Ministère
de la Cybersécurité
et du Numérique
Québec

Indication d'application
concernant les Règles relatives à l'assurance de l'identité numérique

Statut	En vigueur
Diffusion	Non restreinte
No de référence	IA-SI-2022-001-OP
Organismes visés	Organismes publics
Indication formulée par	Chef gouvernemental de la sécurité de l'information
Référence légale	LGGRI, chapitre G-1.03, art. 12.6 et art. 21
Date de formulation	2022-10-04
Date d'entrée en vigueur	2022-10-04
Dernière mise à jour	S. O.
Expiration	Indéterminée

SECTION I
Objet et champ d'application

1. La présente indication d'application complète les Règles relatives à l'assurance de l'identité numérique (ci-après « Règles »), déterminées par l'arrêté numéro 2022-05 du ministre de la Cybersécurité et du Numérique en date du 26 août 2022, afin de préciser les exigences de mise en œuvre de ces règles.

Elle intéresse plus particulièrement les dirigeants de l'information (DI), agissant à titre de chef délégué de la sécurité de l'information (CDSI), dans l'exercice de leurs fonctions conformément à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, ci-après appelée « Loi »).

2. La présente indication d'application s'applique aux organismes publics visés à l'article 2 de la Loi.

SECTION II
Détermination du niveau d'assurance de l'identité requis pour un service

3. La présente section précise ce qui est attendu dans la détermination du niveau d'assurance de l'identité requis pour un service sous la responsabilité d'un organisme public.

Elle s'adresse plus particulièrement aux secteurs d'affaires des organismes publics, afin que de tels secteurs soient en mesure d'appliquer les Règles lorsqu'une personne entend utiliser ou autrement bénéficier d'un service de tels organismes.

Précisions sur l'évaluation du besoin de confiance

4. Le niveau d'assurance de l'identité est tributaire du besoin de confiance requis pour qu'un organisme public fournisse à une personne, qui est bien celle qu'elle prétend être, un service sous sa responsabilité. Le niveau d'assurance requis pour un service est lié au niveau maximal de préjudices pouvant se produire si un tel service est fourni à une personne qui prétend, à tort, être ou agir au nom d'une autre personne. Ce niveau maximal est déterminé en appliquant et en s'inspirant du tableau en annexe, lequel est constitué d'exemples de préjudices pouvant être causés aux différentes parties concernées :

1° à la personne physique, à l'entreprise ou à l'entité visée par le service sollicité;
2° aux organismes publics, formant l'Administration publique au sens du premier alinéa de l'article 2 de la Loi, ou à l'État.

La détermination du niveau d'assurance de l'identité en s'appuyant sur les exemples de préjudices présentés à ce tableau permet notamment de conclure que :

1° tout service où il est possible de consulter des renseignements personnels, confidentiels ou sensibles nécessiterait minimalement le niveau d'assurance de l'identité **élevé** considérant les exemples de préjudices à une personne physique relatifs à l'atteinte à l'identité ou à la protection des renseignements personnels (« PRP »). Il en est de même pour les entreprises ou les autres entités concernant leurs renseignements confidentiels;
2° tout service en soutien à l'identité ou servant à émettre des preuves à l'appui de l'identité nécessiterait le niveau d'assurance de l'identité **élevé** ou **très élevé** considérant les exemples de préjudices à un ou plusieurs organismes publics, ou plus généralement à l'État, relatifs à l'atteinte à l'identité ou à la PRP;
3° tout service offert à une personne physique, à une entreprise ou à une autre entité servant par exemple à l'impôt, aux rentes, aux subventions, aux crédits ou aux allocations nécessiterait minimalement le niveau d'assurance de l'identité **élevé** considérant les exemples de préjudices à une personne physique, aux entreprises ou à d'autres entités, relatifs aux pertes financières et aux potentielles violations du cadre législatif et réglementaire.

Pour l'application de la présente indication d'application, lorsqu'il est fait référence à « renseignement sensible » au tableau en annexe, est alors visé un renseignement personnel qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un degré élevé d'attente raisonnable en matière de vie privée.

