **Le détenteur de l'information :**
   - approuve les matrices de profils d'accès applicatif des systèmes relevant de sa responsabilité en tenant compte des exigences de sécurité consignées au registre de catégorisation et des obligations légales, réglementaires ou autres;
   - transmet au détenteur du référentiel des profils d'accès à l'information les matrices de profils d'accès applicatifs approuvées.
4. **Le détenteur du référentiel des profils d'accès à l'information :**
   - intègre les matrices de profils d'accès reçues des détenteurs de l'information et de la direction des technologies de l'information.

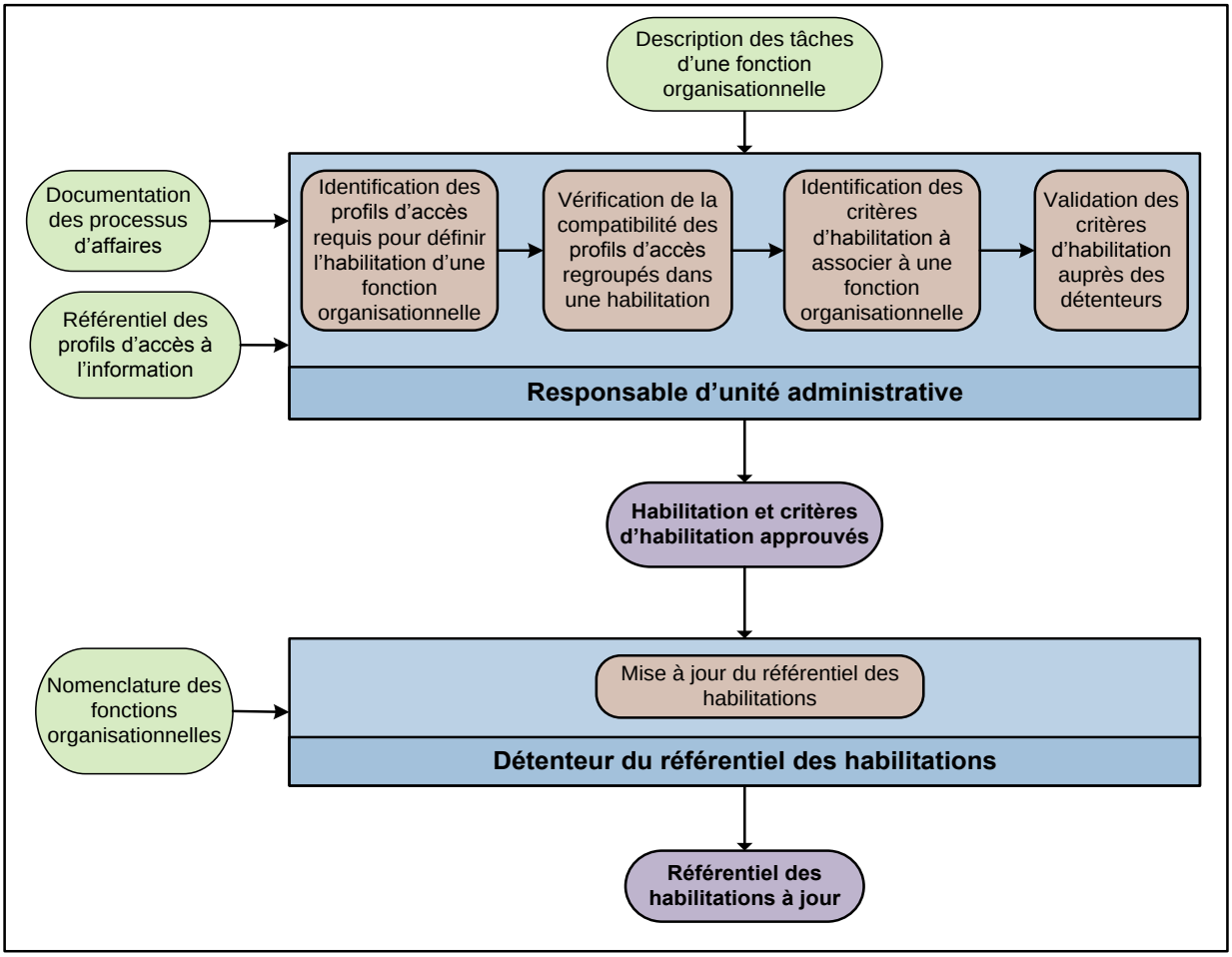
4.2.2 Mise en place du (des) référentiel(s) des habilitations

Le référentiel des habilitations permet aux responsables des unités administratives de définir, pour chaque fonction organisationnelle relevant de leur autorité, les accès nécessaires pour accomplir les tâches associées ainsi que les critères d'habilitation requis pour occuper la fonction.

Il revient à chaque organisme de décider, selon sa taille, du nombre de référentiels des habilitations qui lui convient.

Un exemple de référentiel des habilitations est présenté à l'annexe IV « Exemple de référentiel des habilitations ».La figure ci-dessous présente le détail de la mise en place du référentiel des habilitations.

Figure 5: Mise en place du référentiel des habilitations



Ainsi, sur la base de la description des tâches associées à une fonction organisationnelle et de la documentation des processus d'affaires, chaque responsable d'unité administrative :

- ✓ identifie dans le référentiel des profils d'accès à l'information les profils d'accès applicatifs et les profils d'accès général requis pour accomplir les tâches associées à la fonction et ainsi définir l'habilitation correspondante;
- ✓ s'assure que les profils regroupés dans une habilitation ne présentent pas d'incompatibilité compte tenu du principe de séparation des tâches. En cas d'incompatibilité, il en fait part au détenteur de l'information afin de remédier à la situation;
- ✓ identifie les critères d'habilitation requis par la fonction en tenant compte des exigences de sécurité relatives aux profils d'accès identifiés et des obligations légales et réglementaires régissant les tâches à accomplir;
- ✓ valide auprès des détenteurs de l'information les critères d'habilitation relatifs à la sécurité de l'information;
- ✓ approuve l'habilitation définie et les critères d'habilitation associés et les transmet au détenteur du référentiel des habilitations.

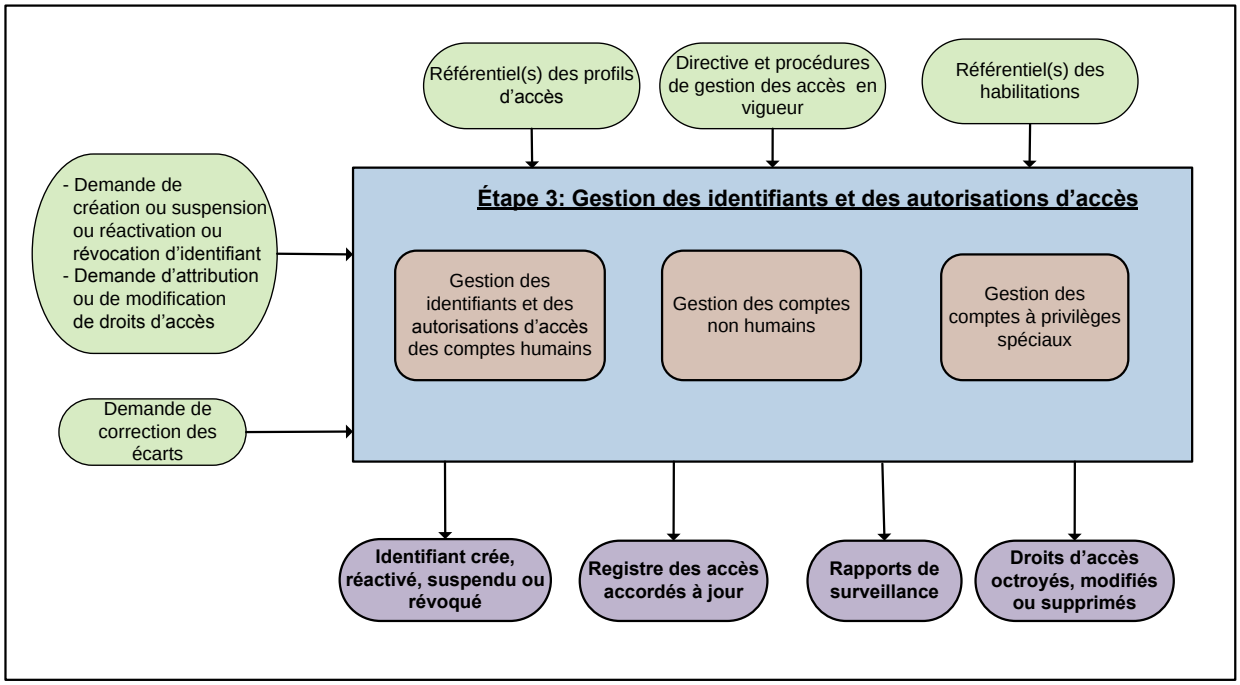
4.2.3 Correction des écarts relatifs aux profils d'accès ou aux habilitations

Après le constat des écarts lors de la révision des accès, étape 4 du processus de gestion des accès présentée à la section 4.4, la correction de ces écarts consiste en :

- ✓ les responsables d'unités administratives vérifient la description de tâches des fonctions organisationnelles sous leur autorité et font les ajustements nécessaires à la définition des habilitations non conformes. Ils transmettent les habilitations modifiées au détenteur du référentiel des habilitations pour mise à jour;
- ✓ les détenteurs de l'information vérifient les matrices de profils d'accès applicatifs associées aux systèmes de mission sous leur responsabilité et s'assurent qu'elles sont conformes aux versions actuelles des systèmes. Ils transmettent les matrices de profils d'accès ajustées au détenteur du référentiel des profils d'accès à l'information pour mise à jour.

