

Direction générale adjointe

CENTRE OPÉRATIONNEL DE  
CYBERDÉFENSE (DGAC OCD)

# CYBERSÉCURITÉ

Directive ministérielle  
Gestion des accès à l'information

MSSS-DIR08

2023-02-23



## Table des matières

Préambule	3
Objectifs	3
Champ d'application et portée	3
Cadre légal et administratif	3
Définitions	4
Obligations	4
1. Encadrer la gestion des accès	5
2. Réaliser la gestion des accès	5
3. Contrôler et réviser les accès	6
4. Surveiller et améliorer le processus de gestion des accès	6
Obligations des principaux intervenants	6
Sanctions	7
Entrée en vigueur et révision	8

---

## Préambule

---

Le ministère de la Santé et des Services sociaux (MSSS) détient des renseignements personnels et confidentiels qui doivent être protégés adéquatement, de toute divulgation, accès ou utilisation non autorisée, et ce, tout au long de leur cycle de vie.

La gestion des accès est primordiale dans la protection de l'information<sup>1</sup>. Elle permet de protéger les programmes du ministère, ses services, ses renseignements sensibles, et de maintenir la confiance du public en sa prestation de services. Elle vient en complément de la gestion des identités et de l'authentification<sup>2</sup>.

Dans ce contexte, le MSSS prend en compte la nécessité d'une gestion des accès structurée, bien définie et actuelle pour être efficace et faire face aux cybermenaces. La présente directive établit les fondations permettant de mettre en place une telle gestion des accès.

---

## Objectifs

---

La présente directive vise à :

- Définir les obligations en matière de gestion des accès logiques à l'information;
- Préciser les rôles et responsabilités des principaux intervenants du MSSS, en matière de gestion d'accès.

---

## Champ d'application et portée

---

Cette directive s'applique au MSSS. Elle s'applique également :

- À tous les domaines d'activités de l'organisation;
- Aux ressources informationnelles et à l'information, peu importe sa nature, le support numérique sur lequel elle se trouve (enregistrement sonore ou vidéo, données électroniques ou numériques, etc.) ou sa localisation, et ce, durant tout son cycle de vie;
- À l'information confiée au MSSS en vertu d'une entente;
- À la conservation de l'information assurée par un tiers.

---

## Cadre légal et administratif

---

Le cadre légal et administratif applicable est celui défini dans la politique provinciale de sécurité de l'information (PPSI),

---

<sup>1</sup> Les informations en format non numérique, ainsi que les accès physiques ne font pas l'objet de cette directive.

<sup>2</sup> La présente directive n'aborde pas la gestion des identités et de l'authentification.

sans toutefois s'y limiter.

Cette directive s'inscrit également en conformité avec les exigences :

- De la Directive gouvernementale sur la sécurité de l'information;
- Du Cadre ministériel de gestion de la sécurité de l'information.

## Définitions

Pour l'application de la présente directive, les termes suivants signifient:

TERME	DESCRIPTION
<b>Accès à haut privilège</b>	<p>Il désigne un accès spécial ou des capacités qui s'étendent au-delà de celles d'un accès standard. L'accès à haut privilège permet aux organisations de sécuriser leurs infrastructures et leurs applications, de poursuivre leurs activités de façon efficace et de préserver la confidentialité des données sensibles et des infrastructures critiques.</p> <p>L'accès à haut privilège peut être associé à des utilisateurs humains, mais aussi à des utilisateurs non humains comme des applications et des identités de machines.</p> <p>Par exemple, accès liés aux comptes d'urgence, compte de service, compte d'administrateur, etc.</p>
<b>Principe du droit d'accès minimal (de moindre privilège)</b>	<p>Droit d'accès restreint afin que l'utilisateur puisse accomplir avec celui-ci, les seules tâches autorisées et nécessaires à l'exercice de ses fonctions<sup>3</sup>.</p>
<b>Séparation des tâches</b>	<p>Procédure de contrôle consistant à attribuer à des personnes différentes des responsabilités relatives à l'autorisation et à l'enregistrement des opérations et à la garde des actifs afin de réduire les possibilités qu'une même personne puisse commettre et dissimuler des erreurs et des fraudes dans le cadre normal de l'exercice de ses fonctions<sup>4</sup>.</p>