5. L'identification du niveau d'assurance de l'identité requis d'un service devrait notamment impliquer les analystes d'affaires, les responsables de la protection des renseignements personnels ainsi que le personnel de l'organisme public concerné qui a la connaissance de la clientèle et de la mission du service.

SECTION III
Identification

6. La présente section précise ce qui est attendu en ce qui concerne l'identification d'une personne visée à la sous-section 2 de la section III des Règles.

Elle s'adresse plus particulièrement à tout contributeur à la vérification de l'identité, incluant les sources de confiance et les organismes publics émettant des secrets partagés.

Précisions sur les sources de confiance

7. Une « source de confiance », aussi connue comme « source qui fait autorité », est une autorité détenant des dossiers ou un registre de dossiers qui respecte les critères suivants :

1° est reconnue comme fiable et sécuritaire par le gouvernement ou l'ensemble de la société civile;
2° offre des garanties sur la sécurité des données;
3° offre des garanties sur l'exactitude et la qualité des données;
4° offre des garanties sur le respect de la vie privée dans la collecte et l'utilisation des données;
5° documente les processus de collecte et de conservation des données;
6° respecte les lois au regard de la protection et de l'utilisation des renseignements personnels;
7° assure la protection des données, notamment en s'assurant de leur chiffrement au repos et en transit.

8. Une source de confiance peut notamment être une source officielle de données numériques gouvernementales au sens de la Loi.

Listes des preuves d'identité reconnues (pour une personne)

9. Les documents originaux suivants sont considérés comme étant une preuve de l'identité essentielle :

1° émis par le gouvernement du Québec :
- certificat ou copie officielle de l'acte de naissance;

2° émis par une autre province du Canada :
- certificat ou copie officielle de l'acte de naissance;

3° émis par le gouvernement du Canada :
- certificat de citoyenneté (preuve de citoyenneté;);
- document de confirmation de résidence permanente;

4° émis par une autorité étatique, une source alors jugée fiable :
- tout document établissant l'identité et la date de naissance d'une personne.

10. Les documents originaux suivants sont considérés comme étant des preuves à l'appui de l'identité aussi appelées preuves de l'identité contextuelles:

1° émis par le gouvernement du Québec :
- permis de conduire (SAAQ);
- carte d'assurance maladie (RAMQ);

2° émis par une autre province du Canada :
- permis de conduire avec photo;
- carte d'assurance maladie avec photo;
- carte d'identité avec photo;

3° émis par le gouvernement du Canada :
- passeport;
- documents de statut d'immigrant (ex. : IMM 1442);
- pièces d'identité officielles pour les militaires, les policiers ou les diplomates en poste au Canada;
- certificat sécurisé de statut d'Indien;
- carte de citoyenneté émise avant le 1er février 2012[1];
- carte de résident permanent;

4° émis par tout autre gouvernement :
- passeport;
- preuve d'identité avec photo (si la pièce d'identité est rédigée dans une langue autre que le français ou l'anglais, elle doit être accompagnée d'une traduction officielle).

11. Toute preuve d'identité ayant une date d'expiration doit être valide au moment de l'identification.

Précisions sur la vérification de l'identité par un agent

12. La vérification de l'identité par un agent visée à la section V des Règles doit être effectuée suivant l'une des méthodes suivantes :

1° sur place (en présence physique);
2° par un moyen technologique permettant de voir et d'entendre de façon simultanée la personne (ex. : vidéoconférence);
3° via une vidéo enregistrée où la personne doit effectuer plusieurs actions aléatoires qui lui sont demandées.

13. Toute méthode autorisée pour l'identification d'une personne doit comporter un test de vivacité permettant à l'agent de s'assurer qu'il s'adresse à un humain, que son apparence n'est pas modifiée ou altérée et que le contexte est propice à l'identification.

14. Advenant que les conditions de l'appel, lors d'une identification par vidéoconférence, ne permettent pas l'identification ou que celle-ci soit mise en doute, le responsable de l'identification doit informer la personne concernée des raisons pour lesquelles il ne pourra vérifier son identité et l'agent doit terminer l'appel.

