BUREAU DES NORMES ORGANISATIONNELLES

POLITIQUE CPS-1001

Titre :

POLITIQUE ENCADRANT LA PROTECTION ET LA SÉCURITÉ DE L'INFORMATION

Date d'entrée en vigueur :
2012-03-01

Responsable :
Responsable de la surveillance de l'information

Thème et sous-thème :
Protection et sécurité de l'information

Adoptée par :
Conseil d'administration

Date de la dernière adoption :
2022-09-29

INTRODUCTION

Contexte

Pour remplir sa mission, Revenu Québec recueille, produit et utilise une information abondante. Cette information est principalement constituée de renseignements sur sa clientèle (citoyennes, citoyens, entreprises, représentants et partenaires) et les membres de son personnel. Ces renseignements sont soumis à des règles de protection légales.

Cette information peut revêtir une importance stratégique pour Revenu Québec ou pour l'État. De plus, elle peut présenter une valeur légale, administrative, économique ou patrimoniale. En conséquence, elle est une ressource essentielle qu'il convient de protéger et de sécuriser durant tout son cycle de vie. La protection des renseignements confidentiels (PRC) et la sécurité de l'information (SI) constituent les principaux volets de la protection et la sécurité de l'information (PSI). Ces volets sont complétés par la gouvernance et la valorisation de l'information.

Pour traiter cette information, Revenu Québec fait largement appel aux technologies de l'information, qui sont intégrées à ses processus opérationnels. Il effectue également des échanges électroniques avec ses partenaires, ses mandataires et ses fournisseurs de services, en plus d'offrir des services en ligne à sa clientèle, aux représentants ainsi qu'au personnel de ceux-ci. Enfin, il fournit des services à d'autres ministères et organismes. Pour toutes ces raisons, la protection de son infrastructure technologique est primordiale.

Conscient de la valeur de l'information qu'il détient, Revenu Québec doit en assurer la protection et la sécurité. Il doit également veiller au respect de la vie privée de sa clientèle. Dans ce contexte, il est important d'établir des orientations stratégiques à ce sujet et de communiquer les principes directeurs de l'organisation en matière de PSI.

Champ d'application

Cette politique porte sur la PSI et couvre tout le cycle de vie de l'information, de sa collecte ou de sa création jusqu'à son archivage ou à sa destruction. Elle vise les informations suivantes :

- l'information détenue ou utilisée par Revenu Québec, peu importe sa nature, sa localisation et le support sur lequel elle se trouve;
- l'information confiée à des tiers et toute forme d'échange, y compris l'information échangée dans le cadre de la prestation électronique de services;
- l'information qui est confiée à Revenu Québec par un ministère, un organisme ou un gouvernement, dans le cadre d'un mandat.

Cette politique s'adresse à tous les membres du personnel[1] de Revenu Québec, à ses partenaires, à ses mandataires et à ses fournisseurs de services. Elle doit notamment être considérée dès l'étape de conception d'un processus ou d'un système d'information, lors de l'élaboration d'ententes ou de l'acquisition d'une solution technologique, ou encore lors de la modification d'un de ces éléments.

1. Pour l'application de cette politique, par *membres du personnel*, on entend les dirigeants et les employés tels qu'ils sont définis dans le *Code de déontologie à l'intention des dirigeants et des employés* (CRH-4501). Le mot *dirigeant* désigne la personne nommée à titre de présidente-directrice générale ou de président-directeur général, les personnes nommées à titre de vice-présidentes et directrices générales ou de vice-présidents et directeurs généraux, de directrices générales ou de directeurs généraux ainsi que tous les gestionnaires de Revenu Québec. Pour ce qui est du mot *employé*, il désigne toute personne faisant partie de l'effectif de Revenu Québec et travaillant à temps plein ou à temps partiel à titre permanent, temporaire, occasionnel, saisonnier ou étudiant.

