

Guide des pratiques de sécurité

*Institut
de la statistique*

Québec



Cette publication est rédigée par Louise Harvey

Pour tout renseignement concernant l'ISQ
et les données statistiques dont il dispose,
s'adresser à :

Institut de la statistique du Québec
200, chemin Sainte-Foy
Québec (Québec)
G1R 5T4
Téléphone : (418) 691-2401

ou

Téléphone : 1 800 463-4090
(sans frais d'appel au Canada et aux États-Unis)

Site Web : www.stat.gouv.qc.ca

© Gouvernement du Québec

Toute reproduction est interdite
sans l'autorisation expresse
de l'Institut de la statistique du Québec.

Mai 2003

Table des matières

Avant-propos

Ce que dit la Loi sur l'Institut de la statistique du Québec

Ce que disent les autres lois

Les principes directeurs

L'engagement à la confidentialité

Le contrôle de l'accès aux locaux

Les technologies de l'information

La transmission par télécopieur

La protection des renseignements personnels sur les employés

La Politique de communication en vertu des articles 27 et 28
de la Loi sur l'Institut de la statistique du Québec

L'exploitation des fichiers de microdonnées
des enquêtes de l'Institut

Lexique

Avant-propos

La protection des renseignements qu'il recueille ou qu'il reçoit en vertu de sa loi constitutive est au cœur des préoccupations de l'Institut de la statistique du Québec. L'obligation d'assurer la protection des renseignements statistiques constitue, en effet, la pierre angulaire sur laquelle repose toute l'activité de l'Institut. L'assurance que les renseignements recueillis ou obtenus seront gardés confidentiels confère à l'Institut toute sa crédibilité, amène les individus, les entreprises et les organismes à collaborer à ses enquêtes en toute confiance, ce qui assure la qualité des résultats.

Afin de vous aider comme employés de l'Institut – ou à titre de personnes dont les services sont retenus par lui – à bien comprendre vos responsabilités en matière de protection des renseignements, et pour vous permettre de vous acquitter de vos devoirs en cette matière, le présent *Guide des pratiques de sécurité* (que l'on pourra commodément appeler notre « GPS ») a été élaboré par le Secrétariat de l'Institut et mis à la disposition de chacun sur le réseau intranet.

Le but poursuivi par ce guide est de fournir l'information de base dont vous avez besoin dans l'exercice de vos fonctions pour tout ce qui concerne, de près ou de loin, la protection des renseignements confidentiels à l'Institut, et ce, dans un langage simple et clair, sur un support facile d'accès. Ce guide ne se substitue pas, toutefois, aux politiques et aux diverses directives adoptées par l'Institut en matière de confidentialité, et chaque employé est responsable de prendre connaissance des directives qui le concernent plus directement.

Cet ensemble de textes – dotés d'hyperliens qui renvoient à d'autres sections du *Guide*, à des documents complémentaires sur l'intranet ou sur Internet ou qui vous mettent en contact avec des personnes-ressources – fait ressortir l'essentiel des politiques et des directives déjà adoptées par le Comité sur la protection des renseignements personnels et des autres renseignements confidentiels de l'Institut. Au fur et à mesure que des directives seront adoptées ou modifiées, le *Guide* sera mis à jour pour refléter ces changements.

J'invite donc chacun de vous, nouvel employé ou plus ancien, à consulter régulièrement cette section de l'intranet. Je ne saurais trop insister sur la nécessité de vous tenir informés de tout changement ou ajout qui y sera apporté.

Le **Secrétariat de l'Institut** sera heureux de recevoir toute suggestion de nature à améliorer ce guide et susceptible d'en faire un ouvrage de référence aussi utile que possible.

Yvon Fortin,
Directeur général,
Avril 2003

Ce que dit la Loi sur l'Institut

L'obligation à la confidentialité

L'obligation à la confidentialité à laquelle vous êtes soumis en tant qu'employé de l'Institut de la statistique du Québec, ou à titre de personne dont les services sont retenus par l'Institut, est énoncée à l'[article 25](#) de la Loi sur l'Institut de la statistique du Québec (L.R.Q., c. I-13.011).

Cette **obligation à la confidentialité** stipule que tous les employés de l'Institut, quel que soit leur statut d'emploi (employés réguliers ou occasionnels), ainsi que toutes les personnes dont les services sont retenus pour réaliser un mandat (contractuels) et celles qui font l'objet d'un prêt de service, ne peuvent révéler un renseignement qui a été obtenu en vertu de la Loi sur l'Institut et qui peut être rattaché à une personne, à une entreprise, à un organisme ou à une association en particulier.

L'article 25 interdit non seulement la révélation **directe** d'un tel renseignement, mais également sa révélation **indirecte**, par quelque moyen que ce soit, par exemple par déduction, par comparaison ou par recoupement. En d'autres mots, vous devez vous assurer, lorsque vous publiez des compilations statistiques, qu'aucune information relative à une personne, à une entreprise, à un organisme ou à une association en particulier ne peut être déduite par recoupement ou par comparaison avec une autre information. De la même manière, vous ne pouvez communiquer aucun fichier de données, même épurées (dénominalisées), c'est-à-dire dont on a enlevé les noms ou toute autre variable permettant l'identification, s'il y a risque que, par recoupement ou par comparaison avec une autre information, quelqu'un puisse en tirer une information relative à une personne, à une entreprise, à un organisme ou à une association en particulier.

Cette obligation à la confidentialité imposée par la Loi est maintenue au-delà de la durée de votre emploi ou de votre contrat à l'Institut. Elle est d'une durée illimitée.