4.3 Étape 3 : Gestion des identifiants et des autorisations d'accès

Figure 6: Étape 3 du processus de gestion des accès



- ✓ Tels qu'illustré à la figure ci-dessus, l'étape de gestion des identifiants et des autorisations d'accès prend appui sur la directive de gestion des accès et les procédures afférentes, le (les) référentiel(s) des habilitations et le (les) référentiel(s) des profils d'accès à l'information. Elle couvre :
  - la gestion des identifiants et des autorisations d'accès des comptes humains, qui consiste à :
  - créer, modifier, enregistrer et résilier les identifiants associés à chaque compte humain, à la demande du gestionnaire;
  - octroyer, modifier, supprimer les accès autorisés à chaque identifiant, à la demande du gestionnaire;
  - vérifier si une demande d'octroi d'autorisation d'accès n'engendre pas un conflit de séparation des tâches;
  - s'assurer auprès du gestionnaire qu'une demande d'autorisation d'accès est justifiée lorsqu'elle n'est pas conforme au référentiel des habilitations;

- mettre à jour le registre[23] des accès accordés. Un exemple de registre des accès accordés est présenté à l'annexe V : « Exemple de registre des accès accordés »;
- surveiller les tentatives d'accès à des fonctions non autorisées et les accès à l'information sensible ou critique et informer le détenteur de l'information de toute activité anormale.

✓ **la gestion des comptes non humains,** appelés également comptes fonctionnels. Ces comptes ne servent pas à l'authentification d'un utilisateur particulier, mais à la communication entre deux composantes du système – par exemple, pour fonctionner, les systèmes de gestion de bases de données (SGBD) exigent la création et l'activation de comptes propres au système qui les héberge. La gestion de ces comptes consiste à :

- appliquer rigoureusement la procédure de leur création;
- s'assurer que les droits d'accès accordés à ces comptes sont basés sur le principe du privilège minimal, en tout temps;
- mettre à jour le registre des accès accordés;
- contrôler rigoureusement les accès aux authentifiants de ces comptes;
- révoquer ces comptes quand ils ne sont plus utiles;
- assurer la traçabilité de tout accès ou tentative d'accès de ces comptes;
- surveiller les activités de ces comptes et informer le détenteur de l'information de toute activité anormale.

✓ **la gestion des comptes à privilèges spéciaux,** qui consiste à :

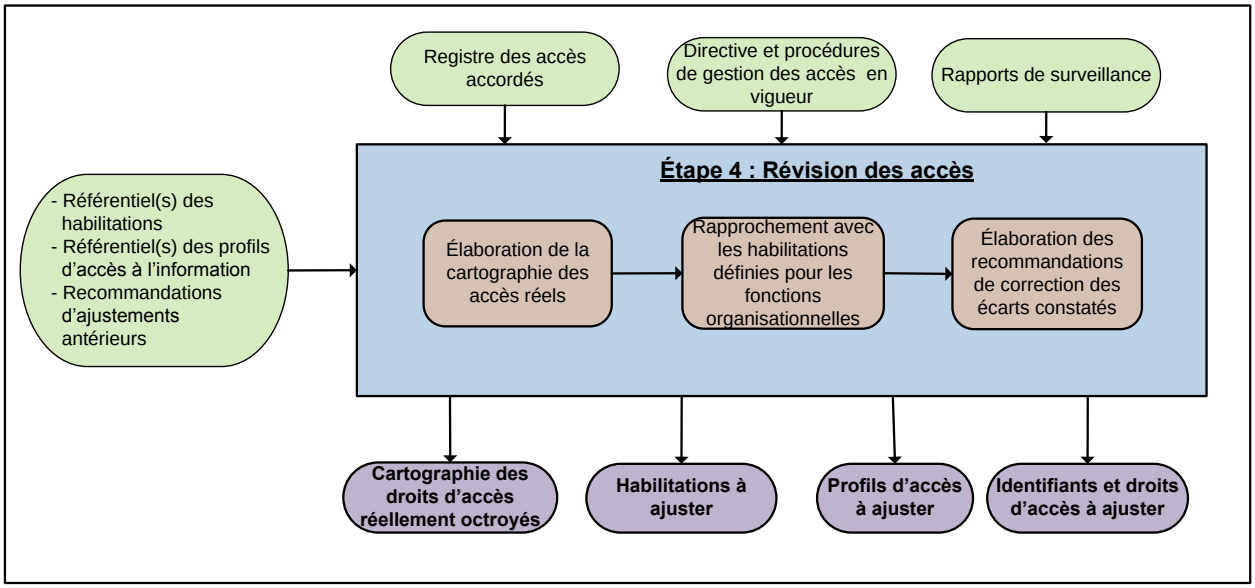
- appliquer rigoureusement la procédure de leur création;
- s'assurer que les droits d'accès accordés à ces comptes sont basés sur le principe du privilège minimal en tout temps;
- mettre à jour le registre des accès accordés;
- empêcher toute utilisation non justifiée ou inappropriée de ces comptes;
- vérifier la liste des utilisateurs bénéficiant d'un accès privilégié;
- surveiller les activités des comptes à privilèges spéciaux et informer le détenteur de l'information de toute activité anormale;
- vérifier les opérations en ligne des comptes à privilèges spéciaux pour détecter toute transmission non justifiée de données sensibles ou l'introduction inappropriée d'applications non approuvées;
- assurer la traçabilité de tout accès ou tentative d'accès de ces comptes.

23. **Registre des accès accordés :** répertoire dans lequel sont consignées toutes les permissions d'accès accordées à un compte.

4.4 Étape 4 : Révision des accès

Cette étape est à réaliser au moins une fois par an pour l'ensemble des comptes, et plus souvent pour les accès aux ressources stratégiques et les comptes à haut risque. Les tâches couvertes par cette étape sont généralement supportées par des outils logiciels et elles sont réalisées en étroite collaboration entre la direction des technologies de l'information, les détenteurs de l'information et les responsables d'unités administratives.

Figure 7: Étape 4 du processus de gestion des accès



Comme l'illustre la figure ci-dessus, l'étape de révision des accès consiste à élaborer une cartographie (inventaire) des utilisateurs avec leurs accès réels aux ressources et à effectuer un rapprochement entre les habilitations définies pour les fonctions organisationnelles et les accès réels des personnes qui les occupent afin de repérer tous les écarts. Ainsi, elle permet :

- ✓ de détecter les comptes orphelins;
- ✓ de détecter les comptes avec droits d'accès excessifs;
- ✓ de repérer les problèmes d'incompatibilité dans les droits d'accès compte tenu du principe de la séparation des tâches;
- ✓ de procéder à une analyse croisée entre les personnes, leurs droits d'accès, leurs mandats et les accès effectués. Ainsi, l'analyse croisée répond aux questions suivantes :
  - les droits d'accès réellement attribués correspondent-ils aux droits d'accès approuvés pour chacun des identifiants utilisateurs?
  - les identifiants utilisateurs et les droits d'accès associés sont-ils en décalage par rapport aux droits d'accès requis par l'utilisateur pour accomplir ses tâches?
  - les identifiants utilisateurs exploitent-ils toutes les fonctions qui leur ont été accordées par l'habilitation associée à l'identifiant?

- ✓ de faire un rapprochement entre les habilitations et les droits d'accès réellement accordés aux utilisateurs et aux comptes non humains afin de détecter :
  - les identifiants possédant des droits d'accès correspondant à ceux approuvés;
  - les identifiants possédant des droits d'accès qui ne correspondent pas à ceux approuvés;
  - les identifiants dont les droits d'accès ne sont pas vérifiés et approuvés à la fréquence prévue;
  - les identifiants associés à des utilisateurs, qui ont été révoqués ou désactivés;
  - les utilisateurs possédant des identifiants et des droits d'accès et qui n'ont fait l'objet d'aucune demande d'accès ou d'approbation.
- ✓ d'élaborer les rapports de recommandations pour remédier aux écarts constatés.