[1] Le gouvernement du Canada a cessé de délivrer les cartes de citoyenneté en février 2012.

15. Si une identification par vidéoconférence est interrompue, le processus d'identification de la personne concernée ne peut se poursuivre et le responsable doit en informer avec diligence cette personne.

16. Lors d'une vérification d'identité via une vidéo, l'identification s'effectue à l'aide d'une application ou d'un système contrôlé par l'entité chargée de l'identification où la personne concernée se filme et effectue certaines actions. Ces actions ne doivent pas être connues d'avance par cette personne et celles-ci lui sont présentées aléatoirement parmi une liste d'actions prédéfinies non publicisée. La vidéo de la personne concernée, une fois terminée, ne peut être modifiée ou téléchargée.

17. Une vérification de la vidéo doit être effectuée par un agent. L'agent doit notamment s'assurer de la continuité de la vidéo et du fait que les actions sont menées tel que demandé et de manière fluide.

Advenant que les conditions, lors d'une telle vérification, ne permettent pas l'identification ou que celle-ci soit mise en doute, l'agent doit refuser l'identification de la personne concernée et l'entité chargée de l'identification doit informer avec diligence cette personne des raisons du refus.

18. Advenant l'interruption du processus menant à l'identification d'une personne dans les cas visés aux articles 14 à 17, l'identification de la personne doit être reprise depuis le début en prenant les mesures correctives adéquates pour assurer son identification ou être effectuée au moyen d'une vérification de l'identité sur place.

Choix de la méthode de vérification d'identité

19. Lorsque plusieurs méthodes pour la vérification de l'identité sont disponibles, la personne concernée doit pouvoir choisir la méthode d'identification qu'elle entend utiliser.

Une méthode de vérification de l'identité ayant recours à la biométrie doit offrir une méthode alternative dans le respect de la loi.

Secrets partagés pour l'identification au niveau d'assurance de l'identité moyen

20. Un secret partagé doit répondre aux caractéristiques suivantes :

1° il doit être constitué d'au moins 8 caractères alphanumériques, incluant minimalement 2 lettres, ou bien d'un minimum de 9 chiffres;
2° il peut être constitué ou dérivé d'une partie ou de la totalité d'un ou de plusieurs attributs de l'identité uniquement s'ils constituent moins de 50 % de la longueur du secret partagé et que le reste du secret est constitué de caractères alphanumériques aléatoires offrant au moins un million de combinaisons;
3° il ne doit pas être basé sur le nom ou la relation avec un membre de la famille;
4° le document émis sur lequel apparaît le secret partagé doit contenir au moins un numéro unique qui identifie la personne à laquelle il se rapporte;
5° le nom complet sur le document émis le concernant doit être le nom sous lequel la personne était officiellement connue au moment de sa transmission. Les pseudonymes, alias ou raccourcis, initiales du nom de famille ou initiales de tous les prénoms sont interdits;
6° le document émis le concernant doit être valide (non expiré, non falsifié ou non révoqué). Dans le cas où le secret partagé est émis régulièrement, le document doit avoir été émis dans les 24 mois précédant l'usage du secret partagé. Dans le cas où le secret découle d'une preuve d'identité, le secret est valide pour toute la période de validité de cette preuve;
7° il doit comporter un faible taux de compromission lors de vols connus de renseignements personnels.

Exemples de secrets partagés acceptables : le numéro de l'avis de cotisation émis par Revenu Québec, le numéro de l'avis pour l'émission du permis de conduire ou un numéro de dossier ou de membre relatif à une qualification professionnelle.

Exemples de secrets partagés non acceptables : le numéro de la carte d'assurance maladie, le numéro de permis de conduire, le nom de famille de la mère à sa naissance et le numéro d'assurance sociale (NAS) émis par le gouvernement du Canada.

21. Le mode de transmission du secret partagé doit permettre d'avoir l'assurance que la personne concernée qui reçoit le secret partagé est bien celle visée par la transmission qui lui en est faite. Par conséquent, la destination (ex. : adresse courriel, adresse postale, SMS) où sera acheminé le secret partagé doit correspondre à une destination déjà connue par au moins une source de confiance.