La notion de « renseignement confidentiel »

En énonçant l'obligation à la confidentialité, l'article 25 définit en même temps la notion de « renseignement confidentiel ». Au sens de la Loi sur l'Institut de la statistique du Québec, un renseignement confidentiel est celui qui a été obtenu en vertu de la Loi sur l'Institut (recueilli par enquête ou obtenu d'un autre organisme sur fichier administratif) et qui peut être associé à une personne, à une entreprise, à un organisme ou à une association en particulier. Voici quelques exemples de ce type de renseignements :

- une réponse fournie par un répondant à une question posée dans le cadre d'une enquête de l'Institut;
- un commentaire formulé par un répondant à l'occasion d'une enquête de l'Institut, même si ce commentaire n'a pas de rapport direct avec le sujet de l'enquête;
- un renseignement relatif à une personne, à une entreprise, à un organisme ou à une association en particulier, provenant d'un fichier administratif d'un ministère ou d'un organisme, et dont l'Institut a obtenu copie;
- le nom d'une personne, d'une entreprise, d'un organisme ou d'une association en particulier qui participe à une enquête de l'Institut;
- le nom d'une personne qui a contribué à ce que l'Institut entre en contact avec des répondants, par exemples le nom d'un parent, d'un enseignant ou du directeur d'une école qui a permis à l'Institut d'enquêter un enfant, ou encore le nom d'un employeur qui a permis de conduire une enquête auprès d'un employé;
- le nom d'une personne, d'une entreprise, d'un organisme ou d'une association en particulier qui a refusé de participer à une enquête de l'Institut.

Les méthodes de masquage utilisées pour réduire les risques de divulgation indirecte peuvent également être confidentielles. Enfin, même si une information confidentielle peut paraître banale ou anodine, sa divulgation est strictement interdite.

L'Institut ne peut donc révéler que des moyennes, des tendances, des indices, des totalisations ou des compilations statistiques dépouillés de toute possibilité de révélation directe ou indirecte d'une information relative à un individu, à une entreprise, à un organisme ou à une association en particulier. Il ne peut également communiquer que des fichiers de données publics, c'est-à-dire des fichiers complètement masqués.

Une infraction à l'obligation à la confidentialité

Vous seriez reconnu coupable d'une infraction à l'obligation à la confidentialité si vous commettiez les actes mentionnés aux paragraphes 1 à 5 de l'[article 41](#) de la Loi sur l'Institut.

Essentiellement, une infraction à l'article 25 consiste à révéler, sans excuse légitime, un renseignement confidentiel; à se servir d'un tel renseignement à des fins personnelles (par exemple, pour faire des placements ou pour spéculer sur un bien, etc.); à obtenir ou à essayer d'obtenir des renseignements dont on n'a pas besoin dans l'exercice de ses fonctions; à se présenter faussement comme un employé de l'Institut; à inciter un employé de l'Institut à révéler un renseignement confidentiel.

Les amendes prévues en cas de manquement

Les amendes auxquelles vous vous exposez en commettant une infraction à l'obligation à la confidentialité sont de 200 \$ à 1 000 \$, ou de 500 \$ à 2 500 \$ en cas de récidive ([article 42](#)). En plus de ces amendes prévues par la Loi, vous êtes évidemment exposé à des mesures disciplinaires pouvant aller jusqu'au congédiement.

Les seules communications autorisées par la Loi

La Loi sur l'Institut de la statistique prévoit de façon très claire **les cinq possibilités de communication de renseignements** obtenus en vertu de cette loi :

1. Une entente a été conclue en vertu des articles 7 ou 9, c'est-à-dire une entente avec un autre gouvernement, avec l'un de ses ministères ou organismes, avec une organisation internationale ([article 7](#)), ou avec un ministère ou un organisme du gouvernement du Québec ([article 9](#)). Les [articles 8, 10 et 11](#) précisent de façon très rigoureuse les modalités qui s'imposent dans ce cas.
2. La personne, l'entreprise, l'organisme ou l'association sur qui porte le renseignement a préalablement donné son consentement écrit à cette communication ([article 26](#)).
3. Si le renseignement a déjà un caractère public en vertu d'une autre loi, le directeur général de l'Institut peut en autoriser la communication ([article 29](#)). Des exemples de renseignements ayant un caractère public en vertu d'une loi sont mentionnés à l'[article 57](#) de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.
4. Le directeur général de l'Institut peut autoriser par écrit la communication de listes de noms et d'adresses de personnes morales, d'entreprises, d'associations ou d'établissements selon leur secteur d'activité économique ou par tranche de nombre d'employés, ou la communication de listes de produits extraits, obtenus, traités, fabriqués, transportés, etc. par des personnes morales, des entreprises, des associations ou des établissements au cours de leurs activités ([article 28](#)). Une telle communication ne peut, cependant se faire que dans le cadre de modalités administratives rigoureuses et uniquement sous réserve de nombreuses conditions : par exemples, à la condition que les informations fournies ne servent pas à des fins de mise en marché, de sollicitations, ni à des fins commerciales, ou encore à la condition qu'elles ne servent pas à des activités susceptibles de porter préjudice aux répondants qui ont fournis ces renseignements.
5. Un renseignement obtenu par l'Institut en vertu de sa loi constitutive peut être révélé sans le consentement de la personne, de l'entreprise, de l'organisme ou de l'association concerné, lorsque cette divulgation est requise aux fins d'une poursuite en vertu de la Loi sur l'Institut de la statistique du Québec ([article 26](#)). Un renseignement obtenu par l'Institut en vertu de sa loi constitutive ne peut être révélé dans aucun autre cas de poursuite judiciaire.

Des principes directeurs qui traduisent l'esprit de la loi

Afin que vous puissiez traduire concrètement, dans vos gestes de tous les jours, les obligations qui vous sont imposées par la Loi, l'Institut a adopté **diverses politiques ou directives** en matière de confidentialité dans le domaine des technologies de l'information, d'accès aux locaux, etc. Chacune de ces politiques et de ces directives s'inspire de quelques grands principes directeurs, qui sous-tendent les moyens dont s'est doté l'Institut pour remplir ses obligations de confidentialité. Ces principes directeurs sont les mêmes dans toutes les agences statistiques des pays démocratiques.

Vous trouverez le **texte intégral** de ces principes directeurs à la section « Politiques, normes, procédures et lois » de l'intranet. Vous pouvez également en consulter un **résumé** à la section intitulée « Les principes directeurs » du présent document.