Ces recommandations peuvent être traitées comme suit :

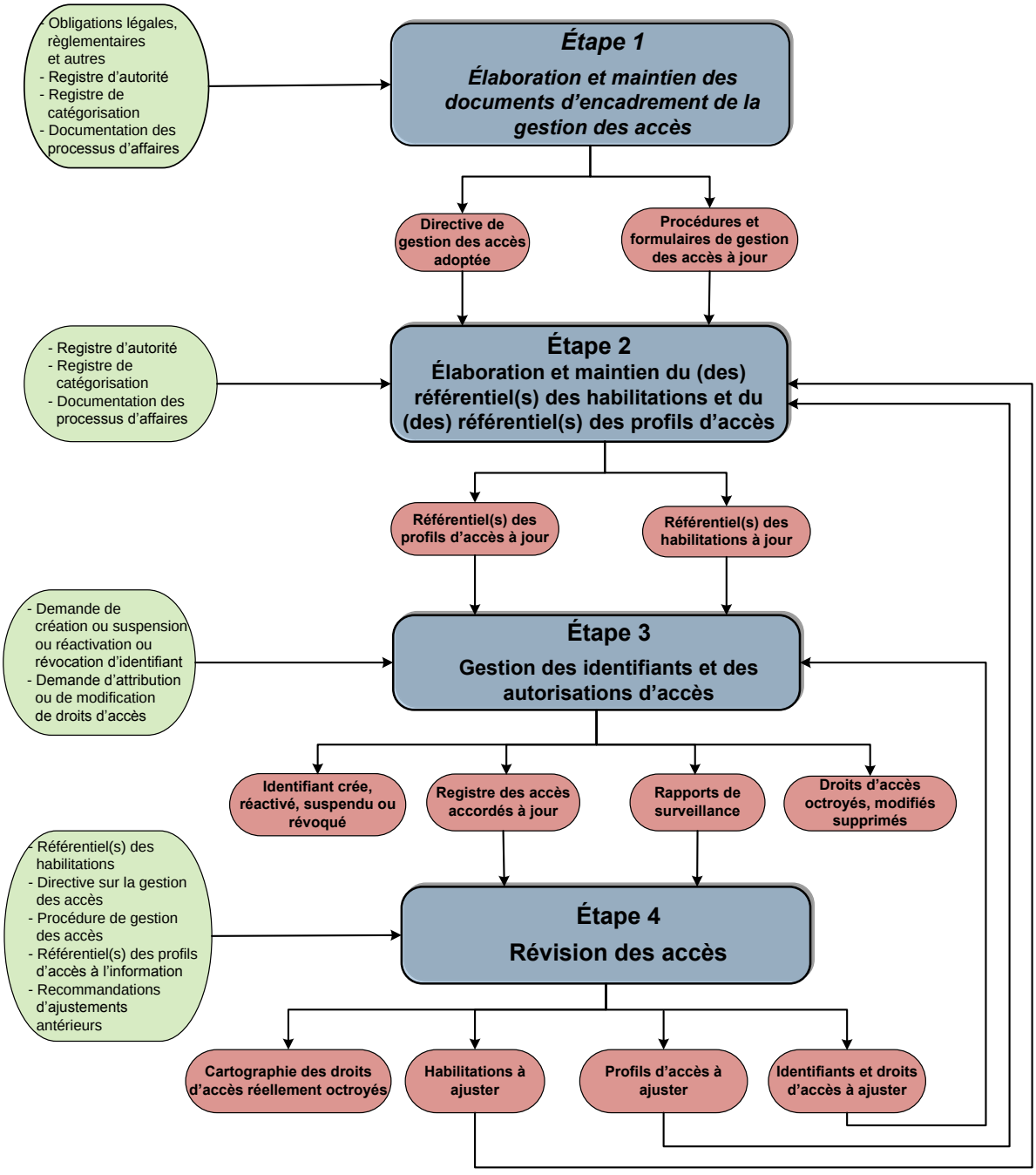
- ✓ les responsables d'unités administratives font des demandes d'ajustement des accès autorisés de leurs employés ou mettent à jour les définitions des habilitations non conformes;
- ✓ les détenteurs de l'information vérifient les accès octroyés aux utilisateurs de leurs applications pour s'assurer que les profils d'accès applicatif définis répondent correctement aux habilitations associées. De plus, ils révoquent tous les droits d'accès injustifiés;
- ✓ le responsable des technologies de l'information vérifie et valide les accès accordés aux comptes non humains et aux comptes à privilèges spéciaux et procède aux mises à jour requises.

La révision des accès permet de remédier aux situations suivantes :

- ✓ des utilisateurs qui cumulent des habilitations à mesure qu'ils changent de fonction au sein de l'organisme et ceux qui se voient attribuer des habilitations injustifiées;
- ✓ des oublis de modification des droits d'accès à la suite d'un mouvement du personnel;
- ✓ des changements fréquents dans les responsabilités d'un même employé;
- ✓ des oublis de mise à jour des matrices de profils d'accès applicatif suite à des modifications apportées aux systèmes de mission;
- ✓ des oublis de mise à jour des habilitations et des critères d'habilitation suite à des changements de structure organisationnelle ou dans la description de tâches des processus d'affaires.

Une vue globale de l'ensemble des étapes du processus de gestion des accès est illustrée par la figure suivante.

Figure 8: Vue synthèse du processus de gestion des accès



La mise en place de certaines bonnes pratiques de gestion des accès, voir section 6 « Pratiques associées à la gestion des accès », peut être un prélude à la mise en place d'un processus formel de gestion des accès.

5. Documents d'encadrement de la gestion des accès

La gestion des accès est généralement encadrée par :

- ✓ une directive de gestion des accès logiques;
- ✓ des procédures de mise en œuvre des différents volets de la gestion des accès.

5.1 Directive de gestion des accès logiques

La directive de gestion des accès est élaborée par le responsable organisationnel de la sécurité de l'information (ROSI) en collaboration avec d'autres intervenants en sécurité de l'information. Elle est soumise à la validation du comité chargé de la sécurité de l'information et à l'approbation du sous-ministre ou du dirigeant de l'organisme.

L'adoption de la directive par la haute direction témoigne de l'importance accordée à la protection de l'information que détient l'organisme et démontre son engagement à assurer une gestion des accès adéquate à son patrimoine informationnel.

D'application obligatoire, la directive de gestion des accès précise les exigences de haut niveau et les dispositions à respecter par les principaux intervenants pour assurer la sécurité des accès à l'information de l'organisme. Elle précise également les sanctions prévues en cas de non-respect des dispositions de la directive.

Lors de l'élaboration de la directive de gestion des accès, il convient de tenir compte :

- ✓ des exigences en matière de sécurité pour chaque système de mission;
- ✓ des risques auxquels sont exposés les systèmes de mission, et particulièrement les systèmes stratégiques;
- ✓ de la législation et des obligations contractuelles en matière de protection de l'accès aux données ou aux services;
- ✓ des exigences de l'organisme en matière d'exploitation et de sécurité de l'information;
- ✓ des politiques de diffusion de l'information et d'autorisation des accès;
- ✓ des exigences relatives à la fréquence de révision des contrôles d'accès;
- ✓ des situations nécessitant une approbation particulière.

La mise en œuvre de la directive de gestion des accès est appuyée par des procédures formelles décrivant les étapes à réaliser, les moyens à employer et les méthodes à suivre pour atteindre les objectifs visés.

Il est important d'organiser, à l'intention de l'ensemble des intervenants, des séances de formation et de sensibilisation afin de s'assurer d'une bonne compréhension des énoncés de la directive.

La directive de gestion des accès est diffusée auprès de l'ensemble des employés et des tiers concernés.

Par ailleurs, la directive de gestion des accès est à réexaminer suite à des changements juridiques, organisationnels ou technologiques majeurs.
Un exemple de directive de gestion des accès est présenté à l'Annexe VI.

5.2 Procédures

Afin de bien documenter le processus de gestion des accès, il est important d'élaborer plusieurs procédures, principalement :

- ✓ la procédure d'élaboration et de maintien du référentiel des habilitations;
- ✓ la procédure d'élaboration et de maintien du référentiel des profils d'accès à l'information;
- ✓ la procédure de gestion des identifiants et des autorisations d'accès.

Les sections suivantes présentent des éléments de contenu pour chacune des procédures citées. Il appartient à chaque organisme de les adapter à sa propre réalité organisationnelle et technologique. De plus, il est important de réviser périodiquement ces procédures pour tenir compte d'éventuels changements au sein de l'organisme – structure organisationnelle, activités, lois et règlements.

5.2.1 Procédure d'élaboration et de maintien du (des) référentiel(s) des habilitations

Cette procédure permet de répondre aux questions suivantes :

- ✓ Qui intervient dans la définition et la validation des habilitations et des critères d'habilitation à associer à chaque fonction organisationnelle?
- ✓ Quelles sont les règles à respecter lors de la définition et de la validation de ces habilitations?
- ✓ Quelles sont les conditions qui déclenchent la révision des habilitations et des critères d'habilitation? Et comment assurer cette révision?
- ✓ Est-ce que l'organisme désigne un (des) détenteur(s) du (des) référentiel(s) des habilitations et quelles sont ses (leur) tâches? Si non, comment est assurée la mise à jour de l'information relative aux habilitations?
- ✓ Est-ce que l'organisme a besoin de mettre en place un seul ou plusieurs référentiels des habilitations?

5.2.2 Procédure d'élaboration et de maintien du (des) référentiel(s) des profils d'accès à l'information

Cette procédure permet de répondre aux questions suivantes :

- ✓ Quelles sont les règles à respecter lors de la définition des profils d'accès?
- ✓ Qui intervient dans la définition des profils d'accès applicatif de chacun des systèmes de mission de l'organisme, et comment?