Dispositions légales et réglementaires

Les lois, règlements et décrets applicables à Revenu Québec sont notamment les suivants :

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) [Loi sur l'accès]
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1)
- Loi sur les archives (RLRQ, chapitre A-21.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03) [LGGRI]
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 2)
- Directive gouvernementale sur la sécurité de l'information (décret n° 1514-2021 du 8 décembre 2021)

Les régimes particuliers applicables à Revenu Québec sont notamment les suivants :

- Loi sur l'administration fiscale (RLRQ, chapitre A-6.002) [LAF]
- Loi sur l'Agence du revenu du Québec (RLRQ, chapitre A-7.003)
- Loi sur les biens non réclamés (RLRQ, chapitre B-5.1)
- Loi facilitant le paiement des pensions alimentaires (RLRQ, chapitre P-2.2)

ÉNONCÉ DE LA POLITIQUE

Objectifs

Cette politique démontre l'engagement de Revenu Québec à l'égard de la PSI. Elle constitue le fondement de la documentation normative en matière de PSI et vise les objectifs suivants :

- assurer la PSI tout le long du cycle de vie de l'information, conformément aux obligations légales auxquelles Revenu Québec est assujetti;
- établir et communiquer les orientations stratégiques de Revenu Québec en matière de PSI;
- renforcer la relation de confiance entre Revenu Québec et sa clientèle;
- définir les principes directeurs en matière de PSI devant guider les membres du personnel en vue d'assurer la confidentialité, la disponibilité et l'intégrité de l'information ainsi que de prévenir toute atteinte aux règles visant la PRC;
- responsabiliser les membres du personnel afin de minimiser les risques liés à la PSI.

Orientations et principes directeurs

Les énoncés qui suivent constituent les orientations (O) et les principes directeurs (P) de la PSI.

Ils s'inspirent des meilleures pratiques dans le domaine, notamment de la suite de normes ISO/CEI 27 000 et de celles du National Institute of Standards and Technology (NIST), en particulier les *Cyber Security Framework* (NIST CSF) et *Privacy Framework* (NIST PF). Ils visent à assurer la PSI tout le long du cycle de vie de l'information.

O1. Renforcer la confiance entre Revenu Québec et sa clientèle

P1. La PSI est assurée tout le long du cycle de vie de l'information.

P2. La PSI doit contribuer au renforcement de la relation de confiance entre Revenu Québec et sa clientèle, tout en favorisant l'utilisation des services offerts à celle-ci et à ses représentants.

O2. Responsabiliser tous les intervenants

P3. La PSI est appuyée par la haute direction, et l'engagement de cette dernière à cet égard doit se refléter aux différents paliers de l'organisation.

P4. Les responsabilités relatives à la PSI, à Revenu Québec, incombent à tous les membres du personnel, aux partenaires, aux mandataires et aux fournisseurs de services.

O3. Assurer une saine gouvernance et une saine gestion de la PSI

P5. La gouvernance et la gestion de la PSI sont encadrées et assurées par la personne désignée à titre de responsable de la surveillance de l'information (RSI), suivant une délégation par la personne nommée à titre de présidente-directrice générale ou de président-directeur général (PDG). La PSI repose sur une approche globale, concertée et intégrée de la PRC et de la SI.

P6. La personne désignée à titre de chef délégué de la sécurité de l'information ou de cheffe déléguée à la sécurité de l'information (CDSI) est responsable d'assurer la mise en œuvre de la gouvernance et de la gestion de la SI. La personne désignée à titre de responsable de l'accès à l'information et de la protection des renseignements confidentiels (RAIPRC) est responsable d'assurer la mise en œuvre de la gouvernance et de la gestion de la PRC. La personne désignée à titre

de responsable de la gouvernance et de la valorisation de l'information (RGVI) est responsable d'assurer la mise en œuvre de la gouvernance et de la valorisation de l'information, responsabilité qui inclut la gestion de l'information.

P7. Le comité organisationnel stratégique en protection et sécurité de l'information (COSPSI), qui est de niveau stratégique, et le comité organisationnel d'intégration en protection et sécurité de l'information (COIPSI), qui est de niveau tactique, soutiennent la personne nommée à titre de PDG dans l'exercice de ses responsabilités et l'exécution de ses obligations en lui fournissant l'assurance raisonnable qu'une saine gouvernance et une saine gestion de la PSI sont en place au sein de Revenu Québec.