Vous avez des questions?

Pour toute question concernant la Loi sur l'Institut de la statistique du Québec, vous pouvez communiquer avec **Julie Blackburn**.

Ce que disent les autres lois

En plus de la Loi sur l'Institut de la statistique du Québec, qui vous indique, à titre d'employé de l'Institut ou comme personne dont les services sont utilisés par l'Institut, vos obligations en matière de confidentialité (voir section intitulée « [Ce que dit la Loi sur l'Institut de la statistique du Québec](#) »), quatre autres lois du Québec contiennent des dispositions relatives à la confidentialité. Les deux premières de ces lois s'adressent à vous en tant que membre de la fonction publique québécoise, et les deux autres vous concernent, de manière plus générale, à titre de citoyen.

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)

Communément appelée Loi sur l'accès, cette loi reconnaît à chaque individu le droit à la confidentialité des renseignements qui le concernent et qui permettent de l'identifier ([articles 53 et 54](#)). Elle impose également aux ministères et organismes du gouvernement du Québec l'obligation de préserver la confidentialité de tels renseignements ([article 62](#)).

Si vous communiquez sciemment un renseignement personnel sans y être autorisé, vous commettez une infraction à la Loi sur l'accès et vous êtes passible d'une amende de 200 \$ à 1 000 \$, ou de 500 \$ à 2 500 \$ en cas de récidive ([article 159](#)).

Comme on le voit, la Loi sur l'accès a pour objectif d'assurer le caractère confidentiel des renseignements qui concernent les personnes physiques, c'est-à-dire les particuliers. Quant à la Loi sur l'Institut de la statistique du Québec, elle couvre un univers plus large, puisqu'elle se préoccupe en outre des renseignements relatifs aux entreprises, aux organismes et aux associations. Par ailleurs, la Loi sur l'Institut de la statistique du Québec interdit également les révélations indirectes de tels renseignements (voir la section intitulée « [Ce que dit la Loi sur l'Institut](#) »).

La Loi sur la fonction publique (L.R.Q., c. F-3.1.1)

En tant qu'employé de l'État, vous êtes tenu à la confidentialité sur ce dont vous avez connaissance dans l'exercice de vos fonctions. Cette obligation, qui vous incombe en vertu de l'[article 16](#) de la Loi sur la fonction publique, découle d'un ensemble de règles d'éthique et de discipline auxquelles doit se soumettre tout fonctionnaire (par exemple, celui-ci doit faire preuve de loyauté, d'honnêteté, d'impartialité, de neutralité politique, il doit exercer ses fonctions dans l'intérêt du public, etc.

Si vous contrevenez à l'une ou l'autre de ces règles d'éthique et de discipline (énumérées aux articles 5 à 12 de la Loi sur la fonction publique), vous êtes « passible d'une mesure disciplinaire pouvant aller jusqu'au congédiement selon la nature et la gravité de la faute ».

Le Code civil et la Charte des droits et libertés

Les deux importants textes législatifs que sont le Code civil et la Charte des droits et libertés de la personne du Québec considèrent que le droit à la vie privée constitue un droit fondamental pour tout individu.

Le Code civil du Québec (L.Q., 1991, c. 64) établit en effet, dès le départ ([article 3](#)), que toute personne a le droit à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation **et de sa vie privée**.

La Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12) va dans le même sens. À l'[article 5](#), elle affirme que « toute personne a droit **au respect de sa vie privée** ».

Ce droit fondamental de chaque personne au respect de sa vie privée vous impose donc le devoir absolu de garder confidentielle toute information relative à un individu et à laquelle vous auriez accès dans l'exercice de vos fonctions.

Vous avez des questions?

Pour toute question concernant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, vous pouvez communiquer avec [Julie Blackburn](#).

Les principes directeurs

Les politiques et les directives dont s'est doté l'Institut en matière de protection des renseignements confidentiels reposent sur **quelques grands principes fondamentaux** qui guident le fonctionnement de l'Institut. Toutes les agences statistiques nationales des pays démocratiques, de même que toutes les agences statistiques d'organismes internationaux, adhèrent d'ailleurs à de tels principes directeurs.

Ces principes directeurs – ou lignes de conduite – sont les suivants :

« Rien qui ne soit essentiel à sa mission » et « Pas plus longtemps qu'il ne le faut »

L'Institut ne recueille, n'obtient et ne conserve de l'information qu'aux fins de sa mission, c'est-à-dire uniquement à des fins statistiques.

En conséquence, la durée de conservation d'un renseignement qui permet d'identifier une personne physique ou morale (**renseignement d'identité**) ne doit pas excéder le temps qu'il faut pour utiliser ce renseignement à des fins statistiques. Ainsi, dès que possible après la collecte ou l'obtention de l'information, les renseignements d'identité doivent être remplacés par des numéros séquentiels. De même, tout fichier servant à l'appariement entre les numéros séquentiels et les renseignements d'identité ne doit être conservé que le temps nécessaire à la production de statistiques.

« Accès aux personnes autorisées seulement »

Les seules personnes autorisées à avoir accès à un document contenant des renseignements sur des personnes physiques ou morales sont celles qui travaillent directement à la collecte de ces renseignements ou à leur traitement en vue de produire des données agrégées et des analyses à partir de ces données agrégées. En conséquence, seuls les employés de l'Institut qui ont besoin, dans l'exercice de leurs fonctions, d'accéder à un document contenant des renseignements sur des personnes physiques ou morales peuvent obtenir cet accès.

L'employé qui dispose d'un tel accès doit veiller, dans son environnement de travail, à éliminer les risques que d'autres employés non autorisés puissent prendre connaissance de ces renseignements.