- ✓ Quelles sont les conditions qui déclenchent la révision des profils d'accès applicatif? Et comment assurer cette révision?
- ✓ Qui intervient dans la définition des profils d'accès général?
- ✓ Quelle est l'approche préconisée par l'organisme pour définir les profils d'accès général?
- ✓ Quelles sont les conditions qui déclenchent la révision des profils d'accès général? Et comment assurer cette révision?
- ✓ Est-ce que l'organisme désigne un (des) détenteur(s) du (des) référentiel(s) des profils d'accès à l'information, et quelles sont ses (leur) tâches? Si non, comment est assurée la mise à jour de l'information relative aux profils d'accès?

5.2.3 Procédure de gestion des identifiants et des autorisations d'accès

Cette procédure permet de garantir que les demandes relatives aux droits d'accès sont transmises aux bonnes personnes pour approbation et traitement. Elle permet également de réduire les délais de traitement afférents.

Cette procédure spécifie généralement :

- ✓ Pour les demandes de création, suppression ou modification d'un identifiant :
  - Comment sont formulées les demandes (manuelles, électroniques ou par téléphone)?
  - Où doivent être transférées les demandes?
  - Quels sont les délais à respecter pour déposer une demande?
  - Quels sont les renseignements à fournir dans la demande ou quel est le formulaire à remplir selon les droits d'accès à traiter?
  - Qui approuve la demande?
  - Quels sont les critères d'approbation pour chaque type de demande? Ces critères peuvent être différents d'une application ou d'un système à l'autre.
- ✓ Pour la gestion des mots de passe utilisateur :
  - les règles d'attribution des identifiants et mots de passe initiaux;
  - les règles de communication des mots de passe aux utilisateurs;
  - les règles de réinitialisation des mots de passe pour les utilisateurs bloqués;
  - les règles de vérification des opérations sur les mots de passe;
  - les règles de recherche de mots de passe faciles à deviner et qui pourraient être à l'origine d'incidents en sécurité de l'information.
- ✓ Pour la conservation et le traitement des données relatives aux demandes d'accès :
  - Quelles sont les données à conserver selon les types de compte (comptes à privilèges spéciaux, autres comptes) : les accès accordés, les approbations, les dates de début et dates de fin?
  - Quelle est la période de conservation?

- Quelles sont les exigences réglementaires de conservation?
- Quel est l'emplacement des données conservées?
- Comment sont conservées les identités désactivées, mises hors service et supprimées?

6. Pratiques associées à la gestion des accès

La gestion des accès est encadrée par un ensemble de pratiques regroupées selon les volets suivants :

- ✓ Gestion d'accès utilisateur;
- ✓ Gestion des privilèges;
- ✓ Contrôle d'accès au réseau;
- ✓ Contrôle d'accès aux systèmes d'exploitation;
- ✓ Contrôle d'accès aux applications et à l'information;
- ✓ Accès des dispositifs mobiles;
- ✓ Télétravail.

6.1 Gestion d'accès utilisateur

Pratique	Description
P1	Mettre en place une procédure formelle d'enregistrement des utilisateurs, qui définit minimalement les tâches suivantes : • les autorisations d'accès requises compte tenu de la sensibilité de l'information; • l'attribution sécuritaire et contrôlée des codes utilisateurs et mots de passe initiaux; • la mise à jour ou le retrait des accès lorsque nécessaire – p. ex. départ, mutation, promotion, etc.
P2	Définir les accès de tout utilisateur sur la base des habilitations associées à la fonction organisationnelle qu'il occupe et des règles d'identification et d'authentification en vigueur.
P3	Établir les règles de gestion des mots de passe (p. ex. choix, modification, initialisation, etc.) et les diffuser auprès de l'ensemble des utilisateurs. Ces règles doivent être applicables à l'ensemble des comptes, y compris les comptes à privilèges spéciaux.
P4	S'assurer que toute attribution d'accès à des données stratégiques est précédée d'un engagement formel de l'utilisateur relativement au respect des règles de protection des moyens d'accès fournis et au devoir de signalement en cas de divulgation non autorisée.
P5	S'assurer que l'accès aux postes de travail et aux applications est fait à l'aide de comptes utilisateurs nominatifs et non génériques.

P6	Ne pas permettre aux utilisateurs d'avoir accès à leur poste de travail en tant qu'administrateur (avoir le droit d'installer des outils). Toute exception doit être documentée et approuvée.
P7	Appliquer une période d'inactivité acceptable, après ouverture d'une session, à tous les comptes utilisateurs, y compris les comptes à privilèges spéciaux.
P8	Mettre en œuvre des mesures appropriées pour limiter le nombre de tentatives d'accès infructueuses. Une fois le nombre de tentatives atteint, le code utilisateur est désactivé.
P9	Réviser les droits d'accès d'un utilisateur après son départ, son transfert, sa mutation ou tout autre changement relatif à ses tâches et ses fonctions.
P10	Réviser périodiquement les accès attribués.
P11	Répertorier les droits d'accès, leurs modifications et leurs violations.
P12	Informer l'utilisateur : • de la mise en place des journaux d'activités permettant de détecter et de retracer toute activité et tout accès non autorisé; • qu'en l'absence de moyens sécurisés sur son poste de travail, il doit s'abstenir de transmettre des données sensibles vers ou depuis l'extérieur de l'organisme; • des sanctions auxquelles il s'expose en cas de non-respect des dispositions réglementaires mises en place en matière de gestion des accès.
P13	Sensibiliser l'utilisateur : • à l'importance de choisir un mot de passe sécuritaire, selon les bonnes pratiques en la matière, et de le garder secret en tout temps; • à l'importance de verrouiller son poste de travail lorsqu'il s'absente de son bureau; • aux contraintes légales et aux moyens de sécurisation de l'information à laquelle il accède; • à l'obligation de signaler, sans délai, toute atteinte à la sécurité de l'information à laquelle il accède.

6.2 Gestion des comptes à privilèges spéciaux

Pratique	Description
P14	Encadrer et contrôler rigoureusement l'octroi et l'utilisation des privilèges d'accès. Ainsi : • les types d'accès privilège sont identifiés et documentés pour chacune des composantes – applications, bases de données, systèmes d'exploitation, composants informatiques, documents, etc.; • les privilèges spéciaux sont octroyés sur la base du principe du « privilège minimal », c'est-à-dire le minimum requis pour effectuer les tâches associées à la fonction de l'utilisateur; • les privilèges de haut niveau sont accordés au moyen d'un compte utilisateur distinct de celui employé dans le cadre des opérations ordinaires; • les motifs d'attribution des privilèges d'accès de haut niveau doivent rester valides durant toute la période de leur attribution; • un compte unique et nominatif est requis pour chaque accès octroyé. Les comptes génériques[24] sont à éviter, à moins d'en justifier techniquement l'utilisation. Cette précaution permet de responsabiliser les propriétaires des comptes privilèges à l'égard des actions effectuées; • une procédure formelle de révision des privilèges est mise en place afin d'en assurer le maintien ou la révocation; • les comptes privilèges sont plus fréquemment révisés que les comptes ordinaires; • des mécanismes de surveillance (p. ex : système d'alerte) sont mis en place pour contrôler les activités réalisées par les comptes à haut risque.
P15	Établir les règles de gestion des mots de passe pour les administrateurs des réseaux, les administrateurs des systèmes d'exploitation et les administrateurs des applications.
P16	S'assurer que l'accès en tant qu'administrateur réseau, administrateur système ou administrateur d'application est fait au moyen d'un compte utilisateur nominatif et non générique afin de retracer les auteurs des actions effectuées et responsabiliser les intervenants.
P17	S'assurer que les postes de travail des administrateurs des réseaux, des administrateurs des systèmes ou des administrateurs d'applications se verrouillent automatiquement au-delà d'une période d'inactivité prédéterminée. Cette précaution permet de restreindre les risques d'une utilisation frauduleuse des privilèges de l'administrateur.

24. **Compte générique** : compte anonyme n'appartenant pas à une personne en particulier. Il peut être employé par plusieurs utilisateurs (exemples : « compta1 », « compta2 »).

6.3 Contrôle d'accès au réseau

Pratique	Description
P18	Identifier et authentifier toute personne qui accède au réseau informatique de l'organisme.
P19	Mettre en place les mesures de contrôle appropriées pour repérer tout équipement se connectant au réseau informatique de l'organisme – système de prévention des intrusions, système de détection des intrusions.
P20	Mettre en place des mesures d'isolement de tout équipement non autorisé qui tente d'accéder au réseau de l'organisme.
P21	Protéger à l'aide de coupe-feu les serveurs accessibles par Internet.
P22	Diviser le réseau de l'organisme en zones dont le niveau de sécurité est fonction du degré de sensibilité de l'information et de la criticité des applications.
P23	Utiliser des coupe-feu entre les différentes zones du réseau informatique de l'organisme afin de diminuer les risques d'intrusion et d'accès non autorisé.
P24	S'assurer que seuls les ports réseaux nécessaires sont ouverts et disponibles. Une vérification des ports ouverts est effectuée périodiquement.