La transmission par courriel du secret partagé implique toutefois un risque élevé de compromission, car les services de courriel sont des cibles attrayantes pour les cybercriminels. Le mode de transmission à la personne concernée doit assurer l'intégrité et la confidentialité du secret partagé.

22. Advenant que la banque de données ou le registre d'un organisme contenant des informations utilisées comme secrets partagés par un service d'identification soit compromis ou exposé, de manière partielle ou totale, l'organisme doit :

1° appliquer son processus de gestion d'incidents pour gérer cette compromission;
2° s'assurer de prendre les mesures nécessaires pour qu'une vérification de toutes les identités qui ont été délivrées en utilisant un ou des secrets partagés possiblement compromis ou exposés soit réalisée;
3° cesser toute utilisation de ces secrets partagés pour la délivrance de nouvelle identité.

Advenant le cas où il n'y a pas suffisamment de secrets partagés pour procéder à une identification, il est possible de transmettre à la personne un code de vérification.

Code de vérification

23. Un code de vérification est une information transmise par l'organisme à une personne concernée, destiné à être utilisé une seule fois. Le code de vérification dans le cadre d'une identification peut être utilisé pour le remplacement d'un seul secret partagé. La transmission du code de vérification doit se faire à une destination déjà connue par au moins une source de confiance. Les modes de transmission permis sont par téléphone (SMS ou appel vocal) et par courrier.

24. Le code de vérification doit être composé d'au moins 6 caractères alphanumériques, incluant minimalement 2 lettres et être généré aléatoirement.

25. Le code de vérification ne peut pas être dérivé des attributs de l'identité ou d'une combinaison de ceux-ci, ni être généré en les utilisant.

26. Le code de vérification expire au plus tard après :

1° 15 jours s'il est transmis par courrier;
2° 30 minutes s'il est transmis par téléphone (SMS ou appel vocal).

SECTION IV
Authentification

27. La présente section apporte des précisions sur l'authentification visée à la sous-section 3 de la section III des Règles.

Elle s'adresse plus particulièrement aux contributeurs à un tel processus.

Précisions sur l'authentification pour une entreprise ou une autre entité

28. Une entreprise ou une autre entité ne peut pas s'authentifier sans l'intermédiaire d'une personne physique. Une entreprise ou une autre entité ne peut donc pas, sans une personne physique, accéder à son compte pour y effectuer des actions. Seules des personnes physiques qui sont les représentants dûment autorisés pourront utiliser leur

compte lié à celui de l'entreprise ou de l'entité concernée pour effectuer des actions dans le cadre de leur mandat.

Précisions sur les facteurs d'authentification

29. Lors d'un niveau d'assurance de l'identité **moyen** et en lien avec l'obligation d'utiliser une authentification multifacteur de base prévue aux Règles, il est nécessaire d'utiliser minimalement deux types de facteurs d'authentification différents.

En utilisant une authentification multifacteur de base, l'un de ces deux facteurs s'appuie sur un code à utilisation unique (facteur de type « ce que l'on possède »), transmis à la personne concernée par des modes qui peuvent inclure l'appel téléphonique (SMS ou appel vocal), le courriel ou le courrier.

30. Lors d'un niveau d'assurance de l'identité **élevé** et en lien avec l'obligation d'utiliser une authentification multifacteur avancée prévue aux Règles, il est nécessaire d'utiliser minimalement deux types de facteurs d'authentification différents.

Pour un facteur de type « ce que l'on possède », les méthodes considérées plus sécuritaires et autorisées sont les suivantes :

1° le jeton cryptographique;
2° le certificat;
3° le jeton logiciel;
4° le code à usage unique;
5° l'application sollicitant une approbation;
6° toute autre méthode jugée équivalente.

Pour un facteur de type « ce que l'on possède », les modes de transmission d'un code à utilisation unique interdits sont les suivants:

1° le SMS;
2° l'appel vocal;
3° la télécopie (fax);
4° le courriel;
5° le courrier.