« Des chercheurs très encadrés »

Pour l'aider à exploiter autant que possible les données qu'il détient et pour en tirer toute la connaissance scientifique qui peut en être dégagée, l'Institut peut retenir les services de personnes qui ne font pas partie de son personnel. (Voir la section intitulée « [Politique relative à l'exploitation des fichiers de microdonnées des enquêtes de l'ISQ](#) ». Ainsi, le directeur général peut embaucher des membres de comités d'analyse propres aux activités de l'Institut, des chercheurs associés à des programmes mis de l'avant par des organismes publics ou à des projets acceptés par des organismes officiels de soutien et d'encadrement de la recherche, ou encore des experts dans le traitement des données.

Toutes ces personnes sont soumises aux mêmes obligations de confidentialité que les employés de l'Institut et elles doivent, notamment, signer un engagement à la confidentialité. Les mandats confiés à ces personnes font l'objet d'ententes ou de contrats prévoyant de façon très explicite des garanties de confidentialité et des mesures administratives, physiques et technologiques propres à assurer la sécurité de l'information à laquelle on leur donne accès.

« Les seules communications autorisées »

L'Institut ne peut communiquer à un autre organisme public un renseignement sur une personne physique ou morale qu'à la condition expresse qu'il y ait eu préalablement entente avec cet autre organisme public, conformément à l'[article 7](#) ou à l'[article 9](#) de la Loi sur l'Institut. Cependant, comme le précise l'[article 10](#) de cette loi, les renseignements qui concernent une personne physique ou morale qui se serait opposée à cette transmission ne seraient pas transmis.

« Seuls les fichiers rendus anonymes peuvent être publics »

Le directeur général de l'Institut peut autoriser la diffusion de fichiers rendus anonymes, c'est-à-dire complètement masqués, afin de réduire dans toute la mesure du possible les risques de divulgation directe et indirecte de renseignements sur une personne physique ou morale.

L'engagement à la confidentialité

Pour l'instant, la Loi sur l'Institut de la statistique du Québec ne contient aucune disposition qui rendrait obligatoire, pour les employés de l'Institut et les personnes dont il retient les services, la signature d'un engagement à la confidentialité ou d'une déclaration de discrétion, comme tel est le cas pour d'autres lois québécoises.

Toutefois, dès la création de cet organisme, le directeur général a rendu obligatoire la signature d'un tel engagement à la confidentialité, pour renforcer les dispositions de la Loi sur l'Institut ayant trait aux obligations de confidentialité, pour rendre ces dispositions plus visibles et pour faire comprendre aux employés, ainsi qu'aux personnes dont les services sont retenus par l'Institut, **leur responsabilité personnelle à cet égard**.

La [Politique relative à l'engagement à la confidentialité](#) identifie les personnes qui doivent signer un tel engagement et elle consigne les différentes modalités de gestion en cette matière.

Qui est visé?

Que vous soyez employé de l'Institut, et quel que soit votre statut d'emploi (employé régulier ou occasionnel), ou que vos services aient été retenus par l'Institut en vertu d'une entente ou d'un contrat pour réaliser un mandat, vous êtes tenu de signer un engagement à la confidentialité à votre entrée en fonctions ou au moment d'entreprendre vos travaux.

En quoi consiste cet engagement?

En signant l'engagement à la confidentialité, vous vous engagez solennellement à respecter l'obligation de confidentialité qui vous est imposée par l'[article 25](#) de la Loi sur l'Institut, et qui consiste à ne pas révéler, ni directement ni indirectement, c'est-à-dire par déduction, par comparaison, par recoupement, etc., un renseignement obtenu en vertu de la Loi sur l'Institut et qui peut être rattaché à une personne, à une entreprise, à un organisme ou à une association en particulier.

La durée de cet engagement

Votre engagement à la confidentialité est illimité dans le temps, c'est-à-dire qu'il est valide au-delà de la durée de votre emploi ou de votre mandat à l'Institut.

Devant qui cet engagement est-il signé?

L'engagement à la confidentialité est signé devant une personne qui agit à titre de « commissaire à l'assermentation », c'est-à-dire une personne qui détient un permis (une « commission ») du ministère de la Justice pour agir à ce titre.

Compte tenu que l'Institut a des bureaux à Québec et à Montréal, une personne agit comme commissaire à l'assermentation dans chacune de ces deux villes. Louise Harvey, du Secrétariat à Québec, et France Lacoursière, de la Direction de l'administration à Montréal, exercent les fonctions de commissaires à l'assermentation à l'Institut. De plus, Denis Ouellette-Roussel, responsable du Centre d'accès aux données de recherche de l'Institut (CADRISQ), situé sur le campus de l'Université de Montréal, agit également comme commissaire à l'assermentation auprès de la clientèle de ce centre.

Exceptionnellement, en l'absence de la commissaire à l'assermentation, l'engagement à la confidentialité peut être signé devant la conseillère juridique de l'Institut.

Quand cet engagement doit-il être signé?

Si vous êtes un nouvel employé de l'Institut, vous êtes invité à signer un engagement à la confidentialité au moment de votre entrée en fonctions, ou dès que possible. Si vos services sont retenus par l'Institut comme contractuel, vous devez signer cet engagement à la confidentialité avant d'entreprendre les travaux inhérents à votre mandat.

La responsabilité administrative en matière d'engagement à la confidentialité

Le Secrétariat de l'Institut a la responsabilité administrative de l'engagement à la confidentialité. À ce titre, la titulaire de cette unité administrative (Louise Harvey) est responsable d'appliquer la politique d'engagement à la confidentialité de l'Institut et de mettre à jour au besoin, de conserver une copie de chaque formulaire signé et de constituer un registre (une liste) de toutes les personnes ayant signé un tel engagement.

Le rôle de chaque unité administrative de l'Institut

Chaque fois qu'un nouvel employé entre en fonctions, ou que les services d'une personne sont retenus par l'Institut, le gestionnaire concerné ou la personne qu'il a déléguée doit prendre rendez-vous avec la commissaire à l'assermentation pour faire signer l'engagement à la confidentialité.

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant l'engagement à la confidentialité, vous pouvez communiquer avec [Louise Harvey](#).