6.4 Contrôle d'accès aux systèmes d'exploitation

Pratique	Description
P25	Identifier et authentifier tout administrateur accédant à un système d'exploitation. Un code unique est attribué à chaque administrateur.
P26	Mettre en œuvre les mesures appropriées pour limiter le nombre de tentatives d'accès infructueuses. Une fois le nombre de tentatives atteint, le code administrateur est désactivé.
P27	Journaliser les accès et tentatives d'accès aux systèmes d'exploitation et appliquer les règles de conservation afférentes.
P28	S'assurer que des règles de gestion de mot de passe pour les comptes administrateurs du système sont adoptées par l'organisme.
P29	S'assurer que l'accès au système d'exploitation est fait au moyen de comptes nominatifs et non génériques afin de retracer, éventuellement, les auteurs des actions effectuées et ainsi responsabiliser les intervenants.

6.5 Contrôle d'accès aux applications et à l'information

Pratique	Description
P30	S'assurer que le détenteur de l'information autorise les accès à l'information dont il est responsable.
P31	Octroyer les accès à l'information selon le principe du « privilège minimal », c'est-à-dire le minimum requis pour accomplir les tâches associées au rôle de l'utilisateur.
P32	Établir et appliquer les exigences concernant les connexions à distance aux applications.
P33	Journaliser et conserver les accès et tentatives d'accès aux applications sensibles, de manière facilement exploitable, afin d'identifier les actions effectuées et leurs auteurs.
P34	Ne confier la maintenance de toute application qu'à un personnel dûment habilité et autorisé.
P35	Contrôler l'usage des ports USB des postes de travail accédant à des applications sensibles – p. ex. : interdiction de copie de l'ensemble des données contenues dans un fichier.
P36	Vérifier périodiquement les droits d'accès et les profils d'accès applicatifs pour s'assurer de l'adéquation des droits d'accès attribués aux fonctions réellement occupées par chaque utilisateur.
P37	Intégrer aux ententes et contrats des clauses permettant d'encadrer les interventions des sous-traitants sur les applications en vue de garantir la sécurité des données.
P38	Mettre en place des moyens sécurisés dans un environnement contrôlé et restreint pour tout accès aux applications ou processus d'exploitation traitant de l'information sensible.

6.6 Accès des dispositifs mobiles

Pratique	Description
P39	Établir les restrictions d'utilisation et la directive de mise en œuvre des dispositifs mobiles.
P40	S'assurer que les réseaux sans fil sont sécurisés en raison du risque d'interception de l'information qui y circule – (p. ex. : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc.
P41	S'assurer que les accès distants aux systèmes d'information par des dispositifs mobiles font préalablement l'objet d'une authentification de l'utilisateur et du dispositif.
P42	Désactiver les fonctions des systèmes d'information qui permettent l'exécution automatique du code sur les dispositifs mobiles sans l'autorisation de l'utilisateur.
P43	Mettre en place des mesures de sécurité robustes (p. ex. : authentification à deux facteurs, chiffrement, etc.) pour les accès par Internet aux outils d'administration système ou réseau.
P44	Limiter le nombre de tentatives d'accès (p. ex. : verrouillage automatique du dispositif mobile après un nombre prédéterminé de tentatives d'accès infructueuses) et mettre en place une procédure[25] de retour à la normale après verrouillage.
P45	Envisager l'utilisation de mécanismes d'authentification forte pour les accès à l'information sensible.
P46	Rendre obligatoire l'utilisation d'un code pour le déverrouillage du dispositif mobile.
P47	Sensibiliser les utilisateurs de dispositifs mobiles aux risques de sécurité de l'information à laquelle ils ont accès et les former à l'utilisation des bonnes pratiques en la matière.

25. **Une procédure de retour à la normale après verrouillage** permet à l'utilisateur de déverrouiller son appareil, après validation de son identité.

6.7 Télétravail

Dans le cas où l'organisme autorise le télétravail, les pratiques suivantes sont à appliquer :

Pratique	Description
P48	Ne permettre le télétravail[26] qu'aux utilisateurs bénéficiant d'une autorisation administrative formelle spécifiant les permissions d'accès à distance qui leur sont accordées.
P49	S'assurer que l'accès à distance aux activités d'administrateur est préalablement autorisé et s'effectue à partir de consoles de gestion spécialisées qui requièrent une authentification robuste.
P50	Sensibiliser les utilisateurs effectuant du télétravail aux risques de sécurité de l'information à laquelle ils ont accès et à leurs responsabilités à cet égard.
P51	S'assurer que les règles d'autorisation et de restriction des accès à distance sont clairement définies et approuvées par les détenteurs de l'information.
P52	Mettre en place des mécanismes automatisés de surveillance des accès et de détection du non-respect de l'application des méthodes d'accès à distance établies.
P53	Mettre en place des mécanismes de vérification pour s'assurer que tous les employés effectuant du télétravail protègent l'information utilisée, conformément aux exigences de sécurité établies par l'organisme.

26. Télétravail : activité professionnelle qui s'exerce en dehors des bureaux de l'employeur et pour laquelle on fait appel aux technologies de l'information et de la communication pour communiquer à distance. [OQLF, 2008]

Références

[1] AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, RÉPUBLIQUE FRANÇAISE, *Maîtriser les risques de l'infogérance : externalisation des systèmes d'information*, 2010, [En ligne], http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf.

[2] BRAINWAVE, *Reprenez le contrôle de vos identités*, Brainwave Identity GRC, Gouvernance des habilitations, 2014.

[3] CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA, CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION, « La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie », *Catalogue des contrôles de sécurité*, ITSG-33_annexe 3, 2012.

[4] *CISSP All-in-One Exam guide*, 5th Edition, Shon Harris, Chapter 4 « Access control », 2010.

[5] CLUSIF, GROUPE DE GESTION DES IDENTITÉS, *Gestion des identités*, 2007, [En ligne], https://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-Gestion-des-identites.pdf.

[6] CLUSIR, Guillaume Garbey, Gilles MORIEUX, Ismaël CISSE et Victor JOATTON, *La gestion des identités et des accès*, 2009, [En ligne], http://www.clusir-rha.fr/sites/default/files/upload/Lyon/SSI/CLUSIR_Gestion%20des%20identites%20et%20des%20acces%20V10%201-partie%201.pdf.

[7] CNIL, *10 conseils pour la sécurité de votre système d'information*, 2009, [En ligne], http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/10-conseils-pour-la-securite-de-votre-systeme-dinformation/.

[8] CNRS, Guillaume Harry, *IAM : Gestion des identités et des accès, concepts et états de l'art* 2013, [En ligne], https://aresu.dsi.cnrs.fr/IMG/pdf/IAM_gestion_des_identites_et_des_acces.pdf.

[9] FORRESTER, Andras Cser*, Build your Identity and Access Management Strategy*, 2012.

[10] FORUM DES COMPÉTENCES, avec la contribution de Solucom management et IT Consulting, *Habilitations dans les systèmes d'information*, 2010, [En ligne], http://www.forum-des-competences.org/files/resourcesmodule/@random4e12fd120be99/1310025977_Publication_Habilitation.pdf.

[11] MSSS, GESTION DES RESSOURCES INFORMATIONNELLES, *Règle particulière sur la sécurité logique*, 2013, [En ligne], , http://msssa4.msss.gouv.qc.ca/fr/document/d26ngest.nsf/3f4763bf7e3c23a78525660f00727c27/0c830c0490e37d1485257ba3004d6c22/$FILE/04%2002%2003%2001%20-%20RP%20-%20S%C3%A9curit%C3%A9%20logique%20(version%201-00).pdf.

[12] CA TECHNOLOGIES, SUMNER BLOUNT, MERRITT MAXIM, « Rôle de la gestion des identités et des accès dans la réalisation d'une mise en conformité continue », *Gestion de*

la sécurité, 2012, [En ligne], http://www.ca.com/~/media/5916CA4A69504875B2FAF2E094ECE145.pdf.

[13] GOVERNMENT OF CANADA, *Entreprise Security Architecture (ESA) Essentiel Security Controls*, 2014.

[14] HITACHI ID SYSTEMS, INC, *Best Practices for Securing Privileged Accounts*, 2011.

[15] IIA THE INSTITUTE OF INTERNAL AUDITORS, GTAG, SAJAY RAI, ERNST et YOUNG LLP, *Guide pratique d'audit des technologies de l'information : gestion des identités et des accès*, 2007.

[16] ISO/CEI 27002, *Code de bonne pratique pour la gestion de la sécurité de l'information*, 2e édition, juin 2005.

[17] NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, INFORMATION ASSURANCE DIRECTORATE, *CGS Access Management Capability*, version 1.1.1, 2012.

[18] NIST, Vincent C. Hu, et Karen SCARFONE, *Guidelines for Access Control System Evaluation Metrics*, 2012.

[19] NIST, Vincent C. Hu, David F. FERRAIOLO et D. RICK KUHN, *Assessment of Access Control Systems*, 2006.

