Ontario

Normes d’intégration des Données de la Fonction Publique de l’Ontario (FPO)

Ministère des Services au public et aux entreprises et de l’Approvisionnement

Octobre 2026

Table des matières

Introduction 4

Objet 5

Date d'entrée en Vigueur 5

Autorité Légale 5

Application 6

Portée 6

Renseignements Personnels Sur la Santé 7

Surveillance Indépendante 7

Examen Périodique 8

Principes d'intégration des Données 9

Termes 10

Définitions 10

Exigences Relatives à l'intégration des Données 14

Avant la Collecte et l'acquisition des Données 15

1. Gouvernance et Responsabilisation 15
2. Formation sur la Protection des Renseignements Personnels et la Sécurité 18
3. Gestion des Risques d'atteinte à la Vie Privée 20
4. Signalement des Atteintes à la Vie Privée 23
5. Contrôles de Sécurité et Gestion des Cyberrisques 25

Collecte et Acquisition des Données 28

6. Spécifications Relatives à la Légalité et à la Finalité 28
7. Minimisation des Données 29
8. Couplage des Données Respectant la Vie Privée 30

Avant la Divulgation des Données 31

9. Anonymisation 31
10. Ententes 32

Après la Divulgation des Données 33
11. Conservation et Destruction des Données 33
12. Production de Rapports Publics 34
13. Exigences Supplémentaires Relatives aux Services Extraministériels d'intégration des Données 34
14. Responsabilisation et Responsabilités 36
Annexe A: Lois, Instruments de Politique, Normes et Lignes Directrices Connexes 41

Introduction

Le gouvernement de l'Ontario recueille et gère un large éventail de données, notamment des renseignements personnels, afin d'offrir des services publics, d'administrer les programmes autorisés par la loi et de faire respecter les lois. Lorsque cela est autorisé, ces renseignements peuvent également servir à surveiller et à évaluer l'efficacité des initiatives gouvernementales. Bien que ces renseignements puissent fournir des informations utiles, leur utilité est limitée lorsqu'ils sont pris isolément.

Toutefois, la combinaison d'ensembles de données provenant de sources multiples pour créer des ensembles de données nouveaux et enrichis – un processus appelé *intégration des données* – peut accroître considérablement la valeur analytique de l'information et générer des connaissances qui seraient impossibles à obtenir à partir d'ensembles de données individuels seulement.

Lorsqu'elle est effectuée de façon appropriée, l'intégration des données permet de mieux comprendre les besoins sociétaux, aide à répondre à des questions complexes en matière de politiques, éclaire l'élaboration de politiques et favorise l'amélioration significative et continue des programmes et des services dans des domaines comme la santé, les services sociaux, le logement et l'éducation, en optimisant l'utilisation des données déjà disponibles.

Bien que l'intégration des données présente une grande valeur publique, elle peut aussi engendrer des risques pour la protection des renseignements personnels lorsqu'on combine des données concernant des personnes. Pour protéger la vie privée des personnes tout en favorisant des pratiques responsables d'intégration des données, le gouvernement de l'Ontario a modifié la *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (LAIPVP) en 2019, afin d'y inclure des exigences relatives à l'intégration de données responsable, sécurisée et respectueuse des renseignements personnels dans la partie III.1 de la LAIPVP.

Pour favoriser une intégration des données respectueuse de la vie privée, les Normes d'intégration des données de la fonction publique de l'Ontario (les « Normes »), établies en vertu de la partie III.1 de la LAIPVP, fournissent aux services d'intégration des données (SID) désignés un cadre complet et axé sur la protection de la vie privée, leur permettant d'assurer une intégration des données sécuritaire, sécurisée, respectueuse de la vie privée et responsable.

Cette approche favorise l'accès à des constatations opportunes, fiables et exploitables tirées de renseignements détenus par le gouvernement, tout en protégeant la vie privée et en maintenant la confiance du public.

Objet

Les normes définissent des exigences précises et des étapes pratiques essentielles qui obligent les services d'intégration des données (SID) à protéger la confidentialité et la sécurité des renseignements personnels tout au long du cycle de vie de l'intégration des données, depuis le lancement et l'approbation du projet jusqu'à la collecte et à l'acquisition des données, leur couplage et leur anonymisation, l'accès aux données et leur analyse ainsi que la production de rapports publics.

Les normes adoptent une approche de gestion des risques axée sur la protection des renseignements personnels dès la conception, exigeant que les SID intègrent les considérations relatives à la protection des renseignements personnels dans la planification, la conception, la gouvernance, la mise en œuvre et la gestion continue des activités d'intégration des données, des processus opérationnels et des systèmes informatiques.

En respectant ces normes, les SID veillent à ce que l'intégration des données soit gérée de manière à renforcer la confiance du public, à réduire les risques liés à la protection des renseignements personnels et à la sécurité, et à promouvoir la transparence et la responsabilisation du gouvernement.

Date d'entrée en Vigueur

Ces normes entrent en vigueur en octobre 2026 et remplacent les Normes d'intégration des données de la fonction publique de l'Ontario publiées en avril 2021.

Autorité Légale

Les normes sont établies par le directeur du numérique et des données (DND) en vertu du paragraphe 49.14(1) de la partie III.1 de la LAIPVP.

Les normes s'appliquent parallèlement à toutes les politiques, normes et directives applicables du gouvernement de l'Ontario en matière de gestion de l'information, de technologies de l'information, de cybersécurité, de protection des renseignements personnels et de conservation des documents, et elles doivent être interprétées conjointement avec celles-ci.

La mise en œuvre des normes doit être conforme aux obligations, restrictions et exigences juridiques en vigueur, notamment celles énoncées dans la LAIPVP, la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), la *Loi de 2006 sur les archives publiques et la conservation des documents*, la *Loi de 2017 contre le racisme*, et/ou toute autre loi et réglementation connexes applicables.

En cas de conflit entre les présentes normes et la LAIPVP, ses règlements, la LPRPS, la *Loi de 2006 sur les archives publiques et la conservation des documents*, la *Loi de 2017 contre le racisme* ou toute autre loi ou tout autre règlement applicable, les exigences juridiques ont préséance.

Application

Les présentes normes s'appliquent à tous les ministères et organismes externes désignés comme « service d'intégration des données » (SID) dans le *Règlement de l'Ontario 366/19* (Règl. de l'Ont. 366/19) : Intégration des données en vertu de la LAIPVP. Sont concernés:

- les services ministériels d'intégration des données (SMID);
- les services interministériels d'intégration des données (SIID);
- les services extraministériels d'intégration des données (SEID);

Tous les SMID, les SIID et les SEID (collectivement appelées les services d'intégration des données « SID ») sont tenus de se conformer aux présentes normes conformément au paragraphe 49.14(4) de la partie III.1 de la LAIPVP.

Ces normes ne s'appliquent pas aux activités de couplage de renseignements personnels qui sont régies par d'autres lois ou autorités légales en dehors de la partie III.1 de la LAIPVP (p. ex. l'intégration des données régie par la *Loi de 2017 sur la lutte contre le racisme*). Ces activités demeurent assujetties aux exigences, aux mesures de protection et aux limites prévues par les lois et les autorités juridiques qui leur sont applicables.

Les ministères qui ne sont pas désignés comme SID, mais qui effectuent des activités d'intégration de données en vertu d'autres autorités légales peuvent utiliser ces normes comme guide pour favoriser des pratiques uniformes, sécuritaires et respectueuses de la vie privée.

Portée

Les normes établissent les exigences applicables aux SID quant à la collecte, au couplage, à l'anonymisation, à l'utilisation, à la conservation et à l'élimination des renseignements personnels en vertu de la partie III.1 de la LAIPVP.

Les activités d'intégration des données ne peuvent être menées qu'aux fins autorisées en vertu de l'article 49.2 de la LAIPVP, plus précisément pour appuyer l'analyse relative à a) la gestion ou à l'affectation des ressources, b) la planification de la prestation des programmes et services offerts ou financés par le gouvernement de l'Ontario, c) l'évaluation de ces programmes et services. Les droits individuels à la protection des

renseignements personnels et l'intérêt public doivent être dûment évalués et protégés avant toute autorisation de collecte de données.

Les résultats de l'intégration des données ne seront pas utilisés pour identifier une personne ou un ménage, cibler des personnes, prendre des décisions au sujet de l'admissibilité individuelle à des services ou à des prestations, ou créer un désavantage pour certaines personnes ou certains groupes concernés. Les ensembles de données aux fins d'analyse seront anonymisés conformément aux exigences de la partie III.1 de la LAIPVP et des normes.

Renseignements Personnels Sur la Santé

La définition de renseignements personnels figurant au paragraphe 2(1) de la LAIPVP comprend les renseignements relatifs aux antécédents médicaux, psychiatriques ou psychologiques d'une personne. La partie III.1 de la LAIPVP autorise également, dans des circonstances précises, la collecte de renseignements personnels sur la santé auprès d'entités réglementées en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* aux fins d'intégration des données autorisées, sous réserve des conditions et restrictions établies à la partie III.1 de la LAIPVP et aux présentes normes. Par conséquent, les renvois aux renseignements personnels dans les présentes normes peuvent comprendre des renseignements personnels sur la santé, à moins que le contexte n'indique le contraire.