Le contrôle de l'accès aux locaux

L'Institut est très soucieux de contrôler la circulation des personnes dans ses locaux. Pour assurer ce contrôle, il a adopté diverses mesures administratives (par exemple, il n'y a qu'un seul poste d'accueil, tant à Québec qu'à Montréal), procédé à des aménagements physiques (par exemple, certaines portes ne permettent la circulation que dans le sens de la sortie) et il s'est pourvu de moyens technologiques (système informatisé de détection des entrées). La [Politique relative au contrôle de l'accès aux locaux](#) consigne l'ensemble de ces mesures et elle édicte les règles à respecter en cette matière.

Toutefois, l'efficacité de ces mesures, de ces aménagements et de ces moyens technologiques dépend d'un facteur crucial, d'un élément stratégique : l'humain! C'est-à-dire vous! C'est vous qui êtes **personnellement responsable** du succès ou de l'échec de cette politique.

Voici donc l'essentiel de ce que vous devez savoir pour vous acquitter adéquatement de vos obligations en cette matière.

Votre carte d'accès aux locaux

Cette carte, qui vous est remise dès votre entrée en fonctions à l'Institut, vous permet de circuler librement là où vos tâches sont susceptibles de vous amener de façon habituelle. Selon l'unité administrative à laquelle vous appartenez et la nature de vos fonctions, cette carte vous donnera accès à certains locaux et vous en interdira d'autres. Votre accès à certains locaux sera également modulé en fonction de l'heure du jour et du jour de la semaine.

Cette carte est donc l'un des éléments d'un système informatisé de contrôle de l'accès aux locaux. Elle porte un numéro visible et chaque carte est associée, par ordinateur, à la personne pour qui elle a été émise. Chacune de vos entrées par l'une ou l'autre des portes donnant accès aux locaux de l'Institut est autorisée ou interdite par ce système de contrôle de l'accès, et chacune de ces entrées est également enregistrée par ce système.

De manière générale, votre carte vous donne le droit d'accéder à tous les étages occupés par l'Institut (dans votre ville seulement) les jours ouvrables, entre 7 h 30 et 17 h 30 à Québec et de 7 h 30 à 18 h 00 à Montréal (sauf à certains locaux accessibles seulement aux employés désignés).

Votre carte vous donne également le droit d'accéder à l'étage où se trouve votre bureau tous les jours de la semaine, 24 heures par jour, 365 jours par année.

Comme vous êtes responsable de votre carte d'accès et **de l'usage qui en est fait**, vous ne pouvez la prêter à qui que ce soit. Si vous la perdez, vous devez en aviser immédiatement la Direction de l'administration qui l'invalidera et vous en remettra une autre. Si vous l'oubliez, vous devez également en informer la Direction de l'administration qui émettra une carte temporaire à votre intention.

Lorsque vous franchissez l'une des portes donnant accès aux locaux de l'Institut, **vous devez vous assurer qu'aucune personne non autorisée ne pénètre en même temps que vous** dans les locaux de l'Institut. Quiconque n'affiche pas, bien en évidence, sa carte d'identité avec photo (voir point suivant) ou une carte portant la mention « Visiteur » n'est pas autorisé à se trouver dans les locaux de l'Institut et, en conséquence, il doit être raccompagné hors de ces locaux.

Votre carte d'accès aux locaux est la propriété de l'Institut. Si vous quittez l'Institut, ou si votre contrat est terminé, vous devez la remettre au gestionnaire de votre unité administrative ou à la personne responsable de l'application de la Politique relative au contrôle de l'accès aux locaux.

Votre carte d'identité avec photo

Si vous êtes employé régulier ou occasionnel, ou si vous êtes contractuel ou employé d'un ministère ou d'un autre organisme en prêt de service à l'Institut, une carte d'identité vous est remise à votre entrée en fonctions. En plus de votre photo, cette carte comporte notamment votre nom et une date d'expiration.

Cette carte avec photo doit être portée bien en vue, en permanence. Elle vous permet d'être reconnu comme une personne dont la présence est autorisée dans les locaux de l'Institut. Elle vous permet également d'exercer la surveillance et le contrôle que tous les employés de l'Institut doivent opérer à l'égard des personnes qui se trouveraient dans les locaux de l'Institut et qui ne porteraient pas une telle carte ou la carte prévue pour les visiteurs (voir point suivant).

Le contrôle des visiteurs

L'accueil des visiteurs est restreint à un seul point d'entrée : au 5^e étage à Québec et au 19^e étage à Montréal. Une signalisation adéquate dirige vers ce poste d'accueil tout visiteur qui se présenterait ailleurs à l'Institut. Si vous attendez un visiteur, vous devez donc lui indiquer de se présenter à ce poste d'accueil.

À son arrivée, votre visiteur sera inscrit au registre des visiteurs et on lui remettra un permis de visite (une carte portant la mention « Visiteur »), valide pour une journée seulement, qu'il devra porter en évidence pendant toute la durée de sa visite dans les locaux de l'Institut. La préposée à l'accueil vous avisera par téléphone de l'arrivée de votre visiteur et vous invitera à venir le chercher au poste d'accueil.

Vous devez prendre en charge votre visiteur pendant toute la durée de sa visite, c'est-à-dire que vous devez personnellement l'accompagner en tout temps lorsqu'il circule dans les locaux de l'Institut. Aucun visiteur ne doit circuler dans les locaux de l'Institut s'il n'est pas accompagné par un employé de l'Institut.

À la fin de sa visite, vous devez raccompagner votre visiteur au poste d'accueil où l'heure de son départ est inscrite au registre des visiteurs et où il remet son permis de visite. En dehors des heures normales de travail, c'est-à-dire quand la préposée à l'accueil n'est pas en fonction, vous devez vous assurer de raccompagner votre visiteur en dehors des locaux de l'Institut, vous devez récupérer son permis de visite, remettre immédiatement ce permis de visite au poste d'accueil et inscrire l'heure de départ de votre visiteur au registre des visiteurs.