O4. Gérer les risques et garantir un niveau approprié de PSI

P8. L'information doit être protégée et sécurisée conformément aux exigences de confidentialité, de disponibilité et d'intégrité.

P9. À l'exception d'exigences légales précises, le choix des mesures de PSI doit s'appuyer sur une évaluation des menaces et des risques auxquels l'information peut être exposée.

P10. Les risques liés à la PSI doivent être gérés et maintenus à un niveau acceptable pour l'organisation.

O5. Assurer la SI

P11. La confidentialité, la disponibilité et l'intégrité de l'information doivent être assurées tout le long de son cycle de vie.

P12. La collecte et la rectification de l'information s'effectuent auprès de sources fiables en vue d'en garantir la qualité.

O6. Assurer la PRC et le respect de la vie privée

P13. La PRC et le respect de la vie privée, qu'ils portent sur la clientèle ou un membre du personnel, doivent être assurés tout le long du cycle de vie de l'information visée, conformément aux exigences légales et en fonction du niveau de sensibilité.

P14. Les partenaires, les mandataires et les fournisseurs de services ayant accès à une information détenue par Revenu Québec ou ayant à l'utiliser doivent offrir un niveau de PSI au moins équivalent à celui de Revenu Québec.

P15. Les renseignements provenant d'autres ministères, organismes ou gouvernements, obtenus en vertu d'une loi, doivent être protégés et sécurisés conformément aux lois applicables, ainsi qu'aux exigences internes en matière de SI, en vue de préserver leur confidentialité, leur disponibilité et leur intégrité.

P16. Une évaluation des facteurs relatifs à la vie privée doit être effectuée lorsque requise, conformément aux obligations légales en vigueur auxquelles Revenu Québec est assujetti**.**

O7. Assurer le contrôle et la traçabilité des accès

P17. Les accès aux systèmes d'information ou à tout autre actif informationnel sont contrôlés rigoureusement afin que seuls les accès nécessaires soient accordés aux membres du personnel, dans le cadre des tâches qu'ils exercent et qui sont liées à la mission de l'organisation.

P18. Les accès aux systèmes contenant des renseignements confidentiels sur la clientèle et les membres du personnel sont journalisés en vue d'en garder la trace aux fins de vérification.

O8. Protéger l'infrastructure technologique et sécuriser les communications

P19. La gestion et l'exploitation de l'infrastructure technologique se font de façon sécuritaire pour répondre aux besoins en matière de PSI.

P20. Les communications internes et externes doivent être sécurisées adéquatement, peu importe le support ou le moyen de communication utilisé, en vue de protéger l'information qu'elles contiennent.

O9. Donner accès aux documents ou aux renseignements en toute sécurité

P21. Les documents ou les renseignements demandés en vertu d'une loi sont rendus accessibles de manière sécuritaire en vue de préserver leur confidentialité et leur intégrité.

O10. Assurer la gestion de l'information

P22. L'information reçue ou produite par Revenu Québec est organisée et gérée de manière à en faciliter l'accès, la consultation, le repérage, l'archivage et la diffusion de façon sécuritaire.

P23. Lorsque les fins pour lesquelles une information a été recueillie ou utilisée sont accomplies, elle doit être détruite, conformément aux obligations légales en vigueur auxquelles Revenu Québec est assujetti.

O11. Assurer la sécurité physique de l'information

P24. L'information détenue par Revenu Québec, peu importe son support, est protégée physiquement contre les accès non autorisés et les menaces intentionnelles, accidentelles ou catastrophiques.

O12. Intégrer la PSI dans le plan de continuité des activités

P25. La PSI est intégrée dans le processus de gestion du plan de continuité des activités de l'organisation.

O13. Gérer les événements et les incidents liés à la PSI

P26. Les événements et les incidents liés à la PSI doivent être gérés selon une approche cohérente et efficace afin que leur détection, leur signalement et leur traitement soient effectués dans les meilleurs délais.