Surveillance Indépendante

Le bureau de la Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) assure une surveillance indépendante des institutions assujetties à la LAIPVP, ainsi que des SID exerçant leurs activités en vertu de la partie III.1 de la LAIPVP et des présentes normes.

La CIPVP peut évaluer la conformité des SID à la partie III.1 de la LAIPVP et aux normes, formuler des recommandations, émettre des ordonnances ou exiger des mesures correctives (p. ex. ordonner de mettre fin à la pratique ou aux procédures, de modifier la pratique ou les procédures, de détruire les renseignements personnels recueillis ou conservés en vertu de la pratique ou des procédures, de mettre en œuvre une nouvelle pratique ou de nouvelles procédures) afin d'assurer la conformité aux exigences en matière de protection des renseignements personnels énoncées à la partie III.1 de la LAIPVP et aux normes, conformément aux paragraphes de 49.12(1) à 49.12(7) de la partie III.1 de la LAIPVP.

La CIPVP peut également formuler des commentaires ou des recommandations concernant les incidences des activités d'intégration de données sur la protection des

renseignements personnels en vertu de la partie III.1 de la LAIPVP et des présentes normes, conformément au paragraphe 49.14(1) de la partie III.1 de la LAIPVP.

Examen Périodique

Le gouvernement de l'Ontario examinera périodiquement les normes afin de s'assurer qu'elles continuent de satisfaire aux exigences énoncées au paragraphe 49.14(1) de la partie III.1 de la LAIPVP. Le DND supervisera l'examen périodique. Toutes les parties concernées, les SID et la CIPVP seront consultés avant que toute modification importante ne soit apportée aux normes.

Principes d’intégration des Données

Les principes suivants visent à guider les SID dans l’interprétation et l’application des présentes normes.

Principe 1 – Actif Stratégique

Gérer l’information comme un actif stratégique afin d’en optimiser la valeur, l’utilisabilité et la prise de décisions fondées sur des données probantes.

Principe 2 – Responsabilisation

Protéger les renseignements personnels et les renseignements sensibles utilisés dans le cadre de l’intégration des données et assurer une responsabilisation claire quant à leur traitement approprié pendant les activités d’intégration des données.

Principe 3 – Intérêt Public

Entreprendre la collecte de données à des fins légitimes d’intérêt public et veiller à ce que les droits au respect de la vie privée des personnes concernées soient soigneusement évalués et protégés.

Principe 4 – Proportionnalité et Nécessité

S’assurer que toutes les activités d’intégration de données sont nécessaires aux fins autorisées, justifiées et proportionnelles à l’objectif analytique visé.

Principe 5 – Confidentialité des Données et Sécurité

Intégrer de solides contrôles de confidentialité et de sécurité tout au long du cycle de vie de l’intégration des données et protéger les renseignements personnels contre tout accès, divulgation, perte ou utilisation abusive non autorisés.

Principe 6 – Exactitude

Produire des extrants exacts, fiables et de grande qualité, et cerner et atténuer activement les préjugés, la discrimination et les inégalités.

Principe 7 – Transparence

Mener des activités d’intégration des données de façon transparente et faire preuve de responsabilisation pour soutenir et maintenir la confiance du public.

Termes

Les termes suivants sont utilisés dans l'ensemble des présentes normes pour indiquer le niveau d'obligation associé à une exigence:

Les SID doivent: une exigence obligatoire à respecter impérativement.

Les SID devraient: une exigence recommandée qu'on s'attend à voir respecter. Lorsqu'une autre approche est adoptée, la justification, les risques connexes et les approbations doivent être documentés.

Définitions

Les définitions suivantes visent à faciliter l'interprétation et de l'application uniformes des présentes normes. Lorsqu'un terme est défini dans la loi applicable, la définition législative prévaut.

Terme	Définitions
Cadre Supérieur Responsable	Un cadre au niveau du sous-ministre adjoint ou un directeur, ou son délégué, de l'organisation où se trouve le SID.
Ministère Responsable	Le ministère chargé d'établir des mécanismes de responsabilisation et de soutenir la gouvernance d'un service extraministériel d'intégration des données (SEID) en vertu de la partie III.1 de la LAIPVP.
Directeur du Numérique et des Données (DND)	Le directeur du numérique et des données est nommé en vertu du paragraphe 3(1) de la *Loi de 2019 pour des services simplifiés, accélérés et améliorés*.
Système Informatique d'intégration des Données	L'environnement technologique utilisé pour appuyer les activités d'intégration des données, y compris les infrastructures, les applications, les bases de données, les réseaux, le support de stockage et de sauvegarde, les contrôles de sécurité et les actifs informationnels connexes.
Activités d'intégration des Données	Collecte, utilisation, couplage, anonymisation, analyse, divulgation, conservation ou élimination de renseignements personnels en vertu de la partie III.1 de la LAIPVP aux fins autorisées énoncées à l'article 49.2 de la LAIPVP.
Service d'intégration des Données (SID)	Un SMID, un SIID et un SEID désigné en vertu du Règlement de l'Ontario 366/19 : Intégration des données effectuée en vertu de la LAIPVP.

Terme	Définitions
Renseignements Anonymisés	Les renseignements permettant d'identifier une personne ou qui pourraient raisonnablement servir à l'identifier ont été supprimés.
Anonymisation	Comme cela est décrit au paragraphe 49.1(2) de la partie III.1 de la LAIPVP, l'anonymisation est un processus visant à supprimer : • les renseignements qui identifient un particulier • les renseignements qui pourraient servir, seuls ou avec d'autres, à identifier un particulier d'après ce qu'il est raisonnable de prévoir dans les circonstances
Gestionnaire, SID	Le cadre désigné pour veiller au respect de la partie III.1 de la LAIPVP et des présentes normes, ainsi que des activités quotidiennes du SID.
Membre du SID	Dans le cas d'un SMID et d'un SIID, un agent, un employé ou un mandataire du ministère où se trouve le service et qui travaille au sein du service. Pour un SEID, un agent, un employé ou un mandataire de la personne ou de l'entité qui travaille au sein du service, tel que cela est défini à la partie III.1 de la LAIPVP.
Service Extraministériel d'intégration des Données (SEID)	Une personne ou une entité, ou une division administrative d'une personne ou d'une entité, qui est désignée comme unité extraministérielle d'intégration des données dans le Règl. de l'Ont. 366/19 : Intégration des données en vertu de la LAIPVP.
Personne Responsable de L'institution	Le ministre responsable du ministère où se trouve le SID chargé de surveiller l'administration et la conformité à la partie III.1 de la LAIPVP, à ses règlements et aux présentes normes.
Renseignements Tirés de Renseignements Personnels	Renseignements créés, transformés, liés, agrégés ou autrement tirés de renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP. Lorsque les renseignements personnels comprennent des renseignements qui identifient une personne ou des renseignements qui pourraient être utilisés, seuls ou en combinaison avec d'autres renseignements, pour identifier une personne en fonction de ce qui est raisonnablement prévisible dans les circonstances, elle demeure assujettie à la partie III.1 de la LAIPVP, aux normes et aux exigences législatives, réglementaires et pangouvernementales applicables en matière de protection des renseignements personnels, de sécurité, de conservation, d'élimination et de destruction.

Terme	Définitions
Service Interministériel d'intégration des Données (SIID)	Une division administrative d'un ministère qui est désignée comme un SIID dans le Règl. de l'Ont. 366/19 : Intégration des données en vertu de la LAIPVP.
Service Ministériel d'intégration des Données (SMID)	Une division administrative d'un ministère qui est désignée comme un SMID dans le Règl. de l'Ont. 366/19 : Intégration des données en vertu de la LAIPVP.
Partie III.1 de la LAIPVP	Partie III.1 Intégration des données de la *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (LAIPVP).
Essai de Pénétration	Méthode d'évaluation utilisée pour mettre à l'essai un système, une application ou un réseau afin de déterminer s'il existe des vulnérabilités qui pourraient être exploitées.
Renseignements Personnels	Renseignements concernant une personne identifiable au sens du paragraphe 2(1) de la LAIPVP.
Renseignements Personnels sur la Santé	Renseignements personnels sur la santé au sens du paragraphe 4(1) de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*.
Atteinte à la Vie Privée	Le vol, la perte ou la collecte, l'utilisation, la divulgation, la conservation ou l'élimination non autorisée de renseignements personnels contraires à la loi, aux présentes normes ou aux pratiques autorisées de gestion de l'information.
Évaluation des Facteurs Relatifs à la Vie Privée	Processus servant à déterminer, à évaluer et à gérer les risques d'atteinte à la vie privée associés à la collecte, à l'utilisation, à la divulgation, à la conservation ou à l'élimination de renseignements personnels.
Atteinte à la Sécurité	Incident qui compromet ou pourrait raisonnablement compromettre la confidentialité, l'intégrité ou la disponibilité des renseignements, des systèmes ou des services utilisés pour les activités d'intégration des données.