[20] PINGIDENTITY.COM, *Guide à l'usage des DSI : la gestion des identités nouvelle génération, comment la gestion des identités influence la digitalisation de votre métier?*, 2014.

[21] Sofiane BOULARES, *Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès*, mémoire du maîtrise ès science (M. Sc.), Université du Québec en Outaouais, Département d'informatique et d'ingénierie, 2010.

[22] SECRÉTARIAT GÉNÉRAL, SERVICE DES RESSOURCES HUMAINES, *Missions Aghora et systèmes d'information des ressources humaines;* MINISTÈRE DE L'AGRICULTURE, DE L'AGROALIMENTAIRE ET DE LA FORÊT, RÉPUBLIQUE FRANÇAISE, *Politique d'attribution des habilitations dans le système d'information dédié à la gestion des ressources humaines AGORHA*, 2014, [En ligne], https://www.google.ca/?gws_rd=ssl#q=+gestion+des+habilitations+Agorha.

[23] SOCIÉTÉ DE TRANSPORT DE MONTRÉAL, SECRÉTARIAT ET AFFAIRES JURIDIQUES, *Contrôle des accès logiques aux systèmes et applications d'affaires*, directive sectorielle, gestion des ressources informationnelles et matérielles, technologies de l'information, 2002.

ANNEXE I Acronymes et définitions

Acronymes

COGI : coordonnateur organisationnel de gestion des incidents.

COSI : conseiller organisationnel en sécurité de l'information.

ROSI : responsable organisationnel de la sécurité de l'information

Définitions

Authentifiant : information confidentielle détenue par une personne et permettant son authentification. Elle peut être sous la forme d'un mot de passe, d'un numéro d'identification personnel (NIP) ou autre, selon la technologie utilisée. [OQLF, 2000]

Authentification : procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel. [OQLF, 2003] L'authentification permet de valider l'authenticité de l'entité qui demande l'accès. S'authentifier, c'est apporter la preuve de son identité.

Comptes à privilèges spéciaux : comptes qui comprennent les comptes d'administrateur, les comptes intégrés et les comptes utilisés pour exécuter des programmes de service. Ils sont des comptes hautement sensibles qu'il faut entourer de mesures de sécurité supplémentaires et contrôler périodiquement.

Comptes intégrés : comptes utilisés par un système pour se connecter à un autre système.

Compte générique : compte anonyme n'appartenant pas à une personne en particulier. Il peut être utilisé par plusieurs utilisateurs, par exemple « compta1 », « compta2 ». [7]

Contrôle d'accès : procédure qui consiste à vérifier si un sujet (personne ou dispositif) demandant d'accéder à un objet (fichier, base de données ou dispositif) dispose des permissions nécessaires pour le faire. [21]

Contrôle d'accès : contrôles qui permettent d'autoriser ou d'interdire l'accès utilisateur aux ressources à l'intérieur du système d'information. [3]

Contrôle d'accès : processus par lequel les données d'authentification fournies par une personne, ou toute autre entité, pour avoir accès à un centre ou à un système informatique, sont comparées avec des valeurs de référence définies touchant cette entité, permettant ainsi l'autorisation ou le refus de l'accès demandé, qu'il soit physique ou logique. [OQLF, 2005]

Critères d'habilitation : exigences à respecter par une entité pour avoir l'autorisation d'accès à une information sensible.

Détenteur de l'information : employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-

tendent, relevant de la responsabilité de son unité administrative. Le terme « détenteur de processus d'affaires » est employé lorsque ce rôle se limite à un processus d'affaires déterminé. [*Directive sur la sécurité de l'information gouvernementale*, 2014]

Documents structurants : la Directive sur la sécurité de l'information gouvernementale, le Cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents à portée gouvernementale et l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information.

Droit d'accès logique : désigne l'effet recherché lorsqu'un sujet accède à un objet, c'est-à-dire lire, écrire, modifier, supprimer, imprimer, créer, copier, transmettre et approuver. [21]

Fuite d'information : se produit lorsqu'on permet la lecture d'un fichier « F1 » a une personne qui n'a pas le droit de lire un fichier « F2 », sachant que l'information contenue dans « F1 » peut provenir en partie de « F2 ». [21]

Habilitation : ensemble des droits d'accès autorisés à une entité par une autorité de l'organisme, généralement la hiérarchie immédiate. L'habilitation est associée à une fonction organisationnelle et elle est constituée de l'ensemble des profils d'accès nécessaires à l'accomplissement des tâches associées à la fonction considérée. Ainsi, toutes les personnes qui occupent la même fonction organisationnelle bénéficient, théoriquement, d'une même habilitation. [5]

L'habilitation est appelée également « profil métier » dans certains organismes. Il est important de ne pas la confondre avec l'habilitation sécuritaire qui est un filtrage de sécurité.

Incohérence du système de règles de contrôle d'accès : l'incohérence se traduit par la possibilité de dériver de l'ensemble des règles deux décisions opposées concernant un accès donné : une permission et une interdiction. [21]

Incomplétude du système de règles de contrôle d'accès : un système de règles de contrôle d'accès est incomplet s'il ne permet pas d'arriver à une permission ou une interdiction en réponse à une demande d'accès donnée. Il peut être rendu complet en appliquant une politique d'accès ouvert ou une politique d'accès fermé. [21]

Identification : permet à une entité (personne ou ordinateur) de se faire reconnaître du système par un élément dont on l'a doté préalablement. Cet élément est appelé généralement « identifiant ». S'identifier, c'est communiquer une identité préalablement enregistrée.

L'identification permet de connaître l'identité d'une entité alors que l'authentification permet de vérifier cette identité.

Identification : opération qui consiste, pour une personne ou pour toute autre entité demandant l'accès au système informatique, à communiquer à ce dernier l'identité dont elle se réclame. [OQLF, 2001]

Matrice de profils d'accès applicatifs : grille associée à un système de mission (application) et contenant les profils d'accès applicatifs supportés par ce système ainsi que les exigences de sécurité correspondantes.

Matrice de profils d'accès général : grille associée à une entité administrative et contenant les profils d'accès général définis pour ses utilisateurs ou groupes d'utilisateurs.

Politique d'accès ouverte : politique d'accès qui considère qu'un accès est permis à moins qu'il ne soit explicitement interdit. [21]

Politique d'accès fermée : politique d'accès qui considère qu'un accès est refusé à moins qu'il ne soit explicitement permis. [21]

Principe de privilège minimal : principe qui exige que l'utilisateur ne dispose pas de plus de droits que nécessaire pour accomplir ses tâches. Cela implique que les permissions affectées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches associées à ce rôle. [5]

Principe de séparation des tâches : principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible ou essentielle sont réparties entre plusieurs entités (personnes, processus, etc.), afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité. Il vise à limiter les possibilités d'abus et d'infraction par une seule personne.

Profil d'accès applicatif : profil qui regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction sur un système de mission ou une application (p. ex. pilote d'application, enquêteur, analyste, DBA). Un utilisateur peut avoir un ou plusieurs profils. [5]

Profil d'accès général : profil qui décrit les accès standard, nécessaires à un utilisateur ou un groupe d'utilisateurs, aux ressources autres que les systèmes de mission. Il concerne les accès aux messageries, boîtes aux lettres de partage, listes de distribution, répertoires de données, serveurs, intranet, extranet, etc. [5]

Programmes de services : programmes faisant généralement partie de la bibliothèque de programmes et destinés à augmenter les possibilités de base du système d'exploitation en permettant l'exécution d'opérations courantes telles que la conversion de supports de fichiers, le tri, la fusion et le diagnostic [OQLF, 2002].

Redondance de règles de contrôle d'accès : redondance qui se produit lorsque la même réponse à une demande d'accès est définie dans plusieurs règles. [21]

Registre des accès accordés : répertoire dans lequel sont consignées toutes les permissions d'accès accordées à un compte.

Registre d'autorité : répertoire, recueil ou fichier dans lequel sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information. Dans ce registre sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leurs sont assignés ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information. [Guide d'élaboration d'un registre d'autorité de sécurité de l'information, 2015]

Registre de catégorisation : répertoire dans lequel sont consignés les niveaux d'impacts, en termes de disponibilité, intégrité et confidentialité des actifs informationnels. [Guide de catégorisation de l'information, 2014]

Règle de contrôle d'accès : règle qui définit les paramètres permettant d'évaluer l'autorisation d'accès à un objet. L'application des règles de contrôle d'accès permet d'assurer que les sujets possèdent uniquement les droits d'accès qui leur sont octroyés sur les objets. [21]

Référentiel des profils d'accès à l'information : répertoire dans lequel sont consignées les matrices de profils d'accès applicatifs de chaque système de mission de l'organisme et les matrices de profils d'accès général de chaque direction générale.

Référentiel des habilitations : répertoire dans lequel sont consignés, pour chaque fonction organisationnelle, les profils d'accès applicatifs et les profils d'accès général nécessaires pour accomplir les tâches associées à la fonction ainsi que les critères d'habilitation requis.