Si vous croisez dans les locaux de l'Institut une personne portant une carte « Visiteur » et qui n'est pas accompagnée, vous devez la conduire auprès de l'employé qu'elle est censée visiter ou la raccompagner au poste d'accueil où son départ sera enregistré.

La responsabilité de l'application de la Politique

La Direction de l'administration est responsable de l'application de la Politique de contrôle de l'accès aux locaux. Vous devez vous adresser à cette direction pour signaler ce qui vous semble une anomalie ou pour suggérer un ajout ou une amélioration.

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant le contrôle de l'accès aux locaux, vous pouvez communiquer avec [Richard Delisle](#).

Les technologies de l'information

L'Institut de la statistique du Québec s'est doté d'une [Politique relative à la sécurité informatique](#) et de diverses directives et règles qui ont pour but :

- de garantir la confidentialité des renseignements recueillis ou obtenus par l'Institut en vertu de sa loi constitutive;
- de limiter l'accès aux **actifs informationnels** strictement aux employés de l'Institut qui ont besoin de cet accès dans l'exercice de leurs fonctions;
- d'assurer la **disponibilité** de l'information,
- d'assurer **l'intégrité** des **actifs informationnels**;
- de protéger l'équipement;
- de maintenir les services.

Comme employé de l'Institut ou à titre de personne dont les services sont retenus par l'Institut, voici quelles sont vos obligations en matière de technologies de l'information.

Votre identification au réseau

Vous pouvez accéder au réseau informatique de l'Institut en vous identifiant d'abord à l'aide d'un code d'utilisateur (appelé « numéro d'identifiant ») qui vous est attribué à votre entrée en fonctions (voir la [Politique pour la protection des voies d'accès logiques aux actifs informationnels](#), sur l'intranet). Ce code alphanumérique à sept ou huit positions est unique, et il vous est attribué par la Direction des technologies de l'information à la demande du gestionnaire de votre unité administrative. Pour formuler cette demande, il lui faut remplir le [formulaire](#) destiné à cette fin.

Sur ce formulaire, votre gestionnaire mentionne à quelle unité administrative vous appartenez et quels seront vos besoins en matière d'équipement informatique, y compris une adresse de courriel.

Votre numéro d'identifiant au réseau n'est pas confidentiel.

Votre mot de passe

En plus de votre numéro d'identifiant, vous devez entrer un mot de passe pour pouvoir accéder au réseau informatique de l'Institut. Ce mot de passe est associé à votre numéro d'identifiant et il a pour but d'assurer son **authentification**. (Voir la **Procédure d'identification au réseau**, sur l'intranet.)

Lors de votre première tentative pour accéder au réseau, vous devrez entrer le mot de passe de départ (habituellement « password ») qui vous aura été attribué par la Direction des technologies de l'information. Il vous faudra modifier immédiatement ce mot de passe de départ par un autre de votre choix, en suivant la procédure indiquée.

Votre mot de passe doit être constitué d'au moins cinq caractères. Il ne devrait pas être formé d'un mot facile à deviner (par exemple, votre nom, le prénom de votre enfant ou le nom de votre animal préféré, etc.). Il devrait être composé d'une séquence de lettres, de chiffres et de caractères particuliers impossibles à deviner. Une bonne habitude à prendre est de déterminer votre mot de passe de la manière suivante : faites une phrase, choisissez le premier caractère de chaque mot de cette phrase et ajoutez des signes de ponctuation.

Tous les 40 jours, vous serez invité à remplacer votre mot de passe. Dix mots de passe différents auront été utilisés avant que vous puissiez revenir au premier.

Votre mot de passe est strictement confidentiel. Sous aucun prétexte vous ne devez le communiquer à qui que ce soit. Si, en votre absence, un collègue de travail a besoin de consulter certains de vos fichiers, il doit avoir recours à d'autres moyens pour obtenir cet accès, par exemple en consultant les répertoires de travail communs sur le réseau.

Vous devez changer votre mot de passe chaque fois que vous soupçonnez que quelqu'un de votre entourage le connaît.

Si vous oubliez votre mot de passe, vous devez demander à la Direction des technologies de l'information de vous attribuer un mot de passe temporaire, que vous modifierez immédiatement par un nouveau mot de passe de votre choix.

Afin de prévenir toute intrusion sur le réseau de l'Institut, votre numéro d'identifiant deviendra inutilisable après trois tentatives infructueuses d'accéder au réseau. Vous devrez alors demander l'aide du centre d'assistance de la Direction des technologies de l'information (poste 3030 à Québec et 6060 à Montréal) pour que votre numéro d'identifiant puisse être réutilisé.

Vos sessions de travail

Chaque fois que vous vous absentez de votre poste de travail pour un certain temps (repas du midi, réunion, etc.), vous devez verrouiller votre poste de travail (en appuyant sur les touches CTRL / Alt / Del et en choisissant l'option « Lock Workstation ») ou mettre fin à votre session sur le réseau.

Il faut éteindre votre micro-ordinateur avant de partir en fin de journée. Si, par mégarde, vous oubliez de le faire, vous devrez quand même vous reconnecter au réseau à votre retour, puisque la Direction des technologies de l'information s'assure chaque jour que tous les usagers sont déconnectés du réseau. (Voir la [Procédure d'identification au réseau](#), sur l'intranet.)

Même si, techniquement, il est possible d'ouvrir plus d'une session de travail à la fois en ayant recours à plus d'un micro-ordinateur, il est préférable de n'en ouvrir qu'une seule.

Vos droits d'accès aux répertoires du réseau

Pour des raisons de sécurité, les serveurs où sont emmagasinés les données de l'Institut et les divers logiciels en usage sont subdivisés en différentes zones (ou répertoires). Selon la direction à laquelle vous appartenez et selon les besoins de votre emploi, des droits d'accès à certains répertoires vous seront accordés par la Direction des technologies de l'information, sur recommandation du gestionnaire de votre unité administrative.