Terme	Définitions
Cadre Supérieur	Dans le cas d'un SEID, le responsable administratif de l'organisation ou un autre agent désigné dans le règlement comme cadre supérieur. Lorsqu'un SEID n'est pas une institution ou ne fait pas partie d'une institution, son cadre supérieur est réputé être le responsable de l'institution aux fins de la partie III.1 de la LAIPVP.
Évaluation des Menaces et des Risques	Processus servant à déterminer et à évaluer les menaces, les vulnérabilités et les risques qui pèsent sur les renseignements, les systèmes et les services, ainsi qu'à déterminer les mesures de protection appropriées.
Analyse des Vulnérabilités	Processus utilisé pour déterminer les faiblesses ou les lacunes existantes dans les efforts de protection d'un système d'information.

Exigences Relatives à l’intégration des Données

Cette section définit les normes obligatoires que les SID doivent respecter pour se conformer à la partie III.1 de la LAIPVP et pour assurer une intégration des données sécuritaire et respectueuse de la vie privée.

Les exigences s’appliquent à chaque étape de la gestion des renseignements personnels tout au long du cycle de l’intégration des données, depuis la planification et la préparation jusqu’à la collecte, au couplage à l’anonymisation, à l’analyse et à la production de rapports.

Ces normes doivent être lues et appliquées conjointement avec les exigences législatives et réglementaires applicables, ainsi qu’avec les politiques, les normes et les directives pertinentes du gouvernement de l’Ontario en matière de gestion de l’information, de technologies de l’information, de cybersécurité, de protection des renseignements personnels et de conservation des documents.

Ces normes sont appuyées par des outils, des lignes directrices, de la formation et des mécanismes d’assurance organisationnels qui favorisent la conformité continue, l’amélioration continue, la gestion des risques et la vérifiabilité.

Avant la Collecte et l'acquisition des Données

1. Gouvernance et Responsabilisation

1.1. Le SID doit établir des structures de responsabilités et de responsabilisation claires pour la bonne gestion et la conformité des activités d'intégration des données avec la partie III.1 de la LAIPVP, les présentes normes, les lois, règlements, politiques, normes et pratiques exemplaires applicables en matière d'intégration des données.

1.2. La personne responsable de l'institution gouvernementale ou le cadre supérieur responsable du ministère ou de l'organisation où se trouve le SID, ou son délégué, doit désigner un fonctionnaire de haut niveau (le « gestionnaire du SID ») chargé de surveiller la conformité à la partie III.1 de la LAIPVP, aux présentes normes et aux lois, règlements, politiques et normes applicables en matière d'intégration des données, ainsi que des activités quotidiennes du SID.

1.3. Le gestionnaire du SID doit s'assurer qu'avant d'entreprendre toute activité d'intégration des données, le SID se conforme à la partie III.1 de la LAIPVP, aux présentes normes, ainsi qu'aux lois, règlements, politiques, normes et pratiques exemplaires applicables en matière d'intégration des données.

1.4. En cas de non-conformité, le gestionnaire du SID doit veiller à ce que des mesures correctives appropriées et opportunes soient prises. Le gestionnaire du SID devrait consulter, au besoin, les gestionnaires de programme, les conseillers juridiques, les équipes chargées de la protection des renseignements personnels, de la sécurité et de la conservation des documents afin d'assurer l'application appropriée de toutes les dispositions de la partie III.1 de la LAIPVP et des présentes normes.

1.5. Le gestionnaire du SID doit s'assurer que les décisions, les processus décisionnels, les approbations et toute autre preuve de conformité à la partie III.1 de la LAIPVP et aux présentes normes sont documentés et conservés, et il doit être en mesure de produire ces preuves sur demande aux fins d'audit, d'examen, d'enquête ou de production de rapports. Ces preuves peuvent comprendre, par exemple, des attestations, des évaluations de la protection des renseignements personnels et de la sécurité, des politiques, des pratiques et des procédures.

1.6. Le gestionnaire du SID doit élaborer et documenter un processus impartial et confidentiel permettant aux membres du SID de signaler les lacunes ou les

déficiences opérationnelles, ainsi que les incidents réels ou soupçonnés de non-conformité à la partie III.1 de la LAIPVP et/ou aux présentes normes, sans crainte de représailles. La responsabilité d'enquêter sur les actes répréhensibles doit être déléguée à une partie indépendante du SID qui possède l'autorité, la capacité et l'expertise appropriées.

1.7. Le gestionnaire du SID doit attribuer les rôles et responsabilités pour toutes les activités d'intégration des données, notamment:

- Élaborer, mettre en œuvre, surveiller et mettre à jour, au besoin, les politiques, les procédures et les pratiques relatives aux activités d'intégration des données;
- Suivre les pratiques de couplage et d'anonymisation respectueuses de la confidentialité;
- Évaluer les risques liés à l'anonymisation;
- Signaler les atteintes à la vie privée et les incidents de sécurité;
- Résoudre les problèmes de qualité ou techniques;
- Appliquer les contrôles de divulgation;
- Superviser les évaluations de la protection des renseignements personnels et de la sécurité, ainsi que les ententes de partage de données.

1.8. Tous les membres du SID doivent signer une entente de confidentialité au début de leur emploi ou de toute autre relation avec le SID, et avant d'avoir accès à des renseignements personnels.

1.9. Au minimum, l'entente de confidentialité doit comprendre:

- La confirmation que les personnes qui signent l'accord de confidentialité sont membres du SID et les responsabilités associées à leur rôle particulier;
- Une exigence selon laquelle les membres du SID doivent se conformer à la partie III.1 de la LAIPVP, aux présentes normes et aux autres lois, règlements, politiques, normes et pratiques exemplaires applicables en matière d'intégration des données;
- Une reconnaissance que les membres du SID ont lu, compris et accepté de se conformer aux modalités de l'entente de confidentialité;
- Une explication des fins auxquelles les renseignements personnels peuvent être recueillis et de la façon dont ils peuvent être utilisés en vertu de la partie III.1 de la LAIPVP et des présentes normes;
- Les restrictions relatives à l'accès, à l'utilisation et à la divulgation des renseignements personnels;

- L’interdiction d’utiliser ou de tenter d’utiliser des renseignements anonymisés, seuls ou en combinaison avec d’autres renseignements, pour identifier une personne conformément à l’article 49.8 de la partie III.1 de la LAIPVP;
- L’exigence que les membres du SID avisent le gestionnaire du SID dès qu’ils en ont la possibilité raisonnable, d’une atteinte réelle ou soupçonnée à la vie privée ou à la sécurité;
- Le rôle des membres du SID dans la facilitation d’une demande d’accès à l’information ou de correction de renseignements, ou d’une plainte relative à la protection des renseignements personnels en vertu de la LAIPVP;
- L’obligation pour les membres du SID de restituer en toute sécurité tous les biens appartenant au SID, y compris tous les moyens d’accès physiques (p. ex. cartes d’identification ou d’accès et clés), au plus tard à la date de cessation de l’emploi ou de toute autre relation avec le SID, ou lorsque le gestionnaire du SID détermine que ces biens ou moyens d’accès physiques ne sont plus nécessaires à l’exercice des responsabilités liées à l’intégration des données.

1.10. Le gestionnaire du SID doit veiller à la conformité continue du SID à la partie III.1 de la LAIPVP et aux présentes normes en surveillant et en évaluant régulièrement les pratiques, les procédures, les contrôles de confidentialité et de sécurité du SID pour s’assurer qu’ils demeurent efficaces, appropriés et conformes, et qu’ils sont mis à jour au besoin.

1.11. Le cadre supérieur responsable du SID doit fournir une attestation annuelle de conformité au DND, au début de chaque exercice financier, confirmant que les pratiques d’intégration des données du SID ont été évaluées au regard de la partie III.1 de la LAIPVP et des présentes normes, et qu’elles sont conformes à toutes les exigences.

1.12. Les attestations de conformité doivent comprendre des renseignements précis concernant la conformité des SID à la partie III.1 de la LAIPVP et aux présentes normes, y compris, sans s’y limiter, un résumé de toutes les atteintes à la vie privée et plaintes reçues au cours de l’année précédente, ou une déclaration selon laquelle il n’y a pas eu de telles atteintes ou plaintes.

2. Formation sur la Protection des Renseignements Personnels et la Sécurité

2.1 Le gestionnaire du SID doit s'assurer que tous les membres du SID comprennent leurs responsabilités en matière de protection de la vie privée des personnes, ainsi que les mesures de protection et de contrôle disponibles pour protéger les renseignements personnels.

2.2 Tous les membres du SID, y compris les employés à temps plein, à temps partiel, temporaires et contractuels, doivent suivre avec succès une formation obligatoire sur la protection des renseignements personnels et la sécurité avant d'avoir accès à des renseignements personnels, puis des formations de recyclage annuelles.

2.3 La formation doit être adaptée aux activités d'intégration des données, tenir compte des risques particuliers en matière de protection des renseignements personnels et de sécurité associés à l'intégration des données, correspondre aux rôles spécifiques des membres du SID, faire l'objet d'un suivi, d'une documentation et d'une mise à jour au besoin.