P27. Afin de soutenir la personne nommée à titre de PDG et les autorités, dans tous les cas où survient un incident en PSI dont la gravité est considérée comme étant élevée ou très élevée, un comité de crise en PSI (CCPSI) est mis en place et coordonné par la personne désignée à titre de RSI, avec la collaboration des personnes désignées à titre de CDSI et de RAIPRC. Dans tous les autres cas, la personne désignée à titre de RSI peut mettre en place le CCPSI s'il le juge opportun.

P28. Un registre des événements de sécurité et un registre des incidents de confidentialité doivent être tenus et maintenus à jour. Ceux-ci sont sous la responsabilité de la personne désignée à titre de RSI.

O14. Former et sensibiliser les membres du personnel

P29. Les membres du personnel de l'organisation ainsi que les ressources externes doivent être sensibilisés à la PSI et être formés à ce sujet. Ils doivent également être informés de leurs responsabilités et être outillés pour les exercer.

O15. Gérer la conformité et les exceptions

P30. La conformité aux obligations légales, réglementaires et contractuelles, ainsi qu'aux exigences normatives de Revenu Québec, doit être garantie et vérifiée régulièrement.

P31. Les exceptions à la politique ou à tout document qui en découle, lesquelles sont autorisées par la personne désignée à titre de RSI, doivent faire l'objet d'une évaluation des risques et être gérées conformément aux seuils organisationnels de tolérance aux risques.

O16. Droit de regard et sanctions

P32. Revenu Québec a un droit de regard sur l'accès, l'utilisation et la communication de l'information qu'il détient.

P33. Toute personne (notamment les membres du personnel, les partenaires, les mandataires et les fournisseurs de services) qui enfreint une règle relative à la PSI, notamment en utilisant, en consultant ou en communiquant de façon non autorisée un renseignement **contenu dans un dossier fiscal** est passible de sanctions pénales, conformément aux articles 71.3.1, 71.3.2 et 71.3.3 de la LAF, en plus d'être passible de mesures administratives ou de sanctions disciplinaires.

P34. Les membres du personnel qui enfreignent une règle relative à la PSI, notamment en consultant, en utilisant ou en communiquant de façon non autorisée un renseignement personnel **non contenu dans un dossier fiscal** sont passibles de mesures administratives ou de sanctions disciplinaires.

P35. Les partenaires, les mandataires et les fournisseurs de services sont passibles, en cas d'infraction, de mesures administratives, telles que la résiliation du contrat des personnes qui travaillent pour leur compte.

RÔLES ET RESPONSABILITÉS

Conseil d'administration

Le conseil d'administration établit les orientations stratégiques de Revenu Québec, s'assure de leur mise en application et s'enquiert de toute question qu'il juge importante. Dans ce contexte, il adopte la *Politique encadrant la protection et la sécurité de l'information* (CPS-1001).

Comité des technologies de l'information et comité de gouvernance et d'éthique

Dans le cadre de cette politique, le comité des technologies de l'information (CTI) et le comité de gouvernance et d'éthique (CGE) exercent notamment les responsabilités suivantes :

- examiner la politique;
- recommander au conseil d'administration l'adoption de la politique.

Comité organisationnel stratégique en protection et sécurité de l'information

Dans le cadre de cette politique, le COSPSI exerce notamment les responsabilités suivantes :

- examiner la politique;
- recommander la transmission de la politique au CTI et au CGE pour examen;
- assumer le rôle d'instance décisionnelle stratégique chargée notamment de prendre position sur les préoccupations, les enjeux et les risques organisationnels liés à la PSI.

Comité organisationnel d'intégration en protection et sécurité de l'information

Dans le cadre de cette politique, le COIPSI exerce notamment les responsabilités suivantes :

- examiner la politique;
- recommander la transmission de la politique au COSPSI pour examen;
- assumer le rôle de forum de concertation et d'échanges sur les préoccupations, les enjeux et les risques organisationnels liés à la PSI.