Rôle : un rôle définit les autorisations nécessaires à l'utilisation des objets (applications ou ressources). Un rôle applicatif est un ensemble de droits d'accès propres à une seule tâche dans une application. [5]

Traçabilité : la traçabilité garantit que les accès et tentatives d'accès aux éléments considérés sont enregistrés et que ces renseignements sont normalement conservés et exploitables.

Télétravail : activité professionnelle qui s'exerce en dehors des bureaux de l'employeur et pour laquelle on fait appel aux technologies de l'information et de la communication pour communiquer à distance. [OQLF, 2008]

ANNEXE II Exemple de matrice de profils d'accès général

Secrétariat du Conseil du trésor
Québec

Matrice de profils d'accès général

Entité administrative :	AAAAAA
Responsable d'identification :	XXXXXXX
Date d'identification :	Mai 2015
Responsable validation :	YYYYYY
Date de validation :	Juin 2015

Ressources / Profils d'accès général	Accès Réseau				Internet	Extranet	Intranet	Plateformes de collaboration		Listes de distribution		Messagerie
	K/Securite	L/App	R/Log	U/usager				CODD	SIG	LD1	LD2	
Groupe_Usagers1	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Non	Non	Non	Oui
Groupe_Usagers2	Non	Non	Oui	Oui	Oui	Non	Oui	Non	Non	Non	Oui	Oui
Groupe_Usagers3	Oui	Non	Non	Oui	Oui	Oui	Oui	Non	Oui	Non	Non	Oui
Groupe_Usagers4	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui	Oui	Non	Oui
Groupe_Usagers5	Non	Non	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui
Groupe_Usagers6	Non	Oui	Non	Oui	Oui	Non	Oui	Non	Non	Oui	Non	Oui

ANNEXE III Exemple de matrice de profils d'accès applicatif

Secrétariat du Conseil du trésor Québec

Matrice profils d'accès applicatif

Détenteur de l'information :	YYYYYYY
Nom du système de mission (application) :	**Gestion des enquêtes**
Pilote du système (application) :	XXXXX
Date de validation :	Juin 2015

Rôles / Profils d'accès applicatif	Ajouter dossier enquête	Modifier dossier enquête	Consulter dossier enquête	Valider dossier enquête	Fermer dossier enquête	Assignation enquête	Éditer Rapport "enquêtes en cours"	Éditer Rapport "Dossiers fermés"	Exigences de sécurité			
									Pas de casier judiciaire	Enquêtes de crédit	Niveau d'integrité élevé	Cote de confidentialité
Enquêteur	Non	Oui	Oui	Non	Non	Non	Non	Non	Oui	Non	Oui	Oui
Analyste enquête	Non	Oui	Oui	Non	Non	Non	Non	Non	Oui	Non	Oui	Oui
Responsable enquête	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Oui	Non	Oui	Oui
Chef d'équipe	Non	Non	Oui	Oui	Non	Oui	Oui	Non	Oui	Non	Oui	Oui
Gestionnaire d'enquêtes	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	oui	Oui

ANNEXE IV Exemple de référentiel des habilitations

Secrétariat du Conseil du trésor Québec

Référentiel des habilitations

Entité administrative :	AAAAAA
Nom unité administrative :	BBBB
Responsable unité administrative :	XXXX
Date de dernière mise à jour :	Juin 2015

Fonction organisationnelle	Ressources (Profils d'accès général)	Systèmes de mission (Profils d'accès applicatifs)			Applications externes			Critères d'habilitation				
		Gestion des enquêtes	App2	App3	GR1	B12	EC20	Pas de casier judiciaire	Enquêtes de crédit	Niveau d'integrité élevé	Cote de confidentialité	Expérience
Enquêteur expert	Groupe_Uagers4	Analyste Enquête Enquêteur	Agent de recherche	Rédacteur Rapport Agent de recherche	Agent de recherche	Enquêteur	Agent de recherche	Oui	Non	Oui	Oui	5 ans ou plus
Agent administratif	Groupe_Uagers1		Agent de saisie					Non	Non	Oui	Non	Non
Directeur	Groupe_Usagers4	Chef d'équipe Gestionnaire d'enquête					Agent de recherche	Oui	Non	Oui	Oui	5 ans ou plus

ANNEXE V Exemple de registre des accès accordés

Secrétariat du Conseil du trésor Québec

Registre des accès accordés

Identifiant du compte	Nom utilisateur	Fonction organisationnelle	Unité administrative	Profil d'accès autorisé	Type de profil / applications	Date début	Date fin	Autorisé par	
								Nom gestionnaire	Unité administrative
Compte1	AA BB	Enquêteur expert	BBBB	Groupe_Usagers4	Profil d'accès général	20-10-2014		XXXX	BBBB
Compte1	AA BB	Enquêteur expert	BBBB	Analyste Enquête	Gestion des enquêtes	20-10-2014		XXXX	BBBB
Compte1	AA BB	Enquêteur expert	BBBB	Enquêteur	Gestion des enquêtes	20-10-2014		XXXX	BBBB
Compte1	AA BB	Enquêteur expert	BBBB	Agent de recherche	App2	20-10-2014	10-02-2015	XXXX	BBBB
Compte1	AA BB	Enquêteur expert	BBBB	Rédacteur Rapport	App3	20-10-2014		XXXX	BBBB
Compte1	AA BB	Enquêteur expert	BBBB	Agent de recherche	App3	20-10-2014		XXXX	BBBB
Compte2	CC DD	Directeur	BBBB	Chef d'équipe	Gestion des enquêtes	01-01-2013		XXXX	BBBB
Compte2	CC DD	Directeur	BBBB	Gestionnaire d'enquête	Gestion des enquêtes	01-01-2013		XXXX	BBBB

ANNEXE VI Exemple de directive de gestion des accès logiques

1 Préambule

En assurant un contrôle efficace des accès à l'information, l'organisme réduit les risques encourus à l'égard des objectifs d'intégrité, de disponibilité et de confidentialité de son information et répond à l'obligation gouvernementale énoncée au paragraphe (c) du premier alinéa de l'article 7 de la Directive sur la sécurité de l'information gouvernementale. Celle-ci fait obligation aux organismes publics de s'assurer de la mise en œuvre de processus formels de sécurité de l'information, dont la gestion des accès à l'information.

2 Objet

La présente directive définit les lignes directrices en matière de gestion des accès et les responsabilités à assumer par les principaux intervenants, notamment le sous-ministre ou le dirigeant de l'organisme, le responsable organisationnel de la sécurité de l'information, les détenteurs de l'information, les gestionnaires des unités administratives, le responsable des technologies de l'information, l'administrateur des accès et les utilisateurs.

Elle précise également les sanctions prévues pour tout utilisateur qui contrevient aux dispositions énoncées.

3 Cadre légal et administratif

- ✓ Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
- ✓ Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- ✓ Loi sur les archives (chapitre A-21.1);
- ✓ Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
- ✓ Loi constitutive de l'organisme qui adopte la présente directive;
- ✓ Lois et règlements sectoriels régissant la mission de chaque organisme relativement à la gestion des accès;
- ✓ Règlement sur la diffusion de l'information et sur la protection des renseignements personnels;
- ✓ Directive sur la sécurité de l'information gouvernementale, en vigueur depuis le 15 janvier 2014;
- ✓ Cadre gouvernemental de gestion de la sécurité de l'information, en vigueur depuis le 15 janvier 2014;

- ✓ Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information;
- ✓ Politique de sécurité de l'information de l'organisme, en vigueur depuis……;
- ✓ Cadre de gestion de la sécurité de l'information de l'organisme, en vigueur depuis…….

4 Champ d'application

Cette directive s'applique à :

- ✓ l'information que détient l'organisme dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers;
- ✓ l'information confiée à l'organisme en vertu d'une entente et qui est reconnue comme devant faire l'objet d'un contrôle d'accès;
- ✓ l'infrastructure technologique de l'organisme;
- ✓ toute personne physique ou morale qui, à titre d'employé, de consultant, de stagiaire, de partenaire ou de fournisseur, a un accès, sur place ou à distance, à l'information dont la sécurité est assurée par l'organisme.

5 Acronymes et définitions

5.1 Acronymes

COGI : coordonnateur organisationnel de gestion des incidents.

COSI : conseiller organisationnel en sécurité de l'information.

ROSI : responsable organisationnel de la sécurité de l'information.

5.2 Définitions

L'organisme peut reprendre de l'annexe A « Acronymes et définitions » les définitions des termes employés dans le texte de la directive.

6 Lignes directrices de la gestion des accès

- ✓ La documentation nécessaire à la mise en place du processus formel de gestion des accès doit être élaborée et révisée, si requis.
- ✓ Les accès à l'information doivent être définis sur la base du principe du privilège minimal et du principe de séparation des tâches.
- ✓ Un compte unique et nominatif est requis pour chaque accès octroyé. Les comptes génériques doivent être évités, à moins d'en justifier techniquement l'utilisation. Cette précaution permet de responsabiliser les propriétaires des comptes à l'égard des actions accomplies.