## Obligations

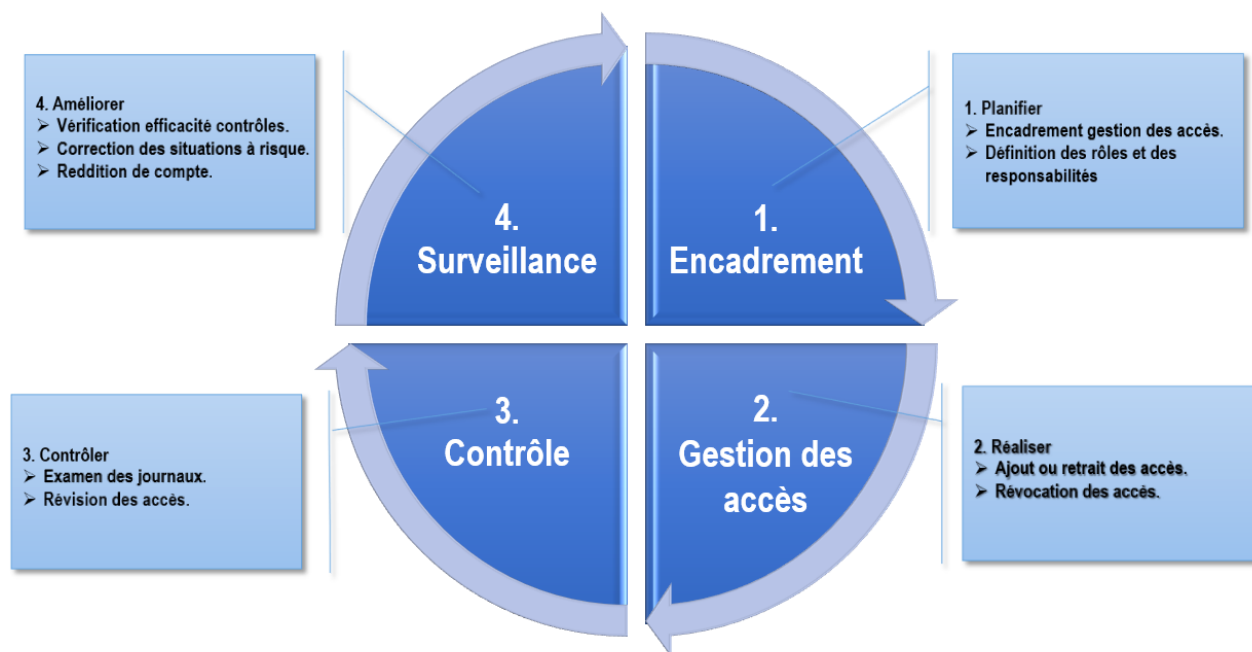
Les obligations de cette directive sont énoncées en lien avec les quatre principaux volets du processus de gestion des accès, comme illustrés ci-dessous<sup>5</sup> :

<sup>3</sup> Office québécois de la langue française, [https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?ld\\_Fiche=2074701](https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?ld_Fiche=2074701)

<sup>4</sup> Office québécois de la langue française, [https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?ld\\_Fiche=504988S](https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?ld_Fiche=504988S)

<sup>5</sup> Vue simplifiée des principaux volets du processus de GIA

[https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources\\_informatiques/secure\\_informations/Gestion\\_identite\\_acces.pdf](https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informatiques/secure_informations/Gestion_identite_acces.pdf)



Principaux volets du processus de gestion des accès

## 1. Encadrer la gestion des accès

- Mettre en place un processus de gestion des accès logiques à l'information, en considérant la sensibilité de l'information et les risques auxquels elle s'expose. Plus précisément :
  - Définir les privilèges d'accès à l'information au respect des principes du « **droit d'accès minimal** » et de la « **séparation des tâches** »;
  - Élaborer des procédures permettant d'octroyer, révoquer, et modifier les droits des accès dans le respect des exigences du MSSS en la matière;
  - Mettre en place des mécanismes de contrôle pour l'octroi, l'utilisation, et la révocation des accès<sup>6</sup>;
  - Former les intervenants du processus de gestion des accès aux exigences de gestion des accès.

## 2. Réaliser la gestion des accès

- Octroyer, modifier ou ajouter des accès aux utilisateurs selon les demandes d'accès dûment approuvées;
- Révoquer des accès immédiatement, lors d'une fin d'emploi ou d'une fin d'affectation d'un employé;

<sup>6</sup> Une attention toute particulière doit être accordée à l'encadrement des accès à haut privilège.