31. Lors d'un niveau d'assurance de l'identité **très élevé**, en lien avec l'obligation d'utiliser une authentification multifacteur prévue aux Règles, il est nécessaire d'utiliser minimalement deux types de facteurs d'authentification différents dont l'un deux doit comporter un dispositif cryptographique. Ce dispositif cryptographique doit lui-même comporter un mécanisme d'activation manuel que déclenche la personne concernée. Cela implique que le dispositif cryptographique ne doit pas pouvoir être exécuté automatiquement, notamment lors de son insertion ou par une liaison sans fil de courte portée.

32. Le code d'authentification à usage unique est valide uniquement pour une durée de 15 minutes suivant son émission.

33. La méthode de génération du code d'authentification à usage unique ne doit pas s'appuyer sur les attributs de l'identité, ni sur des données statiques ou temporelles. Il est recommandé que le code à utilisation unique soit généré aléatoirement et composé d'un minimum de 8 caractères alphanumériques, incluant minimalement 2 lettres.

Connexion avec le plus haut niveau d'assurance

34. Afin d'offrir une expérience uniforme et la plus sécuritaire possible, l'authentification de la personne concernée accédant à un service numérique doit se faire selon le niveau d'assurance de l'identité atteint lors de sa vérification de l'identité, même si un tel service requiert un niveau inférieur. Il est toutefois accepté pour une personne ayant été identifiée à un niveau très élevé de lui permettre de s'authentifier à un niveau élevé pour accéder à des services de niveau élevé ou inférieur.

Durée maximale de session

35. Pour démarrer toute utilisation d'un service numérique, la personne concernée doit d'abord s'authentifier selon l'ensemble des exigences permettant de satisfaire le niveau d'assurance requis par le service. À la suite d'une authentification réussie avec succès, une session est créée.

36. Il est recommandé de mettre fin automatiquement à la session en cours et d'exiger une nouvelle authentification dans les cas suivants :

1° aucune activité n'est détectée pendant une période continue maximale de 30 minutes;
2° la session a été créée il y a plus de 8 heures.

SECTION V
Gestion des données d'identité et du dossier de preuve

Conservation et transmission : chiffrement et isolation des données

37. Toute information utilisée dans le processus d'identification et de représentation confiée par mandat ou procuration, incluant également les vidéos de vérification d'identité, constitue le dossier de preuve. Dans le respect de la loi, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), la présente section prévoit des dispositions au regard de la gestion des données et du dossier de preuve dans le contexte des Règles.

38. Afin de permettre une validation ultérieure que les demandes de vérification de l'identité ont été faites par la personne concernée et non par une personne autre que celle-ci, le dossier de preuve doit être conservé pendant une année complète à compter de la date de la désactivation d'un compte auquel ce dossier est lié.

39. Toutes les informations conservées dans le cadre des processus d'identification, d'authentification et les données du dossier de preuve doivent être conservées chiffrées et la clé de chiffrement doit être changée à une fréquence régulière. L'information conservée, appuyant l'identification ou l'authentification ou le dossier de preuve, devrait être sauvegardée de manière isolée des autres données de l'organisme, dans une infrastructure à cet effet ayant des contrôles de sécurité appropriés.

40. Afin de protéger les données et de limiter les risques de fraude ou d'action malveillante, toute transmission de données, dans le cadre de l'identification ou de l'authentification, doit être chiffrée selon un algorithme de chiffrement répondant à une norme reconnue et adéquate considérant leur degré de sensibilité.

Journalisation et notifications

41. Tout accès aux attributs de l'identité, aux secrets partagés, aux preuves de l'identité, aux dossiers de preuve et aux mandats ou aux procurations doit être contrôlé et journalisé. Les accès doivent être restreints aux personnes qui ont le besoin de connaître et ils doivent également être journalisés.

42. Le détenteur d'un compte doit être notifié de tout changement de renseignements personnels à ce compte (nom, mot de passe, information de contact, etc.) et, dans la mesure du possible, de toute activité jugée inhabituelle.