2.4 À tout le moins, la formation initiale sur la protection des renseignements personnels et la sécurité devrait comprendre:

- Un aperçu des tâches et des responsabilités du SID en matière de protection des renseignements personnels et de sécurité en vertu de la partie III.1 de la LAIPVP, aux présentes normes et aux autres lois, règlements, politiques, normes et pratiques exemplaires applicables en matière d'intégration des données;
- Une explication des fins auxquelles les renseignements personnels peuvent être recueillis et de la façon dont ils peuvent être utilisés en vertu de la partie III.1 de la LAIPVP et des présentes normes;
- Les restrictions relatives à l'accès, à l'utilisation et à la divulgation des renseignements personnels;
- L'interdiction de réidentifier les renseignements qui ont été anonymisés;
- Les mesures de protection administratives, techniques et physiques mises en œuvre par le SID pour protéger les renseignements personnels contre le vol, la perte et la collecte, l'utilisation ou la divulgation non autorisées ainsi que contre la copie, la modification ou l'élimination non autorisées et

les tâches des membres du SID dans la mise en œuvre de ces mesures de protection;

- Les objectifs des avis de collecte, des ententes de partage de données et des rapports annuels, ainsi que leurs principales dispositions;
- Une explication des protocoles du SID relatifs aux atteintes à la vie privée et à la gestion des incidents de sécurité, ainsi que des tâches et responsabilités connexes imposées aux membres du SID en matière de repérage, de signalement, de confinement et de participation à l'enquête et à la correction des atteintes à la vie privée et des incidents de sécurité;
- Un processus visant à gérer une demande d'accès à l'information ou de correction de renseignements, ou une plainte relative à la protection des renseignements personnels déposée en vertu de la LAIPVP.

2.5 Une formation de recyclage annuelle sur la protection des renseignements personnels et la sécurité devrait comprendre les risques émergents en matière de protection des renseignements personnels et de sécurité, les développements technologiques, l'évolution des exigences juridiques et réglementaires, les politiques et normes du gouvernement de l'Ontario en matière de protection des renseignements personnels et de sécurité, ainsi que les pratiques exemplaires pertinentes aux activités d'intégration des données.

2.6 À tout le moins, la formation de recyclage annuelle sur la protection des renseignements personnels et la sécurité devrait porter sur ce qui suit :

- Toute nouvelle politique, norme, pratique et procédure en matière de protection des renseignements personnels et de sécurité, ainsi que les modifications importantes apportées aux politiques, normes, pratiques et procédures existantes en matière de protection des renseignements personnels et de sécurité;
- Tout changement pertinent survenu depuis la dernière formation, notamment les constatations et les recommandations faites découlant des évaluations de la protection des renseignements personnels et de sécurité, les audits, les enquêtes sur les atteintes à la vie privée, les incidents de sécurité, ainsi que les plaintes relatives à la protection des renseignements personnels;
- Les ordonnances, les décisions, les lignes directrices, les fiches d'information et les pratiques exemplaires publiées par la CIPVP.

2.7 Le gestionnaire du SID est chargé de veiller à ce que tous les membres du SID aient suivi la formation initiale et la formation de mise à jour annuelle en matière de protection de la vie privée et de sécurité.

3. Gestion des Risques d'atteinte à la Vie Privée

3.1 Les SID doivent veiller à ce que les risques d'atteinte à la vie privée soient repérés de façon proactive, atténués efficacement et surveillés en permanence.

3.2 Ils doivent effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) pour les infrastructures des TI, les processus opérationnels et les flux de données concernés par les activités d'intégration des données avant de recueillir des renseignements personnels.

3.3 Les SIDs doivent effectuer une EFVP propre au projet avant de recueillir des renseignements personnels ou documenter les raisons pour lesquelles une ÉFVP existante demeure suffisante pour les activités d'intégration des données proposées.

3.4 Les SID doivent mettre à jour une EFVP lorsque des modifications importantes sont apportées aux activités existantes du SID qui comportent des renseignements personnels, notamment:

a) L'utilisation d'une technologie ou d'un processus opérationnel nouveau ou modifié qui comprend la collecte, le couplage, l'anonymisation, l'accès ou la divulgation de renseignements personnels;
b) Un changement important aux fins pour lesquelles les renseignements personnels sont utilisés ou divulgués;
c) La participation de toute autre institution ou tierce partie dans le cadre d'une entente contractuelle ou d'une entente de partage de données avec le SID;
d) Les normes ou les modifications législatives à la partie III.1 qui ont une incidence sur la gestion des renseignements personnels;
e) Lorsque le gestionnaire du SID détermine qu'une EFVP est justifiée étant donné la complexité élevée ou les risques potentiels associés à l'utilisation des renseignements personnels.

3.5 Au minimum, une EFVP devrait comprendre :

- Une description du projet d'intégration des données ou du programme, du processus et des systèmes de TI évalués;
- La confirmation que la collecte, l'utilisation et la communication proposées de renseignements personnels sont autorisées en vertu de la partie III.1 de la LAIPVP;

- Les fins pour lesquelles des renseignements personnels seront recueillis, utilisés et couplés, conformément à l'article 49.2 de la partie III.1 de la LAIPVP;
- Une explication des raisons pour lesquelles la collecte de renseignements personnels est nécessaire, et des raisons pour lesquelles les fins visées ne peuvent raisonnablement être atteintes à l'aide de renseignements anonymisés, de renseignements agrégés ou de renseignements accessibles au public;
- La confirmation que la collecte de renseignements personnels est dans l'intérêt public, comme l'exige le paragraphe 49(4) 4. de la partie III.1 de la LAIPVP;
- Le ou les types de renseignements personnels qui seront recueillis, les sources à partir desquelles ils seront recueillis, la confirmation que ces sources sont autorisées en vertu des paragraphes 49.4(1) ou (2) de la partie III.1 de la LAIPVP, et s'ils seront couplés à d'autres renseignements, y compris la nature et les sources de ces renseignements;
- Une description de la façon dont les renseignements personnels circuleront dans le processus d'intégration des données, ainsi que les rôles précis des membres du SID qui auront accès à ces renseignements;
- Toute limitation ou restriction imposée à la collecte, à l'utilisation, au couplage ou à la divulgation de renseignements personnels et de renseignements tirés de renseignements personnels;
- Si les renseignements personnels seront anonymisés et le processus d'anonymisation qui sera utilisé pour réduire le risque de réidentification;
- La confirmation que l'avis concernant les renseignements personnels a été publié en ligne et qu'il répond aux exigences de l'article 49.10 de la partie III.1 de la LAIPVP;
- Les mesures et pratiques administratives, techniques et physiques qui seront utilisées pour protéger les renseignements personnels, les renseignements tirés des renseignements personnels et les renseignements anonymisés, ainsi qu'une évaluation des risques pour les personnes en cas de vol, perte ou utilisation ou divulgation non autorisée;
- Les mesures que le SID mettra en œuvre pour:
    a) Prévenir ou réduire la probabilité qu'un vol, une perte ou une utilisation ou divulgation non autorisée de renseignements personnels, de renseignements tirés de renseignements personnels et de renseignements anonymisés se produise

b) Atténuer les risques pour les personnes en cas d'un tel événement.

- La période pendant laquelle les renseignements personnels, les renseignements tirés des renseignements personnels et les renseignements anonymisés seront conservés.

3.6 Les SID doivent mettre en œuvre les mesures d'atténuation des risques définies dans l'EFVP avant la collecte de renseignements personnels ou, s'il n'est pas possible de mettre en œuvre des mesures d'atténuation avant la collecte des renseignements personnels, dans un délai raisonnable après cette collecte de renseignements.

3.7 Lorsqu'un SID détermine qu'une mesure d'atténuation recommandée ne sera pas mise en œuvre, il doit fournir la justification et déterminer tout risque résiduel lié à la protection des renseignements personnels, ainsi que les mesures d'atténuation de rechange adoptées pour atténuer efficacement ces risques.

3.8 Les SID doivent documenter les stratégies utilisées pour prévenir, réduire et atténuer les risques cernés et assurer le suivi de la mise en œuvre de toutes les recommandations de l'EFVP dans un plan d'atténuation des risques.

3.9 Lorsqu'une mise à jour est requise, les SID doivent inclure toutes les mesures de prévention et d'atténuation et d'atténuation supplémentaires nécessaires pour faire face aux risques nouveaux ou accrus.

3.10 Les SID doivent obtenir l'approbation de l'EFVP du cadre supérieur responsable du SID avant la collecte des renseignements personnels.

3.11 Les SID doivent fournir une copie de l'EFVP à la CIPVP, sur demande.

3.12 Le gestionnaire du SID doit établir un calendrier pour l'examen périodique de l'EFVP pour s'assurer que les mesures d'atténuation des risques demeurent à jour et efficaces.

4. Signalement des Atteintes à la Vie Privée

4.1 Les SID doivent identifier, atténuer et gérer rapidement les atteintes à la vie privée ou tout incident découlant du vol, de la perte, de l'utilisation, de l'accès ou de la divulgation non autorisés de renseignements personnels.

4.2 Les SID devraient élaborer un protocole d'intervention en cas d'atteinte à la vie privée afin de pouvoir traiter rapidement les incidents tels que les atteintes à la vie privée, les incidents de sécurité ou les vulnérabilités des systèmes.