Personne nommée à titre de présidente-directrice générale ou de président-directeur général (en tant que première dirigeante)

Dans le cadre de cette politique, la personne nommée à titre de PDG (en tant que première dirigeante) exerce notamment les responsabilités suivantes :

- être la première responsable de la PSI ainsi que de sa gouvernance;
- désigner, par délégation, une personne à titre de RSI;
- désigner une personne à titre de dirigeante de l'information, conformément à l'article 8 de la LGGRI, afin que celle-ci agisse à titre de CDSI, en vertu du paragraphe 9.1 du premier alinéa de l'article 10.1 de la LGGRI;
- exercer les fonctions que la Loi sur l'accès confère à la personne responsable de l'accès aux documents ou de la PRC, ou désigner une personne à titre de RAIPRC, afin de déléguer, par écrit, à un membre du personnel de direction, conformément à l'article 8 de la Loi sur l'accès, la totalité ou une partie de ses fonctions, afin de s'assurer du respect et de la mise en œuvre de la Loi sur l'accès au sein de Revenu Québec;
- veiller à faciliter l'exercice des fonctions confiées à la personne désignée à titre de RAIPRC, le cas échéant, conformément à l'article 8 de la Loi sur l'accès;
- désigner une personne à titre de RGVI parmi les membres du comité de direction.

Personne désignée à titre de responsable de la surveillance de l'information

Dans le cadre de cette politique, en vertu des pouvoirs que lui délègue la personne nommée à titre de PDG, la personne désignée à titre de RSI exerce notamment les responsabilités suivantes :

- élaborer et réviser périodiquement la politique;
- encadrer et assurer la gouvernance et la gestion de la PSI en adoptant une approche globale et intégrée de la PRC et de la SI;
- veiller à la mise en œuvre et au respect de la politique ainsi que des obligations légales en matière de PSI;
- être responsable de la gestion des événements et des incidents en PSI;
- mettre en place et coordonner un comité de crise en PSI;
- faire état de la situation ainsi que de la reddition de comptes en PSI, notamment lors des séances du COSPSI;
- autoriser toute exception à la politique ou à tout document qui en découle.

Personne désignée à titre de cheffe déléguée de la sécurité de l'information ou de chef délégué de la sécurité de l'information

Dans le cadre de cette politique, la personne désignée à titre de CDSI exerce notamment les responsabilités suivantes :

- soutenir la personne désignée à titre de RSI dans la mise en œuvre de la politique, plus précisément pour le volet lié à la SI;
- assurer la mise en œuvre de la gouvernance et la gestion de la SI;
- veiller au respect de la politique et des obligations légales en matière de SI;
- assumer les responsabilités prévues à l'article 12.7 de la LGGRI;
- exercer les activités liées à ses responsabilités, décrites à l'article 6 de la *Directive gouvernementale sur la sécurité de l'information*, dont les suivantes :
    - diriger le centre opérationnel de cyberdéfense (COCD),
    - désigner, parmi les membres du personnel d'encadrement sous sa direction, conformément aux indications de la cheffe ou du chef gouvernemental de la sécurité de l'information (CGSI), une personne à titre de responsable opérationnel de cyberdéfense (ROCD), dont le rôle est de voir au bon fonctionnement du COCD.

Personne désignée à titre de responsable de l'accès à l'information et de la protection des renseignements confidentiels

Dans le cadre de cette politique, en vertu des pouvoirs que lui délègue la personne nommée à titre de PDG, la personne désignée à titre de RAIPRC exerce notamment les responsabilités suivantes :

- soutenir la personne désignée à titre de RSI dans la mise en œuvre de la politique, plus précisément pour le volet lié à la PRC;
- assurer la mise en œuvre de la gouvernance et la gestion de la PRC;

- veiller au respect de la politique et des obligations légales en matière d'accès à l'information et de PRC;
- exercer les activités liées à ses responsabilités, décrites à l'article 8 de la Loi sur l'accès, dont les suivantes :
  - assumer la fonction de responsable de l'accès aux documents et de responsable de la PRC,
  - veiller à assurer la mise en œuvre de cette loi.

Personne désignée à titre de responsable de la gouvernance et de la valorisation de l'information

Dans le cadre de cette politique, la personne désignée à titre de RGVI exerce notamment les responsabilités suivantes :

- soutenir la personne désignée à titre de RSI dans la mise en œuvre de la politique, plus précisément pour le volet lié à la gouvernance et à la valorisation de l'information;
- assurer la gouvernance et la valorisation de l'information, responsabilité qui inclut la gestion de l'information.