- ✓ L'octroi et l'utilisation de privilèges (comptes à privilèges spéciaux) doivent être encadrés et contrôlés rigoureusement.
- ✓ Les justificatifs d'attribution des privilèges d'accès de haut niveau doivent rester valides durant toute la période d'attribution de ces privilèges.
- ✓ Les contrôles d'accès doivent être mis en place pour s'assurer que les utilisateurs n'auront accès, en tout temps, qu'à l'information nécessaire à l'exercice de leurs fonctions.
- ✓ Le départ, le transfert ou la mutation d'un utilisateur ainsi que tout autre changement relatif à ses tâches et ses fonctions doit conduire systématiquement à la révision de ses droits d'accès.
- ✓ Toute dérogation aux critères d'habilitation prévus pour disposer des accès requis pour une fonction organisationnelle doit être signée par le gestionnaire et le détenteur concernés.
- ✓ Les mécanismes de contrôle d'accès doivent être mis en place en se basant sur le principe du privilège minimal et du degré de sensibilité de l'information utilisée.
- ✓ Des règles d'autorisation et de restriction des accès à distance doivent être clairement définies et approuvées par les détenteurs de l'information.
- ✓ Les accès attribués doivent être revus de manière périodique. Les droits, leurs modifications et leurs violations doivent être répertoriés.
- ✓ Les habilitations consignées au référentiel des habilitations doivent être, en tout temps, conformes aux descriptions de tâches associées aux fonctions organisationnelles et aux profils d'accès à l'information.
- ✓ Un audit des mécanismes de contrôle de gestion des accès doit être effectué périodiquement.
- ✓ Les utilisateurs de dispositifs mobiles doivent être sensibilisés aux risques de sécurité encourus par l'information à laquelle ils ont accès. Ils doivent être également formés à l'utilisation des bonnes pratiques en la matière.
- ✓ Les utilisateurs doivent être informés de la mise en place des journaux d'activités qui permettent de détecter et de retracer toute activité et tout accès non autorisé.
- ✓ Les équipements informatiques de l'organisme doivent être protégés adéquatement contre tout accès non autorisé et contre toute perte ou tout dommage qui pourrait être causé de façon accidentelle ou délibérée.
- ✓ L'attribution d'un accès à des données stratégiques est précédée d'un engagement formel de l'utilisateur quant au respect des règles de protection des moyens d'accès fournis et au devoir de signalement en cas de divulgation non autorisée ou même de suspicion de divulgation d'information stratégique.
- ✓ Le réseau de l'organisme doit être divisé en zones de sécurité, si requis. Les niveaux de sécurité de ces zones sont fonction du degré de sensibilité de l'information et de la criticité des applications.

7 Partage de responsabilités

Dans le cadre de la mise en place d'un processus formel de gestion des accès, les principales responsabilités assignées par la présente directive sont les suivantes.

7.1 Le sous-ministre ou le dirigeant de l'organisme

- ✓ Approuve la présente directive et en assure la diffusion;
- ✓ S'assure de la mise en place du processus formel de gestion des accès à l'information au sein de son organisme;
- ✓ Approuve toute dérogation aux dispositions de la directive.

7.2 Le responsable organisationnel de la sécurité de l'information (ROSI)

- ✓ Élabore et met à jour la directive de gestion des accès et la soumet pour validation au comité chargé de la sécurité de l'information;
- ✓ Soumet à l'approbation du sous-ministre ou du dirigeant de l'organisme la directive de gestion des accès et assure le suivi de sa mise en œuvre. Il lui soumet également toute dérogation à l'application de la directive.
- ✓ Définit le processus de gestion des accès;
- ✓ S'assure de la documentation et de la mise à jour des procédures nécessaires à la mise en place du processus formel de gestion des accès;
- ✓ S'assure de la mise en œuvre du processus de gestion des accès.

7.3 Le conseiller organisationnel de la sécurité de l'information (COSI)

- ✓ Soutient le ROSI dans l'élaboration et la mise à jour de la directive de gestion des accès;
- ✓ Soutient le ROSI dans la définition du processus de gestion des accès;
- ✓ Met en œuvre le processus de gestion des accès;
- ✓ Définit clairement la procédure d'élaboration et de maintien du référentiel des habilitations;
- ✓ Définit clairement la procédure d'élaboration et de maintien du référentiel des profils d'accès à l'information;
- ✓ Définit clairement la procédure de gestion des identifiants et des autorisations d'accès. Cette procédure couvre tout le cycle de vie d'un utilisateur dans l'organisme – arrivée, mutation, promotion, départ en congé de longue durée, départ définitif;
- ✓ Définit clairement la procédure de gestion et de révision des accès privilèges et des contrôles associés;
- ✓ Organise des séances de sensibilisation des utilisateurs des dispositifs mobiles aux risques de sécurité encourus par l'information à laquelle ils ont accès au moyen de ces dispositifs;

- ✓ S'assure qu'un audit des mécanismes de contrôle de gestion des accès est effectué périodiquement.

7.4 Le coordonnateur organisationnel de la gestion des incidents (COGI)

- ✓ Contribue à l'élaboration, la mise en œuvre et la révision de la directive de gestion des accès;
- ✓ Détermine les menaces et les situations de vulnérabilité liées à la gestion des accès et, si requis, propose des mesures de renforcement des contrôles d'accès;
- ✓ Formule des avis de pertinence sur les mécanismes de gestion des accès mis en place.

7.5 Les détenteurs de l'information

- ✓ Définissent les profils d'accès applicatifs supportés par les systèmes de mission (applications) relevant de leur autorité et s'assurent de la conformité des mécanismes d'accès aux exigences relatives à la sécurité de cette information;
- ✓ Définissent clairement les règles d'autorisation et de restriction des accès à distance à l'information relevant de leur autorité;
- ✓ Définissent les accès à l'information sur la base du principe du privilège minimal et du principe de la séparation des tâches;
- ✓ Autorisent les accès à l'information relevant de leur autorité;
- ✓ Ajustent dans les délais recommandés tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées.

7.6 Les gestionnaires

- ✓ Définissent les habilitations et les critères d'habilitation associés aux fonctions organisationnelles relevant de leur autorité;
- ✓ S'assurent de la conformité, en tout temps, des accès autorisés au principe du privilège minimal et des qualifications de leur personnel aux critères d'habilitation associés aux fonctions occupées;
- ✓ Documentent les processus d'affaires et définissent clairement les règles de séparation des tâches associées;
- ✓ Autorisent et justifient tout besoin d'accès à l'information qui ne fait pas partie des habilitations prévues pour la fonction occupée par l'employé;
- ✓ Assurent le suivi des autorisations d'accès octroyées aux utilisateurs relevant de leur autorité depuis leur arrivée jusqu'à leur départ de leur unité administrative;
- ✓ Ajustent dans les délais recommandés tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées;
- ✓ S'assurent de l'intégration dans les ententes et contrats de clauses garantissant le respect des exigences en matière de sécurité de l'information, dont celles sur la gestion des accès.

7.7 Le responsable de la gestion des technologies de l'information

- ✓ Met en place les solutions technologiques répondant aux exigences de la directive de gestion des accès;
- ✓ S'assure que les profils d'accès général sont clairement définis pour l'ensemble des postes de travail de l'organisme;
- ✓ Met en place les outils de journalisation des accès. Ainsi, lors des vérifications périodiques ou sur demande, il sera possible de savoir qui a accédé à quoi.
- ✓ S'assure que les utilisateurs n'ont pas accès à leur poste de travail en tant qu'administrateur et que toute exception est documentée et approuvée;
- ✓ Met en place sur les postes de travail des mesures de protection contre les accès non autorisés et les vulnérabilités logicielles;
- ✓ Met en place les mécanismes de surveillance et de contrôle des méthodes d'accès à distance.

7.8 L'administrateur des droits d'accès

- ✓ Applique la directive de gestion des accès et les procédures afférentes;
- ✓ Crée les identifiants et les droits d'accès pour les utilisateurs dûment autorisés par les gestionnaires et les détenteurs de l'information;
- ✓ Édite à l'intention des détenteurs et des gestionnaires les rapports périodiques des autorisations d'accès réellement attribuées et s'assure de leur validation.

7.9 L'utilisateur

- ✓ N'emploie l'information à laquelle il a accès que pour des tâches qui lui sont assignées;
- ✓ Est responsable des accès qui lui sont octroyés et redevable auprès de ses gestionnaires de toute action exécutée en utilisant son identifiant et son authentifiant;
- ✓ S'engage formellement au respect des règles de protection des moyens d'accès aux données stratégiques;
- ✓ Signale, sans délai, toute atteinte à la sécurité de l'information à laquelle il accède.

8 Sanctions

Lorsqu'un utilisateur contrevient à la présente directive ou aux réglementations en découlant, il s'expose à des mesures disciplinaires, administratives ou légales en fonction de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

L'organisme peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

9 Dispositions particulières

- ✓ Le responsable organisationnel de la sécurité de l'information est responsable de l'application des dispositions de la présente directive;
- ✓ Le responsable organisationnel de la sécurité de l'information procédera, au besoin, à la révision de la présente directive.

10 Approbation et date d'entrée en vigueur

La présente directive entre en vigueur à la date de son approbation par le sous-ministre.

Sous-ministre Date

Secrétariat
du Conseil du trésor
Québec
Au cœur de l'administration publique