4.3 Le protocole d'intervention en cas d'atteinte à la vie privée doit:

- Désigner les rôles et les suppléants responsables d'intervenir en cas de tels incidents;
- Définir et documenter l'ordre précis des étapes à suivre pour répondre aux incidents;
- Utiliser une matrice de transmission hiérarchique pour établir la gravité du problème au niveau d'intervention approprié;
- Établir des canaux de communication pour une notification efficace, notamment en précisant quand informer le conseiller juridique, l'équipe des TI et de la sécurité, la haute direction, les personnes concernées et la CIPVP;
- Inclure des procédures de confinement et de rétablissement immédiats;
- Documenter toutes les décisions, actions et notifications.

4.4 Les SID devraient organiser des exercices de simulation annuels pour simuler des incidents réels liés à la protection de la vie privée et veiller à ce que les membres des SID sachent exactement qui aviser en cas d'incident.

4.5 En cas d'atteinte à la vie privée mettant en cause des renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP, les SID doivent évaluer rapidement la nature et l'étendue de l'atteinte et déterminer si les obligations de notification prévues aux paragraphes 49.11(3) et (4) de la partie III.1 de la LAIPVP s'appliquent.

4.6 Si une notification est requise, les SID doivent aviser les personnes concernées et la CIPVP à la première occasion raisonnable et conformément aux exigences législatives prévues aux paragraphes 49.11(3) et (4) de la partie III.1 de la LAIPVP s'appliquent.

4.7 Les SID doivent assurer la coordination avec les équipes responsables de la cybersécurité, des technologies, de la protection des renseignements personnels, du service juridique et d'autres équipes pertinentes tout au long des activités d'intervention et de correction de l'atteinte à la vie privée, au besoin.

4.8 Si une atteinte à la vie privée survient chez un fournisseur tiers, les SID doivent collaborer avec le fournisseur dès que possible afin de remédier à l'atteinte et d'aviser les personnes concernées et la CIPVP, s'il y a lieu. Les SID demeurent responsables de veiller à ce que les mesures appropriées de confinement, d'enquête, de correction et de notification soient prises.

4.9 Les SID doivent effectuer une analyse des causes fondamentales après chaque atteinte à la vie privée pour déterminer les facteurs contributifs, évaluer l'efficacité des mesures d'intervention, mettre en œuvre des mesures correctives visant à prévenir la récurrence et faire le suivi d'indicateurs comme le délai de résolution et le taux de transmission hiérarchique afin d'améliorer les processus. Les leçons apprises devraient être consignées et intégrées, au besoin, dans les mécanismes de gouvernance, les programmes de formation, ainsi que dans les politiques et les procédures.

4.10 Les SID doivent tenir un registre de tous les vols ou pertes de renseignements personnels et de toutes les utilisations ou divulgations non autorisées par la partie III.1 de la LAIPVP et les présentes normes, y compris:

- La nature, la portée et le calendrier de l'atteinte, notamment la date de l'atteinte, si elle est connue, et la date à laquelle elle a été détectée, ainsi qu'un résumé de la façon dont elle a été découverte;
- Le type, la sensibilité et le volume de renseignements personnels en cause;
- Le nombre de personnes touchées, ou estimé, et une évaluation des préjudices réels ou potentiels découlant de l'atteinte (p. ex. vol d'identité, perte financière, atteinte à la réputation, discrimination ou perte de vie privée);
- Les mesures correctives prises ou prévues pour réduire et prévenir davantage l'accès, l'utilisation, la divulgation, la perte ou le vol non autorisés de renseignements personnels;
- Les conclusions et recommandations découlant de l'enquête;
- La notification de vol, de perte ou d'utilisation ou de divulgation non autorisée aux personnes concernées et à la CIPVP conformément aux paragraphes 49.11(3) et (4);

- Le nom et le rôle du ou des membres du SID responsables de la gestion de l'atteinte, de la mise en œuvre des mesures correctives et de la surveillance des activités de correction.

5. Contrôles de Sécurité et Gestion des Cyberrisques

Remarque: *Les présentes normes ne visent pas à dresser une liste exhaustive des contrôles de sécurité et des mesures de protection techniques que les SID doivent mettre en œuvre. Cette section présente un ensemble minimal d'exigences pour les SID qui doivent être complétées par les Normes de technologie de l'information du gouvernement de l'Ontario (NIT-GO), ainsi que par les politiques et les directives organisationnelles pertinentes.*

Il incombe au gestionnaire du SID d'examiner l'ensemble des exigences de sécurité à l'échelle de l'organisation pour les systèmes de TI pour l'intégration des données, y compris les évaluations des risques, le choix des mesures de protection et des contrôles, la surveillance continue, l'examen par la direction ainsi que l'amélioration et la surveillance continues.

5.1 Les SID doivent évaluer les risques liés à la protection des renseignements personnels et à la sécurité à toutes les étapes du cycle de vie de l'intégration des données et mettre en œuvre des mesures appropriées pour protéger l'information conformément aux contrôles de sécurité, aux mesures de protection techniques, aux politiques, aux directives et aux normes organisationnelles pertinentes.

5.2 Ils doivent s'assurer que leurs systèmes informatiques d'intégration des données sont harmonisés avec les architectures et les plateformes numériques, de données et de sécurité approuvées par l'organisation.

5.3 Les SID doivent mettre en œuvre des contrôles de sécurité et des mesures de protection techniques appropriés pour protéger les renseignements personnels, les renseignements tirés des renseignements personnels et les renseignements anonymisés. Les mesures de sécurité doivent être appropriées et proportionnelles au niveau de sensibilité des renseignements traités et conservés dans les systèmes de TI destinés à l'intégration des données.

5.4 Lorsque le SID n'est pas assujetti aux exigences, politiques et normes de sécurité informatique et de cybersécurité du gouvernement de l'Ontario, le ministère responsable doit évaluer l'équivalence des mesures de protection et

du modèle opérationnel, et documenter toute mesure d'atténuation requise avant le début de la collecte.

5.5 Les SID externes à la FPO doivent mettre en œuvre des contrôles de sécurité et des mesures de protection techniques équivalents ou supérieurs aux exigences de sécurité du Gouvernement de l'Ontario. Ces SID doivent être en mesure de démontrer leur conformité sur demande au moyen d'évaluations, d'attestations, d'audits et d'autres preuves acceptables par le gouvernement de l'Ontario.

5.6 Les SID doivent veiller à ce que tous les ensembles de données utilisés dans les activités d'intégration des données soient classifiés et traités conformément aux exigences de l'organisation en matière de classification de la sensibilité des renseignements.

5.7 Les renseignements personnels transmis et stockés qui ont été classés comme hautement sensibles doivent être protégés par chiffrement (en transit et au repos) d'un type et d'une force suffisants pour résister aux attaques conformément aux exigences générales de sécurité et de cryptographie de l'organisation. Les clés de chiffrement et les mots de passe doivent être protégés et gérés adéquatement.

5.8 Les SID doivent effectuer une évaluation des menaces et des risques (EMR) pour leurs systèmes informatiques d'intégration de données. Les SID doivent revoir et actualiser périodiquement l'EMR en cas de modification importante aux systèmes informatiques d'intégration de données, aux processus opérationnels, à l'environnement juridique ou de menace ou après des incidents de sécurité majeurs, dans le cadre de la gestion continue des risques et de la gouvernance de la sécurité, afin de garantir la validité et la pertinence de l'évaluation.

5.9 Les SID doivent effectuer des analyses de vulnérabilité et des tests d'intrusion conformément aux exigences de l'organisation pour repérer, évaluer, corriger, atténuer et surveiller en permanence les vulnérabilités des systèmes informatiques d'intégration de données.

5.10 Le gestionnaire du SID doit identifier et documenter les utilisateurs autorisés, leurs rôles et leurs privilèges d'accès connexes avant d'accorder l'accès aux systèmes informatiques d'intégration des données, conformément aux directives de l'entreprise en matière de gestion des identités et des accès.

5.11 Le gestionnaire du SID doit s'assurer que l'accès aux renseignements personnels, aux renseignements tirés des renseignements personnels, aux renseignements anonymisés et aux systèmes informatiques d'intégration des données est limité aux membres autorisés du SID qui ont besoin d'un accès pour exercer des fonctions liées aux activités d'intégration des données conformément au principe de privilège minimal.

5.12 Le gestionnaire du SID doit s'assurer qu'aucun membre du SID ne dispose d'un accès excessif aux renseignements personnels, aux renseignements tirés des renseignements personnels ou aux renseignements anonymisés au moyen de la séparation des tâches et la séparation fonctionnelle des rôles, afin de réduire la probabilité d'une modification non autorisée ou d'une autre mauvaise utilisation des renseignements.

5.13 Le gestionnaire du SID doit évaluer les cas où il est possible d'accorder l'accès à des données anonymisées plutôt qu'à des renseignements personnels afin de minimiser l'exposition à des renseignements sensibles, lorsque cela est possible sur le plan opérationnel.

5.14 Les SID doivent mettre en œuvre des journaux d'audit pour vérifier que seuls les utilisateurs autorisés accèdent aux renseignements personnels, aux renseignements tirés des renseignements personnels et aux renseignements anonymisés. Les renseignements recueillis et conservés dans les journaux d'audit doivent être conformes aux exigences de sécurité de l'entreprise.