Personne désignée à titre de responsable de l'audit interne

Dans le cadre de cette politique, la personne désignée à titre de responsable de l'audit interne (RAI) exerce notamment les responsabilités suivantes :

- réaliser, au besoin ou lorsque cela est requis, des mandats portant sur la PSI, notamment en lien avec le respect des obligations gouvernementales en matière de SI;
- formuler des conseils et/ou des recommandations en ce qui concerne la PSI.

Personnes nommées à titre de PDG (en tant que gestionnaire d'unité administrative), de VPDG ou de DG[2]

Dans le cadre de cette politique, les personnes nommées à titre de PDG (en tant que gestionnaire d'unité administrative), de VPDG ou de DG exercent notamment les responsabilités suivantes :

- assurer la protection et la sécurité des actifs informationnels qui leur sont confiés à titre de détenteur d'actifs informationnels;
- utiliser les actifs informationnels de Revenu Québec conformément à la politique ou à tout autre document qui en découle.

Comité de crise en protection et sécurité de l'information

Dans le cadre de cette politique, le CCPSI exerce notamment la responsabilité suivante :

- assurer la gestion des incidents en PSI dont la gravité est considérée comme étant élevée ou très élevée.

Gestionnaires

Dans le cadre de cette politique, les gestionnaires exercent notamment les responsabilités suivantes :

- sensibiliser le personnel interne et externe à la protection de l'information, aux conséquences d'une atteinte à la sécurité de l'information ainsi qu'à ses responsabilités en la matière;
- s'assurer de l'application et du respect de cette politique au sein de leurs unités administratives (y compris auprès des ressources externes).

Membres du personnel

Dans le cadre de cette politique, les membres du personnel exercent notamment la responsabilité suivante :

- respecter la politique et agir conformément à ses principes directeurs.

Partenaires, mandataires et fournisseurs de services

Dans le cadre de cette politique, les partenaires, les mandataires et les fournisseurs de services exercent notamment la responsabilité suivante :

- respecter la politique et s'y conformer.

DÉFINITIONS

Actif informationnel

Tout élément représentant de la valeur pour l'organisation. L'actif informationnel peut être constitué d'information contenue dans un document, quel qu'en soit le support (par exemple, un support papier ou un support technologique, qu'il soit électronique, magnétique, optique, sans fil ou autre). L'actif informationnel peut aussi être une banque de données, une technologie de l'information, une installation, un bien informatique, ou encore un ensemble formé par l'un ou l'autre de ces éléments.

2. Les sigles désignant la présidente-directrice générale ou le président-directeur général (PDG), les vice-présidentes et directrices générales et les vice-présidents et directeurs généraux (VPDG) ou les directrices générales et les directeurs généraux (DG) sont utilisés dans cet intitulé aux fins de simplification.

Centre opérationnel de cyberdéfense

Le centre opérationnel de cyberdéfense (COCD) est une entité sous la direction d'une personne désignée à titre de CDSI. Il a comme mandat d'assurer le commandement, la coordination, l'amélioration continue et le leadership en matière de cybersécurité. La direction et la coordination de chaque COCD sont assurées par la personne désignée à titre de CDSI, qui désigne une personne à titre de responsable opérationnel de cyberdéfense (ROCD) pour la soutenir à cet égard. Le COCD intervient sur le plan tactique et opérationnel.

Comité du réseau gouvernemental de cyberdéfense

Comité composé de la personne désignée à titre de responsable gouvernemental de cyberdéfense et des ROCD. Ce comité est aussi appelé *cellule de cyberdéfense.*

Confidentialité de l'information

Propriété selon laquelle l'information n'est ni rendue disponible ni divulguée à une personne ou une entité non autorisée.

Cycle de vie de l'information

Ensemble des étapes que franchit une information. Ces étapes s'amorcent par la création ou la collecte de l'information, en passant par son enregistrement, son traitement, son utilisation, sa communication et sa conservation, jusqu'à son archivage ou sa destruction.