- Suspendre les accès d'un utilisateur lors d'une absence prolongée.

---

### 3. Contrôler et réviser les accès

---

- Réviser périodiquement les droits d'accès et corriger rapidement les écarts constatés :
  - Selon le niveau de sensibilité de l'information, la révision des accès doit être effectuée au moins une fois par année.
- Examiner périodiquement et en continu les journaux et les alertes de sécurité des accès, notamment:
  - Les activités des accès à haut privilège;
  - Les accès incompatibles ou non autorisés;
  - Les défaillances et les événements liés à la cybersécurité<sup>7</sup>.

---

### 4. Surveiller et améliorer le processus de gestion des accès

---

- S'assurer que les contrôles du processus sont en place et qu'ils fonctionnent comme prévu;
- Veiller à corriger immédiatement les situations à risques pouvant compromettre l'efficacité du processus de gestion des accès;
- Effectuer une reddition de comptes au CDSI, sur la performance du processus de gestion des accès, qui comporte des indicateurs de suivi et des mesures correctrices.

---

## Obligations des principaux intervenants

---

Cette section énonce les rôles et responsabilités des principaux intervenants qui doivent participer au processus de gestion des accès à l'information, en complément aux responsabilités déjà prévues aux documents de la section « Cadre légal et administratif » :

#### **Chef délégué de la sécurité de l'information (CDSI)**

- S'assurer de l'efficacité et de la conformité du processus ministériel de gestion des accès;

#### **Le Chef de la sécurité de l'information organisationnelle (CSIO)**

- Élaborer et mettre à jour les documents d'encadrement nécessaires à la mise en œuvre du processus de gestion des accès;

---

<sup>7</sup> Aucun utilisateur ne doit avoir la possibilité d'effacer ou de désactiver les journaux ou les alertes concernant ses propres activités.

- S'assurer périodiquement de l'efficacité des mécanismes de contrôles de gestion des accès;
- Procéder annuellement à la reddition de comptes<sup>8</sup> au CDSI.

### **Le détenteur de l'information**

- Définir les profils d'accès supportés par les actifs informationnels relevant de son autorité;
- Définir les règles d'autorisation et de restriction des accès à l'information relevant de son autorité.

### **Le pilote d'application**

- Accorder les accès aux ressources sous sa responsabilité;
- Éditer à l'intention des détenteurs et des gestionnaires, les rapports des accès attribués et s'assure de leur validation par ces derniers;
- Ajuster tout écart constaté dans l'attribution des accès.

### **Le gestionnaire**

- Assurer le suivi des autorisations d'accès octroyées aux utilisateurs relevant de son autorité dès leurs entrées en fonction (demande des accès), jusqu'à leur départ de son unité administrative (révocation des accès);
- Informer le Centre de services du MSSS de tout écart constaté dans l'attribution des accès octroyés à son unité administrative.

### **La direction des opérations technologiques**

- Élaborer et mettre en place des procédures pour la mise en œuvre du processus de gestion des accès;
- Mettre en place les outils technologiques prémunissant le MSSS contre les accès non autorisés et assurant la journalisation et la surveillance des activités liées aux accès à l'information.

### **L'utilisateur**

- Respecter les exigences de la présente directive;
- Utiliser l'information à laquelle l'utilisateur a accès aux seules fins qui lui sont prévues;
- Informer son gestionnaire, ainsi que le Centre de services de tout écart constaté lors de l'attribution des accès.

---

## **Sanctions**

Lorsqu'un employé contrevient ou déroge à la présente directive, il s'expose à des mesures disciplinaires, administratives ou légales pouvant aller jusqu'au congédiement.

---

<sup>8</sup> La reddition de comptes consiste à faire une révision approfondie des différentes procédures, à détecter les anomalies et à apporter les correctifs nécessaires, comme la séparation des tâches incompatibles, la révision des accès, la journalisation et le suivi, et la révocation des accès.

---

## Entrée en vigueur et révision

---

Cette directive entre en vigueur à la date de son approbation. Elle doit être révisée tous les trois ans, ou lors de changements organisationnels majeurs ou lors de l'adoption de nouvelles orientations gouvernementales.

<b>Approuvée par le chef délégué de la sécurité de l'information (CDSI) :</b>	Reno Bernier
<b>Date d'approbation :</b>	2023-02-23