5.15 Le gestionnaire du SID doit veiller à ce que les privilèges d'accès soient régulièrement examinés et révoqués lorsqu'ils ne sont plus nécessaires.

5.16 Les SID doivent élaborer et mettre en œuvre un processus de gestion des incidents de sécurité et définir clairement les rôles et les responsabilités du SID pour ce qui est de signaler les événements et les incidents de cybersécurité, conformément aux directives de l'entreprise relatives à la gestion de ces événements.

5.17 Toutes les atteintes à la sécurité soupçonnées ou confirmées mettant en cause des renseignements personnels, des renseignements tirés de renseignements personnels ou des renseignements anonymisés doivent être immédiatement signalées aux autorités compétentes de l'entreprise, conformément au

processus de gestion des incidents et de transmission hiérarchique à l'échelle de l'entreprise.

Collecte et Acquisition des Données

6. Spécifications Relatives à la Légalité et à la Finalité

6.1 Lorsque la collecte de renseignements personnels est autorisée en vertu de la partie III.1 de la LAIPVP, les SID doivent indiquer clairement leurs besoins en matière de renseignements et les fins auxquelles ils les recueillent.

6.2 Pour chaque nouveau projet d'intégration des données, les SID doivent évaluer, confirmer et documenter le fait que la collecte de renseignements personnels est nécessaire pour atteindre un ou plusieurs des objectifs énoncés à l'article 49.2 de la partie III.1 de la LAIPVP.

6.3 Les SID doivent évaluer si les fins précisées peuvent être raisonnablement atteintes à l'aide de renseignements existants anonymisés, de données agrégées ou de renseignements accessibles au public.

6.4 Les SID doivent confirmer et documenter que la collecte de renseignements personnels est d'intérêt public après avoir tenu compte des droits à la vie privée des personnes concernées et de la façon dont leurs renseignements personnels seront protégés, comme l'exige le paragraphe 49(4) 4. de la partie III.1 de la LAIPVP.

6.5 Les SID doivent s'assurer que les renseignements personnels ne sont recueillis qu'auprès des entités autorisées mentionnées à la partie III.1 de la LAIPVP et confirmer qu'aucune restriction ne s'applique à leur collecte. Les SID doivent documenter les sources de données, les propriétaires des données et les types de données recueillies pour chaque projet d'intégration des données.

6.6 Les SID doivent tenir compte des incidences sur le droit à la vie privée des personnes en effectuant des tests de nécessité, d'efficacité, de proportionnalité et d'intrusion minimale (le « test en quatre parties ») pour s'assurer que la collecte de renseignements personnels est justifiable.

6.7 Les SID doivent veiller à ce que tous les projets d'intégration des données comportant la collecte et le couplage de renseignements personnels reçoivent l'approbation requise du gestionnaire du SID ou du cadre supérieur responsable du SID avant le début du projet.

6.8 Les SID doivent publier une notification de collecte sur un site Web du gouvernement relativement à la collecte proposée de renseignements personnels en vertu de la partie III.1 de la LAIPVP. La notification doit respecter les exigences relatives au contenu de l'article 49.10 de la partie III.1 de la LAIPVP et être exacte, accessible et à jour.

7. Minimisation des Données

7.1 Les SID ne doivent pas recueillir de renseignements personnels en vertu de la partie III.1 de la LAIPVP ni utiliser ou divulguer ces renseignements si d'autres renseignements servent à des fins de collecte, d'utilisation ou de divulgation.

7.2 Les SID doivent prendre des mesures raisonnables pour veiller à ce que la quantité et le type de renseignements personnels recueillis dans le cadre des projets d'intégration des données soient réduits au minimum.

7.3 Lorsque la collecte de renseignements personnels est autorisée, le SID doit travailler avec l'entité requérante et le fournisseur de données afin de déterminer le type de renseignements personnels à extraire des systèmes sources et ainsi limiter la collecte aux renseignements les plus essentiels.

7.4 Les fichiers de données recueillis et stockés ne doivent contenir que les renseignements personnels pertinents requis pour appuyer l'objectif général de la collecte en vertu de la partie III.1 de la LAIPVP. Les renseignements personnels qui ne sont pas requis ne doivent pas être recueillis, transférés, copiés ou conservés au sein du SID.

7.5 Le SID devrait tenir un inventaire de tous les renseignements personnels recueillis et décrire les fins de la collecte, les éléments de données précis, les sources et les décisions relatives à la minimisation des données.

8. Couplage des Données Respectant la Vie Privée

8.1 Les SID doivent veiller à ce que les méthodes utilisées pour effectuer le couplage des données protègent la vie privée, et soient sécuritaires, robustes et fiables. Toutes les activités de couplage individuel au niveau des dossiers impliquant des renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP doivent être effectuées dans le ou les systèmes de TI pour l'intégration des données.

8.2 Les procédures techniques d'intégration des données doivent comporter des processus de travail clairement documentés, conformes aux exigences énoncées dans les présentes normes et la partie III.1 de la LAIPVP.

8.3 Les SID doivent établir et documenter le processus d'approbation requis pour les activités de couplage des données.

8.4 Les SID doivent s'assurer que les exigences en matière d'environnement de couplage sécurisé, de gouvernance et de mesures d'atténuation des risques sont en place, comme cela a été indiqué dans les sections précédentes.

8.5 Les SID doivent veiller à ce que les identifiants directs (p. ex. nom, date de naissance, ID) soient stockés et traités séparément des renseignements analytiques et des statistiques. Aucun membre du SID, à l'exception de l'administrateur du système, ne devrait avoir accès simultanément aux deux types de renseignements sans l'autorisation du gestionnaire du SID ou du cadre supérieur responsable du SID.

8.6 Les SID doivent remplacer les identifiants directs par une clé de couplage des données propre au projet dès que possible dans le flux du travail d'intégration des données. La clé de couplage et les tables de correspondance des identifiants associées doivent être conservées séparément des identifiants directs.

8.7 Les SID doivent mener des évaluations régulières de la qualité des processus de couplage pour repérer et atténuer les erreurs de couplage afin d'assurer l'exactitude des processus de couplage, la validité des analyses et l'interprétation des résultats.

Avant la Divulgation des Données

9. Anonymisation

9.1 Les SID doivent utiliser des méthodes d'anonymisation appropriées afin de garantir qu'aucune personne ne puisse être raisonnablement identifiée lors de la divulgation de renseignements anonymisés.

9.2 Les SID doivent utiliser des techniques d'anonymisation proportionnelles aux risques d'atteinte à la vie privée.

9.3 Les SID doivent tenir compte de facteurs tels que la sensibilité des données, le préjudice potentiel pouvant résulter de la réidentification, la granularité des données, leur divulgation publique et les informations accessibles au public qui pourraient être associées aux données et utilisées pour réidentifier des personnes, entre autres.

9.4 Les SID doivent déterminer le niveau acceptable de risque résiduel de réidentification pour chaque nouvelle divulgation de données, en tenant compte des facteurs mentionnés ci-dessus.

9.5 Les SID doivent réduire le risque de réidentifier la ou les personnes à partir des données, seules ou en combinaison avec d'autres sources d'information raisonnablement prévisibles, à un niveau acceptable.

9.6 Les SID doivent surveiller en permanence les risques de réidentification tout au long du projet d'intégration des données. Lorsque le risque de réidentification dépasse le seuil acceptable, les SID doivent mettre en œuvre des mesures d'atténuation appropriées et consulter les équipes chargées de la protection des renseignements personnels, de la sécurité et des affaires juridiques, au besoin.

9.7 Les SID doivent documenter les méthodes et les décisions d'anonymisation, les mesures de protection, les résultats de l'évaluation des risques de réidentification et les décisions approuvées relativement aux seuils de risque pour chaque nouveau projet d'intégration des données.

9.8 Les SID doivent veiller à ce que les techniques d'anonymisation demeurent efficaces, à jour et fiables au fil du temps grâce à une surveillance, à des améliorations et à des tests réguliers.

9.9 Les SID ne doivent pas divulguer de renseignements personnels, de fichiers de couplage ou tout renseignement qui pourrait raisonnablement permettre un couplage de dossiers ou une réidentification à l'extérieur du SID, sauf dans la mesure permise par l'article 49.9 de la partie III.1 de la LAIPVP.

10. Ententes

10.1 Lorsqu'ils partagent des renseignements anonymisés, les SID doivent s'assurer que les ententes de partage de données appropriées ont été mises en place avant la divulgation.

10.2 Les ententes de partage de données doivent décrire la façon dont l'entité destinataire protégera les renseignements anonymisés et inclure les procédures à suivre en cas d'atteinte à la vie privée ou d'incident de sécurité.

10.3 L'entente de partage de données doit également comprendre des dispositions interdisant à l'entité destinataire de réidentifier les personnes et divulguer ultérieurement des renseignements anonymisés.