Détenteur d'actifs informationnels

Personnes nommées à titre de PDG (en tant que gestionnaire d'unité administrative), de VPDG ou de DG qui sont responsables d'assurer la sécurité des actifs informationnels sous leur responsabilité et de protéger les renseignements confidentiels qu'elles détiennent ou utilisent.

Disponibilité de l'information

Propriété selon laquelle l'information doit être accessible, intelligible et utilisable sur demande, pour les fins auxquelles elle est destinée, par une personne ou une entité autorisée.

Événement en protection et sécurité de l'information

Événement ou situation à caractère indésirable ou inattendu pouvant entraîner une perte de confidentialité, de disponibilité ou d'intégrité de l'information, ou pouvant porter atteinte aux règles de PRC.

Gestion des risques

Approche permettant aux gestionnaires de prendre des décisions éclairées dans un contexte d'incertitude. Elle consiste à déterminer, à comprendre, à évaluer et à communiquer les enjeux importants liés aux risques ainsi qu'à en faire le suivi.

Gouvernance de la PSI

Volet de la PSI qui traite des aspects liés à l'orientation et au contrôle des processus de gestion de la PSI. Il couvre notamment la prise de décisions, le partage des responsabilités, le suivi et l'évaluation.

Gouvernance et valorisation de l'information

Approche stratégique constituée de politiques, de processus, de normes et d'indicateurs permettant l'utilisation optimale de l'information tout au long de son cycle de vie, de manière à atteindre les objectifs de l'organisation et à réduire les risques associés à cette information.

Cette approche globale vise également à permettre la valorisation de l'information, c'est-à-dire le fait de rendre disponibles des informations de qualité, et ce, dans le bon format et au bon moment, à travers un processus de collecte, de traitement et d'analyse dans la poursuite d'un objectif donné.

Incident de confidentialité

Toute forme d'atteinte à la protection des renseignements confidentiels, telle que l'accès non autorisé par la loi à un renseignement confidentiel, l'utilisation ou la communication non autorisée par la loi d'un renseignement confidentiel ou la perte d'un tel renseignement.

Incident en PSI

Événement ou situation à caractère indésirable ou inattendu qui est avéré, pouvant entraîner une perte de confidentialité, de disponibilité ou d'intégrité de l'information, ou pouvant porter atteinte aux règles de PRC ou pouvant compromettre le bon fonctionnement des opérations de l'organisation.

Infrastructure technologique

Ensemble des composants matériels et logiciels, de même que des liens de communication entre eux, qui permettent l'accès aux systèmes d'information et aux divers services constituant le réseau de Revenu Québec, en plus de permettre l'exploitation de ce réseau.

Intégrité de l'information

Propriété selon laquelle l'information doit être exacte, complète, non altérée et maintenue dans son intégralité sur un support qui lui assure une stabilité et une pérennité. De plus, selon ce principe, l'information ne peut être modifiée que par une personne ou une entité autorisée.

Journalisation

Enregistrement, dans des journaux informatiques, de certaines données permettant de déterminer l'identité d'un utilisateur (grâce au code d'utilisateur, aussi appelé *logon ID*), le type d'intervention effectuée (grâce au code de transaction, par exemple), le moment de l'intervention (date et heure) ainsi que le dossier visé. Dans le cas de la centrale de données, il est possible de reconnaître la requête utilisée lorsque le dossier ne peut pas être enregistré.

Protection et sécurité de l'information

Thème regroupant le volet de la PRC et celui de la SI.

Renseignement confidentiel

Renseignement déclaré confidentiel en vertu de la loi. Ce terme englobe notamment les renseignements fiscaux, c'est-à-dire les renseignements provenant de dossiers fiscaux, et les renseignements personnels, c'est-à-dire les renseignements qui concernent des personnes physiques et qui permettent, directement ou indirectement, de les identifier.

Renseignement personnel

Les renseignements personnels sont ceux qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier. Ils sont confidentiels à l'exception d'un renseignement personnel qui a un caractère public en vertu de la loi. Ils ne peuvent être communiqués sans le consentement de la personne concernée que dans la mesure prévue par la loi.