Certains répertoires du réseau sont des zones partagées, c'est-à-dire que plusieurs employés de l'Institut peuvent y avoir accès en mode « lecture et écriture » ou « lecture seule ». D'autres répertoires sont réservés à quelques personnes en particulier, par exemple les membres d'une équipe de projet, ou encore strictement à vous seul. Ainsi, uniquement les personnes qui en ont réellement besoin, dans l'exercice de leurs fonctions, ont accès à certaines données et à certains outils.

Si, dans le cadre de vos fonctions, vous devez avoir accès aux fichiers de données du [Registre des événements démographiques](#), ou à des [fichiers contenant des données provenant de sources fiscales](#), une demande d'accès spécifique devra préalablement être formulée par le responsable de votre unité administrative en utilisant les formulaires prévus à cet effet.


Lorsque vous sauvegardez des données dans l'un ou l'autre des répertoires du réseau, vous devez vous assurer que personne d'autre que les employés autorisés ne peut effectivement y avoir accès. (Voir la [Procédure concernant les données confidentielles sur supports magnétiques](#), sur l'intranet.)

Les copies de sécurité

Seules les données sauvegardées dans les répertoires du réseau font l'objet de copies de sécurité. Comme aucune copie de sécurité n'est faite du disque dur (« C\ ») de votre micro-ordinateur, vous ne devez y conserver aucune donnée nécessaire à votre travail.

La protection contre les virus

Une responsabilité vous incombe personnellement, comme employé de l'Institut ou à titre de personne dont les services sont retenus par l'Institut, de protéger l'équipement informatique mis à votre disposition par votre employeur et d'éviter toute contamination de l'environnement de travail par des virus.

Vous devez d'abord vous assurer que le logiciel de détection des virus est toujours actif sur votre micro-ordinateur. Vous pouvez vous en assurer en vérifiant que l'icône suivante :  apparaît dans la barre de tâches, dans le coin inférieur droit de l'écran de votre micro-ordinateur. En cas de doute, contactez le centre d'assistance de la Direction des technologies de l'information (poste 3030 à Québec et 6060 à Montréal).

De plus, lorsque vous recevez une disquette, un cédérom ou un courriel avec pièce jointe, vous devez toujours soumettre cette disquette, ce cédérom ou ce fichier à l'antivirus. Vous devez aviser le centre d'assistance de la Direction des technologies de l'information lorsqu'un virus est ainsi détecté.

Pour éviter toute contamination, vous devez également détruire, sans l'ouvrir, tout courriel qui provient d'une source douteuse. (Voir la [Procédure de protection contre les virus](#), sur l'intranet.)

Vos communications électroniques

Lorsque vous êtes au bureau et que vous devez communiquer par courrier électronique avec d'autres employés de l'Institut, vous devez absolument recourir au logiciel de courrier électronique Outlook. Pour identifier le destinataire de votre message, vous devez de préférence sélectionner son nom dans la « Liste d'adresses du bureau de poste ». Seule cette façon de procéder garantit la confidentialité de la communication, puisque celle-ci s'effectue par le réseau interne de l'Institut.

Le recours à Internet, en utilisant une adresse de courrier de type « prénom.nom@stat.gouv.qc.ca », ne peut garantir que la communication ne sera pas interceptée par quelqu'un de l'extérieur, puisque cette communication transite par un fournisseur externe, et non par le réseau interne de l'Institut.

Puisque aucune garantie absolue de confidentialité n'est assurée dans vos communications par Internet, vous ne devez pas communiquer de donnée confidentielle grâce à ce réseau, à moins que ces données ne soient préalablement **cryptées** avec un outil de **cryptage** recommandé par la Direction des technologies de l'information.

Même si aucune communication de données confidentielles ne doit être effectuée par courrier électronique, vous devez insérer, à la suite de votre signature, un texte interdisant à la personne qui recevra votre message de le divulguer ou de le reproduire, et l'invitant à vous contacter si votre message lui a été envoyé par erreur.

Afin d'éviter un engorgement et, conséquemment, un ralentissement du réseau, vous devez également vous abstenir de joindre à vos messages électroniques de trop gros fichiers, par exemple des fichiers de 2 mégaoctets (Mo) et plus. Il est préférable de verser de tels fichiers dans un répertoire commun.

Votre comportement sur le Web

Les nouvelles technologies, comme la navigation sur Internet et la messagerie électronique, posent à chacun de nous des questions d'ordre éthique. Les règles d'éthique en vigueur au sein de l'administration publique québécoise s'appliquent en tout temps à vous, comme employé de l'Institut de la statistique du Québec, lorsque vous utilisez les outils mis à votre disposition et, à plus forte raison, lorsque vous êtes dans l'exercice de vos fonctions.

En utilisant les moyens électroniques de communication fournis par votre employeur, vous agissez à titre de représentant de l'Institut. Chacune de vos consultations sur Internet, chacun de vos messages électroniques identifie l'Institut et l'associe à cette consultation ou à cette transmission. Il va de soi que toute communication doit être empreinte de courtoisie et refléter le respect de l'Institut envers ses interlocuteurs.

Conformément à la directive gouvernementale sur l'utilisation éthique du courriel et d'Internet, il est interdit de « visionner, télécharger, copier, partager ou expédier des images ou des fichiers érotiques, de pornographie juvénile ou de sexualité explicite ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste, ou qui contrevient à l'une des dispositions de la Charte des droits et libertés de la personne, ainsi que de toute autre loi du Québec. ».

Normalement, votre micro-ordinateur ne doit servir qu'aux fins de votre travail. Si, en dehors des heures de travail, vous devez consulter des sites à des fins personnelles, ne visitez que des sites à l'abri de toute critique.

Il est interdit de donner suite aux lettres pyramidales, notamment en raison de l'engorgement du courrier électronique qui en découle et pour prévenir toute contamination par des virus. L'écoute de la radio et d'enregistrements vidéo à des fins personnelles, sur le Web, est également interdite.

L'utilisation des nouvelles technologies par tout membre de l'Institut peut faire l'objet d'une vérification ponctuelle et les contrevenants s'exposent, le cas échéant, à des mesures disciplinaires.