ANNEXE (article 4)

Type de préjudices	Exemples de préjudice de niveau faible	Exemples de préjudice de niveau moyen	Exemples de préjudice de niveau élevé	Exemples de préjudice de niveau très élevé
Préjudices pour les personnes physiques				
Perte financière		Perte pouvant causer du stress ou de l'inconfort	Perte pouvant affecter la qualité de vie, perte de crédit, de subvention, de prestation ou d'allocation	Perte pouvant compromettre la sécurité financière ou provoquer une faillite
Violation du cadre législatif et réglementaire		Infraction à une loi ou à un règlement, autre qu'une infraction criminelle, ayant une ou des conséquences à court terme, pouvant mener à une condamnation ou à une sanction modérée telle une amende peu élevée	Infraction à une loi ou à un règlement, incluant une infraction criminelle, entraînant des conséquences à moyen ou long terme, pouvant mener à une condamnation ou à une sanction importante telle une amende élevée, sans toutefois aller jusqu'à l'emprisonnement, une mesure disciplinaire, incluant la mise en accusation ou la formulation d'une plainte selon le cas	Infraction à une loi ou à un règlement, incluant une infraction criminelle, entraînant des conséquences permanentes, pouvant mener à une condamnation ou à une sanction très importante, une amende très élevée ou à l'emprisonnement, une mesure disciplinaire grave, incluant la mise en accusation ou la formulation d'une plainte selon le cas
Atteinte à l'identité ou à la protection des renseignements personnels (PRP) du citoyen concerné par le service	Impacts négligeables en raison d'une divulgation de renseignements personnels à caractère public	Modification de renseignements personnels à caractère public, incidences négatives découlant de l'utilisation de renseignements personnels à caractère public à d'autres fins que celles prévues ou autorisées	Divulgation de renseignements personnels, confidentiels ou sensibles, usurpation d'identité, modification de renseignements personnels, atteinte à la vie privée	Modification de renseignements confidentiels ou sensibles
Atteinte à l'identité ou à la protection des renseignements personnels (PRP) de plusieurs citoyens			Utilisation de renseignements personnels, confidentiels et sensibles à des fins autres que celles prévues ou autorisées	Modification ou divulgation de renseignements personnels, confidentiels ou sensibles, usurpation d'identité, atteinte à la vie privée
Atteinte au droit de la personne	Nuisance, pour un court terme, à la réputation ou à une situation sociale	Perte de confiance ou de privilège personnel pour un court terme	Perte d'emploi, atteinte au statut social	Perte de droits et libertés, exclusion sociale, radiation

Type de préjudices	Exemples de préjudice de niveau faible	Exemples de préjudice de niveau moyen	Exemples de préjudice de niveau élevé	Exemples de préjudice de niveau très élevé
Préjudices physiques ou psychologiques		Blessure mineure ne requérant pas de soins médicaux, stress, limitations temporaires à court terme	Blessure qui requiert des soins médicaux, détresse, limitations temporaires à moyen terme	Blessure grave, décès, maladie ou traumatisme psychologique, limitations permanentes
Préjudices pour les entreprises ou les autres entités				
Perte financière		Perte pouvant avoir une incidence sur le rendement	Perte pouvant réduire la compétitivité, perte de crédit ou de subvention, dévaluation	Perte pouvant compromettre la viabilité, entraîner une fermeture, provoquer une faillite
Violation du cadre législatif et réglementaire		Infraction à une loi ou à un règlement, autre qu'une infraction criminelle, entraînant des conséquences à court terme, pouvant mener à une condamnation ou à une sanction telle une amende	Infraction à une loi ou un règlement, incluant une infraction criminelle, entraînant des conséquences à moyen ou long terme, pouvant mener à une condamnation ou à une sanction telle une amende élevée, sans toutefois aller jusqu'à l'emprisonnement, mesure disciplinaire, saisie, mise en accusation ou la formulation d'une plainte selon le cas	Infraction à un loi ou à un règlement, incluant une infraction criminelle, entraînant des conséquences permanentes, pouvant mener à une condamnation ou à une sanction très importante, une amende très élevée ou à l'emprisonnement, une mesure disciplinaire grave, incluant la mise en accusation ou la formulation d'une plainte selon le cas
Renseignements personnels d'un employé ou d'un client	Impacts négligeables en raison d'un accès non autorisé à des renseignements personnels à caractère public	Modification de renseignements personnels à caractère public, incidences négatives par l'utilisation de renseignements à caractère public à d'autres fins que celles prévues ou autorisées	Divulgation de renseignements personnels, confidentiels ou sensibles, modification de renseignements personnels, atteinte à la vie privée	Modification de renseignements confidentiels ou sensibles
Renseignements personnels de plusieurs employés ou clients			L'utilisation de renseignements personnels et sensibles à d'autres fins que celles prévues ou autorisées	Modification ou divulgation de renseignements personnels, confidentiels ou sensibles, usurpation d'identité, atteinte à la vie privée
Renseignements confidentiels et secret professionnel		Modification de renseignements à caractère public	Divulgation de renseignements confidentiels de l'organisme ou d'un partenaire	Modification de renseignements confidentiels tel un secret de fabrication de l'organisme ou d'un partenaire