Réseau gouvernemental de cyberdéfense

Réseau institué au sein de l'administration publique, dont la mission vise à renforcer les dispositifs de prévention et de réaction à l'égard des cybermenaces. Ce réseau opère sous le commandement et le leadership de la personne désignée à titre de responsable gouvernemental de cyberdéfense, qui assure également la coordination et l'amélioration continue des pratiques du réseau.

Responsables de domaines de la PSI

Personnes désignées par leur VPDG ou leur DG afin d'assurer la gouvernance et la gestion d'un domaine de la PSI au sein de leur direction, ce qui fait d'elles des piliers du modèle de gouvernance de la PSI.

Risque

Tout événement empreint d'un degré d'incertitude qui pourrait avoir un effet positif (opportunité) ou négatif (menace) sur l'atteinte d'un objectif. Le risque s'évalue en prenant en compte à la fois les impacts possibles d'un événement et la probabilité que cet événement se matérialise.

Sécurité de l'information

Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. Ce concept peut également englober d'autres notions telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité.

Seuils de tolérance aux risques

Niveaux de risque maximaux acceptables pour Revenu Québec, répartis par catégories de risque, et au-delà desquels l'organisation ne veut pas se situer.

HISTORIQUE

Description du changement	Instance	Date d'adoption
Mise à jour effectuée le 2023-02-07 afin de modifier la définition de renseignement personnel et de remplacer la référence à la Direction centrale de l'accès à l'information et de la protection des renseignements confidentiels de la Direction générale de la législation par la Direction principale du bureau de la surveillance et de l'accès à l'information et des enquêtes internes, suivant un changement de structure dans l'organisation qui est entré en vigueur le 2022-09-19.	S. O.	S. O.
Refonte légère effectuée afin d'actualiser la politique et de la rendre conforme aux nouvelles dispositions de la LGGRI, de la Loi sur l'accès et de la *Directive gouvernementale sur la sécurité de l'information*, ainsi que pour intégrer les principes de la rédaction inclusive.	CA	2022-09-29
Mise à jour effectuée le 2021-03-04 afin de remplacer *le responsable de la vérification interne* (RVI) par *responsable de l'audit interne* (RAI).	S. O.	S. O.
Mise à jour effectuée le 2020-11-17 afin d'ajouter le tableau relatif à l'évaluation de la diffusion, lequel prévoit que le document est diffusé sur le site Internet de Revenu Québec.	S. O.	S. O.
Mise à jour effectuée le 2020-07-23 afin d'intégrer le contenu dans le nouveau gabarit. Également, la mise à jour vise à ajouter l'expression « et directeurs généraux » à *vice-présidents*.	S. O.	S. O.
La refonte de la politique *Protection et sécurité de l'information* (CPS-1001) entre en vigueur à la date de son adoption et abroge la politique *Sécurité de l'information numérique* (CPS-1002).	CA	2016-09-22
La politique *Protection et sécurité de l'information* (CPS-1001) remplace la *Politique organisationnelle sur la protection et sécurité de l'information* (PO-30).	CA	2012-03-01
La politique *Sécurité de l'information numérique* (CSP-1002) remplace la politique *Sécurité de l'information numérique* (PO-11).	COIPSI	2011-03-08
Cette politique est révisée tous les quatre ans ou lors de changements significatifs pouvant en modifier la teneur.		

Évaluation de la diffusion[3]	Décision	Date de décision[4]
Ce document a fait l'objet d'une évaluation de sa diffusion, conformément au paragraphe 11 du premier alinéa de l'article 4 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 2). Suivant l'évaluation de sa diffusion, il est diffusé sur le site Internet.	Diffusé	2020-11-05

3. La diffusion du document est distincte de son accessibilité à l'externe. Pour toute question concernant son accessibilité, il y a lieu de se référer à la Direction principale du bureau de la surveillance et de l'accès à l'information et des enquêtes internes.
4. La date de décision correspond à la date de signature de l'avis de conformité de la personne désignée à titre de RAIPRC ou de la décision de la personne nommée à titre de PDG, conformément au *Guide en matière de diffusion de l'information dans Internet* (CPS-3009).