10.4 En plus des exigences ci-dessus, l'entente de partage de données devrait comprendre des renseignements sur:

- Les institutions ou entités juridiques qui concluent l'entente de partage des données, y compris le type de SID, ainsi que les devoirs et responsabilités connexes en vertu de la partie III.1 de la LAIPVP;
- Les détails des renseignements anonymisés (p. ex. format de l'ensemble de données, volume, etc.) et les fins pour lesquelles ils seront divulgués;
- Le processus qui sera utilisé pour transférer en toute sécurité les renseignements anonymisés;
- La façon dont les renseignements anonymisés seront conservés en toute sécurité;
- La période de conservation pour les renseignements anonymisés, à savoir s'ils seront supprimés, détruits ou retournés de façon sécuritaire après l'expiration de la période de conservation, et le protocole obligatoire pour la suppression, la destruction ou le retour sécuritaires des renseignements anonymisés.

Après la Divulgation des Données

11. Conservation et Destruction des Données

11.1 Les SID doivent s'assurer que les renseignements personnels, les renseignements tirés des renseignements personnels et les renseignements anonymisés sont conservés et éliminés de façon sécuritaire conformément aux exigences législatives et aux politiques et normes de l'organisation.

11.2 Les SID doivent conserver les renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP, les renseignements tirés des renseignements personnels et les renseignements anonymisés conformément aux exigences législatives, à la politique de l'organisation et aux calendriers de conservation approuvés.

11.3 Les renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP doivent être conservés pendant au moins un an après leur dernière utilisation, ou conformément à une période de conservation approuvée, et ne doivent pas être conservés plus longtemps que nécessaire pour atteindre les fins autorisées en vertu de la partie III.1 de la LAIPVP.

11.4 Les SID doivent éliminer les renseignements personnels, les renseignements tirés des renseignements personnels et les renseignements anonymisés à l'expiration de la période de conservation, au moyen de processus d'élimination autorisés conformément aux exigences de l'organisation, aux calendriers applicables des dossiers et aux protocoles de destruction sécuritaire.

11.5 Les SID doivent documenter les décisions de destruction et les preuves à l'appui confirmant que les renseignements personnels sont conservés pendant au moins un an après la dernière utilisation, ou conformément à une période de conservation approuvée, et toutes les copies des renseignements ont été éliminées de façon sécuritaire de tous les systèmes de TI pour l'intégration des données, y compris les environnements des fournisseurs, après l'expiration de la période de conservation.

12. Production de Rapports Publics

12.1 Les SID doivent publier un rapport annuel décrivant la collecte, le couplage, l'utilisation, l'anonymisation, la divulgation et l'intérêt public des activités d'intégration de données sur un site Web du gouvernement de l'Ontario ou sur un site Web accessible au public pour un SEID, conformément aux paragraphes 49.13(1)(1.1) et (2) de la partie III.1 de la LAIPVP. Les rapports doivent être rédigés dans un langage clair et facile à comprendre.

12.2 Si une demande d'accès à l'information, une demande de correction ou une plainte relative à la protection des renseignements personnels est reçue, le SID doit collaborer avec le coordonnateur de l'accès à l'information pour coordonner une réponse appropriée, dans les meilleurs délais et conforme à la loi.

12.3 Lorsqu'une plainte relative à la protection des renseignements personnels fait état d'un risque potentiel pour la vie privée ou d'une non-conformité à la partie III.1 de la LAIPVP ou aux présentes normes, le SID doit documenter le problème, en évaluer les incidences et mettre en œuvre des mesures correctives ou d'atténuation appropriées.

13. Exigences Supplémentaires Relatives aux Services Extraministériels d'intégration des Données

Remarque: *Les services extraministériels d'intégration des données (SEID) peuvent exercer leurs activités en dehors du cadre législatif et stratégique du Gouvernement de l'Ontario, mais sont autorisés à recueillir, à utiliser, à coupler et à anonymiser les renseignements personnels en vertu de la partie III.1 de la LAIPVP. Par conséquent, des mesures de protection des renseignements personnels et de sécurité supplémentaires sont requises afin d'assurer des niveaux équivalents de protection des renseignements personnels, de sécurité, de responsabilisation et de transparence.*

Avant qu'un SEID recueille des renseignements personnels en vertu de la partie III.1 de la LAIPVP, le ministère responsable doit:

13.1 **Confirmer l'équivalence**
Évaluer et documenter le fait que la gouvernance, les mesures de protection, les processus et l'environnement technique du SEID offrent un niveau de protection

équivalent ou supérieur aux exigences de sécurité du gouvernement de l'Ontario.

13.2 **Établir des Ententes Officielles**
Conclure une entente écrite (p. ex. une entente de paiement de transfert, un contrat, un protocole d'entente ou un autre instrument exécutoire) qui énonce clairement les rôles, les responsabilités, les mesures de protection et les exigences en matière de conformité nécessaires à la protection des renseignements personnels recueillis en vertu de la partie III.1 de la LAIPVP.

13.3 **Définir les Exigences Applicables**
Dans l'entente, préciser les politiques, les normes et les mesures de protection que doit respecter le SEID, y compris les exigences en matière de confidentialité, de sécurité, de conservation des documents et de gestion des données, équivalentes aux attentes de la FPO, le cas échéant.

13.4 **Confirmer la Conformité :**
L'entente doit comprendre une confirmation de la conformité globale du SEID en vertu du paragraphe 49.14(4) avec l'objet, les fonctions et les exigences énoncés à la partie III.1 de la LAIPVP et des normes.

13.5 **Restreindre l'utilisation et L'accès**
Veiller à ce que les renseignements personnels soient recueillis, utilisés et divulgués uniquement aux fins autorisées en vertu de la partie III.1 de la LAIPVP, et interdire toute utilisation non autorisée.

13.6 **Environnement Sécurisé**
S'assurer que les renseignements personnels sont gérés dans des environnements sécurisés et cloisonnés de façon appropriée, avec des contrôles visant à empêcher tout accès, utilisation ou modification non autorisés.

13.7 **Établir des Exigences en Matière de Notification des Atteintes à la vie Privée et des Changements**
Exiger que le SEID signale immédiatement toute atteinte réelle ou soupçonnée à la vie privée ou à la sécurité et avise le ministère responsable de tout changement important aux processus opérationnels, au flux de données ou à l'infrastructure technique qui pourrait avoir une incidence sur la protection des renseignements personnels ou la sécurité.

13.8 **Pratiques D'audit**
Établir le droit du ministère responsable d'effectuer des audits périodiques ou discrétionnaires afin d'évaluer la conformité à la partie III.1 de la LAIPVP et aux

normes, et exiger que le SEID collabore pleinement à ces audits.

14. Responsabilisation et Responsabilités

14.1 Personne Responsable de L'institution (SMID, SIID)/Cadre supérieur (SEID)

Responsabilités:

- Veiller à ce que toutes les activités d'intégration des données menées par un SID désigné soient conformes à la partie III.1 de la LAIPVP, aux normes, aux lois, aux règlements, aux politiques, aux normes et aux pratiques exemplaires applicables.
- Dans le cas d'un SEID, assurer la conformité aux exigences établies par des ententes avec le ministère responsable, y compris les droits d'audit, les obligations de notification, les mesures de protection des renseignements personnels et les mesures de sécurité.
- S'assurer que la délégation de pouvoirs en vertu de la LAIPVP comprend les responsabilités en matière d'intégration des données.

14.2 Ministère Responsable (SEID)

Responsabilités:

- Établir des mécanismes de surveillance afin de garantir que le SEID maintient des protections équivalentes à la partie III.1 de la LAIPVP et aux normes.

14.3 Cadre Supérieur Responsable

Responsabilités:

- Veiller à ce que les renseignements personnels soient recueillis, utilisés, couplés, anonymisés, divulgués, conservés et éliminés conformément à la partie III.1 de la LAIPVP et aux normes, lois, règlements, politiques, normes et pratiques exemplaires applicables.
- Veiller à ce que les activités d'intégration des données soient entreprises conformément aux fins autorisées et dans l'intérêt public.
- Repérer et atténuer les risques liés à l'accès, à la protection des renseignements personnels, à la sécurité et à la conservation des documents dans l'ensemble des SID, et s'assurer que des mesures correctives sont prises en cas de non-conformité ou de risques pour la protection des renseignements personnels ou la sécurité.
- Dans le cas d'un SEID, assurer la conformité aux exigences établies par

des ententes avec le ministère responsable, y compris les droits d'audit, les obligations de notification, les mesures de protection des renseignements personnels et les mesures de sécurité.
- Fournir une attestation annuelle de conformité au DND, au début de chaque exercice financier, confirmant la conformité à la partie III.1 de la LAIPVP et aux normes.
- Approuver les EFVP pour les activités d'intégration des données.