Type de préjudices	Exemples de préjudice de niveau faible	Exemples de préjudice de niveau moyen	Exemples de préjudice de niveau élevé	Exemples de préjudice de niveau très élevé
Atteinte à la réputation	Nuisance à la réputation, pour un court terme, dans l'espace public	Perte de confiance des employés	Perte de confiance de la clientèle, médiatisation négative, entraînant des conséquences graves	Perte de confiance généralisée, nationale ou internationale
Préjudices pour l'État				
Atteinte à l'identité ou à la protection des renseignements personnels (PRP) d'un citoyen	Impacts négligeables en raison d'une divulgation non autorisée de renseignements personnels à caractère public	Modification de renseignements personnels à caractère public, incidences négatives par l'utilisation de renseignements à caractère public à des fins autres que celles prévues ou autorisées	Divulgation de renseignements personnels, confidentiels ou sensibles, usurpation d'identité, modification de renseignements personnels, délivrance de fausses preuves à l'appui de l'identité	Modification de renseignements confidentiels ou sensibles, délivrance de fausses preuves d'identité essentielles
Atteinte à l'identité ou à la protection des renseignements personnels (PRP) de plusieurs citoyens			L'utilisation de renseignements personnels à des fins autres que celles prévues ou autorisées	Modification ou divulgation de renseignements personnels, confidentiels ou sensibles, usurpation d'identité, délivrance de fausses preuves essentielles ou à l'appui de l'identité
Préjudice sur la prestation de services	Incidence sur la performance du service	Incidence sur les résultats d'un service non essentiel	Viabilité d'un ou de plusieurs services non essentiels compromise, incidence sur les résultats d'un service essentiel	Viabilité d'un ou de plusieurs services essentiels compromise
Atteinte à la réputation		Légère perte de confiance des citoyens envers un organisme ou service	Importante perte de confiance des citoyens envers un ou plusieurs organismes ou services	Embarras hors Québec, relations fédérales-provinciales, diplomatiques et internationales compromises
Préjudice sur les missions du gouvernement		Entrave à l'établissement de politiques gouvernementales importantes	Entrave à l'application efficace de lois	Cessation des activités du gouvernement
Médiatisation		Médiatisation négative modérée	Médiatisation négative significative	Médiatisation négative causant une crise gouvernementale
Préjudice causé à l'économie du Québec		Incidence sur le rendement économique	Perte de la compétitivité à l'échelle nationale ou internationale	Secteurs économiques clés compromis

Indications d’application liées (s’il y a lieu) :

- Indication d’application « Notification lors d’accès ou de changements au compte d’un citoyen » (IA-SI-2020-010-OP) approuvée en février 2022, jusqu’à son abrogation.

Mots-clés : service | identification | authentification | preuve d’identité | besoin de confiance | niveau d’assurance de l’identité | atteinte à l’identité | source de confiance | vérification de l’identité | secret partagé | code de vérification | facteurs d’authentification | gestion des données d’identité | assurance de l’identité numérique