Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Directive sur la gestion de l'identité

Publié : le 01 août 2011

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT39-8/2011F-PDF
ISBN : 978-0-660-09647-6

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Directive on Identity Management

Directive sur la gestion de l'identité

1. Date d'entrée en vigueur

1.1 La présente directive entre en vigueur le 1er juillet 2009.

2. Application

2.1 La présente directive s'applique :

- à tous les ministères au sens des annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP), sauf s'ils en sont exclus en vertu d'une loi, d'un règlement ou d'un décret particulier.
- aux ministères qui utilisent le système de paie de Travaux public et Services gouvernementaux Canada (TPSGC) pour s'acquitter des responsabilités énoncées à la section 6.2.

3. Contexte

3.1 La gestion de l'identité est l'établissement, par une institution gouvernementale, de la légitimité de l'identité de la personne ou de l'organisme avec qui elle transige. La gestion de l'identité est au cœur de l'administration publique et de la plupart des processus opérationnels du gouvernement. Une fois l'identité établie, toutes les activités gouvernementales subséquentes, qui vont de la protection des biens à la prestation de services en passant par les avantages et les droits conférés ainsi que les interventions en cas de catastrophe et d'urgence, reposent sur cette identité.

3.2 La diversité des pratiques de gestion de l'identité à l'échelle du gouvernement du Canada (GC) et d'autres administrations peut accroître les risques d'usage frauduleux de documents d'identité, de vols d'identité, d'octroi irrégulier de droits, de perte d'avantages et de pertes financières pour les particuliers et les gouvernements ainsi que d'atteinte à la vie privée.

3.3 Sans une approche cohérente, uniforme, normalisée et interopérable de gestion de l'identité au gouvernement fédéral et dans les autres administrations, il devient de plus en plus difficile d'élaborer et de déployer des stratégies efficaces d'atténuation des risques pour gérer les défis que représentent la sécurité nationale, le respect de la vie privée, l'intégrité des programmes et la prestation de services axés sur le citoyen.

3.4 Il est de plus en plus évident qu'une approche uniforme de gestion de l'identité appuyée par des normes doit être mise en place. On s'assurera ainsi que les exigences en matière de sécurité sont respectées et que les services sont créés, sont administrés et sont fournis aux bons clients. La mise au point et la mise en œuvre de cette approche normalisée permettront aussi d'en arriver à une solution robuste, évolutive et souple pour une validation adéquate des renseignements d'identité.

3.5 Il incombe aux ministères d'assumer la responsabilité de la gestion de l'identité dans les cas suivants :

- une identification précise est requise pour les besoins de l'administration d'un programme ou d'un service fédéral prévu par la loi;
- la divulgation de l'identité est requise pour bénéficier d'un service gouvernemental, participer à un programme du gouvernement ou devenir membre d'une organisation gouvernementale.

3.6 La présente directive est établie en vertu de l'article 7 de la LGFP.

3.7 La présente directive doit être lue en parallèle avec le *Cadre principal des politiques du Conseil du Trésor*, la *Politique sur la sécuritédu gouvernement*et la *Directive sur la gestion de la sécurité ministérielle*.

3.8 Des exigences obligatoires supplémentaires sont énoncées dans des normes à l'appui des éléments suivants :

- l'assurance de l'information et de l'identité;
- les enquêtes de sécurité;
- la sécurité matérielle;
- la sécurité des TI;
- la gestion des urgences et de la continuité des activités;
- la sécurité des marchés.

4. Définitions

4.1 Pour connaître la définition des termes employés dans la présente directive, se reporter à l'appendice – Définitions.

5. Énoncé de la directive

5.1 **Objectif**

L'objectif de la présente directive consiste à s'assurer d'instaurer des pratiques efficaces de gestion de l'identité en donnant un aperçu des exigences qui aideront les ministères à établir, à utiliser et à valider l'identité.

5.2 **Résultats escomptés**

Voici les résultats escomptés de la présente directive :

5.2.1 de saines pratiques de gestion de l'identité s'harmonisant avec une approche pangouvernementale intégrée en vue de permettre la mise en place d'une gestion efficace de l'identité à l'échelle du GC;

5.2.2 la gestion de l'identité est un élément identifiable qui fait partie intégrante des programmes, des activités et des services du ministère;

5.2.3 la gestion efficace de l'identité permet aux ministères de faire respecter leurs exigences en matière de service et de sécurité et de s'assurer qu'ils transigent avec le bon client lors de la prestation de services;

5.2.4 les ministères veillent à ce que leurs activités de gestion de l'identité autorisent une interopérabilité, s'il y a lieu, qui permet l'échange de renseignements sur l'identité des personnes afin de satisfaire aux objectifs généraux du GC ainsi qu'aux exigences des mandats respectifs des ministères.