14.4 **Gestionnaire, SID**

Responsabilités:

- Assurer la surveillance opérationnelle, la gestion de la conformité et la mise en œuvre des contrôles de protection de la vie privée et des mesures de sécurité au sein d'un SID.
- Assurer la conformité à la partie III.1 de la LAIPVP et aux normes relatives aux données, ainsi qu'aux politiques et normes applicables avant toute activité d'intégration des données.
- Établir et maintenir des politiques, procédures, contrôles et pratiques opérationnelles documentés pour soutenir des pratiques d'intégration des données respectueuses de la vie privée et sécurisées.
- Attribuer les rôles et les responsabilités pour le couplage des données, l'anonymisation, l'évaluation du risque de réidentification, la gestion des atteintes à la vie privée et les évaluations de sécurité.
- Veiller à l'exécution des ententes de confidentialité pour tous les membres du SID.
- Élaborer, mettre en œuvre et documenter la formation sur la protection des renseignements personnels et la sécurité pour tous les membres du SID.
- Veiller à ce que les évaluations de la protection des renseignements personnels, de la sécurité et des risques cybernétiques ainsi que les plans d'atténuation soient terminés avant le début des activités de collecte et de couplage des données.
- Gérer les atteintes à la vie privée, les incidents de sécurité, les obligations en matière de signalement, les mesures correctives et les notifications aux personnes concernées et à la CIPVP, le cas échéant.
- Tenir à jour les documents et les preuves de conformité aux fins des audits, des examens, des enquêtes et des rapports annuels.
- Collaborer avec la commissaire à l'information et à la protection de la vie privée de l'Ontario dans ses enquêtes sur les atteintes à la vie privée, le cas échéant.

14.5 **Membre d'un SID**

Responsabilités :

- Exécuter les activités d'intégration de données autorisées conformément à toutes les exigences, politiques et normes juridiques, de protection des renseignements personnels, de sécurité et opérationnelles applicables.
- Suivre les politiques, processus et procédures établis par le SID en ce qui a trait à la protection des renseignements personnels, à la sécurité, à l'anonymisation, etc.
- Protéger les renseignements personnels et les renseignements anonymisés contre l'accès, l'utilisation, la divulgation, la modification, la perte ou la destruction non autorisés.
- Signaler immédiatement tout incident réel ou soupçonné :
    - Atteintes à la vie privée
    - Incidents de sécurité
    - Lacunes opérationnelles
    - Cas de non-conformité à la partie III.1 de la LAIPVP, aux présentes normes, aux lois, aux politiques et autres normes applicables
- Suivre la formation obligatoire sur la protection des renseignements personnels en ce qui concerne les exigences et les pratiques exemplaires en matière d'intégration des données.
- Participer aux audits, aux examens et aux enquêtes, au besoin.

14.6 **Directeur du Numérique et des Données**

Responsabilités :

- Établir, tenir à jour et superviser les normes.
- Identifier et désigner un responsable au niveau des sous-ministres adjoints (SMA) chargé de s'acquitter de ces responsabilités. Si aucun SMA n'est délégué, ces responsabilités incombent au DND.
- Fournir aux SID une orientation, des conseils et une gouvernance à l'échelle de l'organisation.
- Recevoir et examiner les attestations de conformité annuelles des SID.
- Soutenir la mise en œuvre des présentes normes, notamment en fournissant les cadres, conseils, normes, orientations et outils nécessaires.
- Demander des renseignements aux SID, au besoin pour appuyer le DND

dans son rapport annuel à la CIPVP.
- Rendre compte annuellement, au besoin, à la CIPVP des activités des SID.
- Superviser l'examen périodique des normes et proposer des mises à jour au besoin.

14.7 **Directeur de l'information (DI)**

Responsabilités :

- Intégrer les risques, les considérations de conception et les exigences liés à l'information et aux données, notamment la protection des renseignements personnels, la sécurité de l'information, l'accès à l'information et la conservation des documents à la conception des projets technologiques et des approvisionnements du ministère, et veiller à leur mise en œuvre et à leur suivi.
- Intégrer les considérations et les exigences relatives à la conservation des documents, à l'accès et à la protection des renseignements personnels aux processus de gouvernance des projets de TI pour la conception et la prestation de systèmes, de services et de produits informatiques, y compris lors de l'acquisition de produits de tiers.
- Fournir aux responsables d'activité le soutien technique et logistique nécessaire à la mise en œuvre de cette politique.
- Appuyer la planification et la mise en œuvre des systèmes de gestion du contenu, et fournir un soutien continu lorsqu'ils sont déployés.
- Fournir tout le soutien nécessaire pour l'administration et la gestion des composantes des technologies de l'information des systèmes informatiques du ministère afin que les obligations en matière de conservation des documents, d'accès à l'information et de protection des renseignements personnels soient respectées.

14.8 **Responsable de la Sécurité des Systèmes d'information (RSSI)**

Responsabilités :

- Définir l'orientation, les normes et les directives de l'organisation en matière de cybersécurité pour les SID.
- Appuyer la détermination, l'évaluation et l'atténuation des risques liés à la sécurité et aux cyberrisques associés aux activités d'intégration des données.

- Soutenir les évaluations de sécurité, les interventions en cas d'incident et les mesures correctives liées aux activités des SID.
- Donner des conseils sur les mesures de sécurité et les contrôles nécessaires à la protection des renseignements personnels et des renseignements anonymisés.

14.9 Commissaire à l'information et à la Protection de la Vie Privée de l'Ontario (CIPVP)

Responsabilités :

- Assurer une surveillance indépendante et évaluer si les exigences de la partie III.1 de la LAIPVP et des normes sont respectées, au besoin.
- Exiger des mesures correctives, lorsque la partie III.1 de la LAIPVP l'autorise, pour régler les cas de non-conformité relevés lors des examens et des enquêtes.
- Formuler des commentaires ou des recommandations sur les incidences en matière de protection des renseignements personnels de toute question relative à la partie III.1 de la LAIPVP et aux normes.

Annexe A: Lois, Instruments de Politique, Normes et Lignes Directrices Connexes

La présente annexe fournit une liste non exhaustive des lois, règlements, instruments de politique, normes, directives et lignes directrices clés qui éclairent et appuient le travail des SID.

Lois	• *Loi de 2017 contre le racisme.* • *Loi de 2006 sur les Archives publiques et la conservation des documents.* • *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille* (partie X). • *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique.* • *Loi de 2004 sur la protection des renseignements personnels sur la santé.*
Règlements	• Règl. de l'Ont. 366/19 : Intégration des données en vertu de la LAIPVP • R.R.O. 1990, Règl. 460 : Dispositions générales en vertu de la LAIPVP • R.R.O. 1990, Règl. 459 : Disposition des renseignements personnels en vertu de la LAIPVP
Instruments de Politique Connexes	• Politique générale de conservation des documents, d'accès à l'information et de protection de la vie privée. • Politique générale relative à la cybersécurité et à la gestion des cyberrisques • Politique générale relative à la classification de la sensibilité des renseignements • Politique générale relative à l'assurance de l'identité et des justificatifs (AIJ) au sein du gouvernement de l'Ontario. Politique relative à l'infrastructure à clé publique du gouvernement de l'Ontario

	• Directive de l'Ontario sur les données et les services numériques • Politique sur l'utilisation acceptable des ressources en matière de technologie de l'information (TI). • Directive sur la gouvernance et la gestion des technologies de l'information. • Directive sur la gouvernance et la gestion des informations et ressources de données
Ressources de Gestion des Risques de la FPO	• Directive sur la gestion globale des risques. • Méthodologie d'évaluation des risques.
Normes de Sécurité de la FPO	• NIT-GO 25.0 Exigences générales de sécurité • NIT-GO 25.1 Exigences de sécurité relatives aux routeurs et aux commutateurs. • NIT-GO 25.5 Exigences de sécurité relatives aux réseaux locaux sans fil. • NIT-GO 25.6 Exigences de sécurité relatives aux pare-feu. • NIT-GO 25.7 Exigences de sécurité relatives aux services d'accès à distance. • NIT-GO 25.8 Exigences de sécurité relatives aux serveurs. • NIT-GO 25.10 Exigences de sécurité aux appareils mobiles. • NIT-GO 25.11 Exigences relatives à la conception en matière de sécurité • NIT-GO 25.12 Exigences de sécurité relatives à l'utilisation de la cryptographie. • NIT-GO 25.13 Exigences de sécurité relatives aux applications Web. • NIT-GO 25.18 Normes relatives à la sécurité physique des centres de données. • NIT-GO 25.20 Rapports d'élimination, de perte et d'incident des dispositifs informatisés et des supports de stockage. • NIT-GO 25.21 Principes et exigences pour la sécurité en matière de services infonuagiques.

	• NIT-GO 35 Norme de gestion des changements organisationnels dans la fonction publique de l'Ontario. • NIT-GO 37 Processus de gestion des incidents organisationnels. • NIT-GO 42 Exigences de sécurité relatives à la gestion des vulnérabilités organisationnelles.
Normes Connexes de la FPO	• Normes relatives aux données sur l'antiracisme - Normes relatives aux données en vue de repérer et de surveiller le racisme systémique.
Directives de la FPO	• Documents d'orientation de la FPO sur les évaluations de l'impact sur la protection de la vie privée (EIPV) pour les institutions visées par la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) 2025. • Documents d'orientation de la FPO sur le signalement des atteintes à la vie privée pour les institutions visées par la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) 2025
Directives de la CIPVP	• Lignes directrices du CIPVP sur la dépersonnalisation des données structurées (2025). • CIPVP - Planifier pour réussir : guide d'évaluation de l'impact sur la vie privée pour les institutions publiques de l'Ontario (2025)