6. Exigences

6.1 Les gestionnaires de tous les niveaux qui assument des responsabilités à ce titre, géreront l'identité de façon à atténuer les risques pour la sécurité personnelle, organisationnelle et nationale, protégeront l'intégrité des programmes et permettront une prestation de services bien gérés et axés sur le client. Les gestionnaires de tous les niveaux qui exercent une telle responsabilité sont chargés de ce qui suit :

6.1.1 S'assurer que la nécessité de l'identification est justifiée et qu'ils sont légalement habilités à procéder à une vérification d'identité pour les besoins d'un programme particulier ou à l'appui des activités d'exécution de la loi, de sécurité nationale ou de défense;

6.1.2 Exposer les risques en matière de gestion de l'identité (p. ex. changement de circonstances, erreurs, méfaits), les répercussions sur les programmes, les niveaux d'assurance requis et les options d'atténuation des risques;

6.1.3 Sélectionner un ensemble approprié de données d'identité (comme des caractéristiques personnelles ou des données d'identification) qui est suffisant pour établir une identité unique afin de répondre aux besoins de programme, qui est proportionnel aux risques recensés et qui est assez souple pour permettre la mise en place d'autres méthodes d'identification au besoin;

6.1.4 Mettre en œuvre des solutions de partage de renseignements sur l'identité qui respectent les normes communes du GC.

6.2 Les gestionnaires des ressources humaines assument les responsabilités suivantes :

6.2.1 s'assurer qu'un code d'identification de dossier personnel (CIDP) unique est attribué à chaque fonctionnaire du gouvernement fédéral aux fins de la gestion des données et des transactions concernant l'employé;

6.2.2 s'assurer qu'un numéro individuel d'organisme (NIO) est attribué à chaque employé qui doit être identifié auprès d'un ou de plusieurs organismes de remise à l'extérieur de la fonction publique fédérale.

6.3 Surveillance et exigences en matière de rapport

Au sein des ministères :

Les gestionnaires de tous les niveaux ayant des responsabilités de gestion de l'identité sont chargés de ce qui suit :

- veiller au respect de la présente directive dans leurs services et s'assurer qu'une mesure corrective est prise pour corriger toute lacune relevée.

À l'échelle du gouvernement :

Le SCT est responsable de ce qui suit :

- contrôler la conformité à tous les aspects de la présente directive et vérifier que les résultats escomptés ont été atteints de diverses manière, y compris sans toutefois s'y limiter, des évaluations aux termes du Cadre de responsabilisation de gestion (CRG), des examens des présentations au Conseil du Trésor, les rapports ministériels sur le rendement (RMR), les rapports annuels, les résultats de vérifications, d'évaluations et les études ainsi qu'au moyen d'un dialogue permanent et des travaux des comités.

7. Conséquences

7.1 L'administrateur général est chargé d'enquêter sur les problèmes d'inobservation de la présente directive, puis d'intervenir. Il est également responsable de veiller à ce que des mesures correctives appropriées soient prises pour régler ces problèmes.

7.2 Si le secrétaire du Conseil du Trésor estime qu'un ministère ne s'est peut-être pas conformé à une exigence quelconque de la présente directive, il peut demander à l'administrateur général de :

7.2.1 procéder à une vérification ou à un examen, dont le coût sera imputé au niveau de référence du ministère, pour déterminer si les

exigences de la présente directive ont été satisfaites; et/ou

7.2.2 prendre des mesures correctives et faire ensuite rapport sur les résultats.

8. Références

Les lois qui s'appliquent à la présente directive sont les suivantes :

- *Charte canadienne des droits et libertés*
- *Code criminel*
- *Loi canadienne sur les droits de la personne*
- *Loi sur l'accès à l'information*
- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la gestion des finances publiques*
- *Loi sur la protection des renseignements personnels*
- *Loi sur le casier judiciaire*

Parmi les politiques et les directives du Conseil du Trésor qui s'appliquent à la présente directive, il y a les suivantes :

- *Cadre stratégique sur l'information et la technologie*
- *Cadre de gestion intégrée du risque*
- *Code de valeurs et d'éthique de la fonction publique*
- *Directive sur le numéro d'assurance social*
- *Politique d'évaluation des facteurs relatifs à la vie privée*
- *Politique sur l'accès à l'information*
- *Politique sur l'évaluation*
- *Politique sur l'obligation de prendre des mesures d'adaptation pour les personnes handicapées dans la fonction publique fédérale*
- *Politique sur la gestion de l'information*
- *Politique sur la gestion des risques*
- *Politique sur la gestion des technologies de l'information*
- *Politique sur la protection de la vie privée*
- Politique sur la sécurité du gouvernement
- *Politique sur la structure de gestion des ressources et des résultats*
- *Politique sur la vérification interne*
- *Politique sur le contrôle interne*

9. Demandes de renseignements

Veuillez adresser vos demandes de renseignements au sujet de la présente directive à l'administration centrale de votre ministère. Pour l'interprétation de la présente directive, les responsables de l'administration centrale des ministères devraient communiquer avec la Division de la sécurité et gestion de l'identité.

Appendice – Définitions

Gestion de l'identité (*identity management*)
: Ensemble des principes, pratiques, politiques, processus et procédures utilisés pour réaliser le mandat de l'organisation et ses objectifs liés à l'identité.

Identité (*identity*)
: Référence ou désignation utilisée pour distinguer une personne, une organisation ou un appareil unique et particulier.

Interopérabilité (*interoperability*)
: Capacité des ministères fédéraux de fonctionner en synergie au moyen de pratiques cohérentes de gestion de la sécurité et de l'identité.

Organisme de remise (*remittance agency*)
: Organisation de l'extérieur de la fonction publique fédérale à laquelle les institutions gouvernementales fédérales remettent des sommes d'argent pour le compte des employés (p. ex. des organismes de bienfaisance, des institutions financières et des administrateurs d'assurance).