L'installation de logiciels et d'équipement

Il est interdit de procéder vous-même à l'installation de logiciels, y compris par téléchargement, de même qu'à l'installation d'équipement. Seule la Direction des technologies de l'information peut s'en charger, notamment pour assurer le respect des droits d'auteur et des règles d'utilisation des licences, pour garantir l'intégrité du parc de micro-ordinateurs en évitant les conflits entre pièces de matériel, la contamination par des virus ou les ralentissements du réseau. (Voir la [Procédure assurant le bon fonctionnement des équipements informatiques](#), sur l'intranet.)

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant la sécurité des technologies de l'information, vous pouvez communiquer avec [Denis Gilbert](#).

La transmission par télécopieur

L'utilisation du télécopieur n'offrant pas de garantie suffisante de sécurité, vous ne devez pas y avoir recours pour transmettre un document contenant des renseignements confidentiels.

Cependant, en cas d'absolue nécessité ou urgence, vous devez respecter rigoureusement les règles dictées par la Commission d'accès à l'information en cette matière et énoncées dans le document que vous pouvez consulter à l'adresse suivante : www.cai.gouv.qc.ca/fra/docu/telecopi.pdf.

Parmi les mesures de sécurité prévues à ce document, vous devez vous assurer : que l'utilisateur remplisse un formulaire d'accompagnement indiquant le nom, l'adresse et le numéro de téléphone de l'expéditeur; que l'utilisateur vérifie, après avoir composé le numéro du télécopieur du destinataire, qu'il n'y a pas eu d'erreur de composition; que cet utilisateur vérifie également le rapport de transmission à la fin de la communication; et qu'il communique avec le destinataire pour s'assurer qu'il a bien reçu le message.

De plus, vous devez voir à ce que le formulaire d'accompagnement contiennent une mention interdisant à la personne qui recevra votre message de le divulguer ou de le reproduire, et l'invitant à vous contacter si votre message lui a été envoyé par erreur.

La protection des renseignements personnels sur les employés

En tant qu'employeur, l'Institut de la statistique du Québec détient obligatoirement un certain nombre de renseignements sur vous, à titre d'employé de l'Institut. Citons, par exemple, votre numéro d'assurance sociale, votre adresse personnelle, votre salaire, peut-être un dossier médical, etc. Cette information, indispensable à l'Institut pour gérer ses ressources humaines, constitue des renseignements personnels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) et elle doit, par conséquent, demeurer strictement confidentielle.

L'Institut a donc adopté la [Politique concernant la protection des renseignements personnels relatifs aux employés](#), laquelle précise notamment les mesures de sécurité qui doivent être respectées en ce qui a trait à l'accès aux documents susceptibles de contenir des renseignements personnels vous concernant en tant qu'employé, de même qu'à la conservation, à la transmission et à la destruction de tels documents.

Les trois types de dossiers sur les employés de l'Institut

Votre **dossier principal** contient l'ensemble des documents originaux sur votre titularisation, votre formation, votre assiduité, votre évaluation; éventuellement, il peut contenir aussi des documents comportant des renseignements à caractère médical. Votre dossier principal est unique et il vous suit tout au long de votre carrière. Votre **dossier secondaire**, par ailleurs, ne contient que des copies de certains documents utiles à la gestion interne de votre unité administrative, comme des copies des évaluations de votre rendement, de vos permis d'absence, etc. Enfin, un **dossier administratif**, ne servant qu'à des fins de contrôle financier, contient des copies des actes de titularisation des employés, des avis de majoration de traitement ou de prime, etc. Ce dossier sert uniquement à évaluer les dépenses de rémunération dans les projets.

La détention et la consultation

Le Service des ressources humaines conserve votre dossier principal. Vous seul, de même que toute personne à qui vous auriez accordé, par écrit, ce droit d'accès, pouvez consulter votre dossier principal. De plus, vos supérieurs immédiat et hiérarchique peuvent, sans votre autorisation, consulter ce dossier, à l'exclusion des documents comportant des renseignements à caractère médical et qui sont conservés séparément.

Votre dossier secondaire doit être gardé en tout temps dans un classeur verrouillé de votre unité administrative. Il n'est accessible qu'à vos supérieurs immédiat et hiérarchique, ainsi qu'à une personne désignée.

Les dossiers administratifs de contrôle financier ne sont accessibles qu'à des personnes désignées par la Direction de l'administration.

La transmission

La transmission par la poste de documents contenant des renseignements personnels vous concernant doit être faite uniquement dans des enveloppes cachetées portant la mention « Confidentiel ». L'usage du télécopieur n'est pas recommandé, puisqu'il n'offre pas de garanties suffisantes de confidentialité. En cas de nécessité ou d'urgence, une telle transmission doit se faire en respectant strictement la [directive relative à la transmission par télécopieur](#). Quant à la transmission de renseignements personnels par courrier électronique, elle doit également être conforme à la [procédure établie en cette matière](#).

La destruction

Tout document contenant des renseignements personnels sur un employé doit être détruit par une déchiqueteuse ou déposé dans un bac scellé en attendant sa destruction.

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant la protection des renseignements personnels relatifs aux employés, vous pouvez communiquer avec [Caroline Saint-Pierre](#).

La Politique de communication en vertu des articles 27 et 28 de la Loi sur l'Institut de la statistique du Québec

En vertu de la Loi sur l'Institut de la statistique du Québec, le directeur général de peut autoriser la communication de renseignements recueillis, à leurs propres fins, par des organismes publics et communiqués à l'Institut ([article 27](#)), de même qu'il peut autoriser la communication, sous forme d'index ou de listes, de certains renseignements obtenus par l'Institut, par exemple des listes de noms et d'adresses d'entreprises selon les secteurs d'activité économique, ou encore des listes de produits fabriqués par des entreprises. a communication ([article 28](#)).

La [Politique de communication en vertu des articles 27 et 28 de la Loi sur l'Institut de la statistique du Québec de renseignements individuels relatifs aux entreprises ou assimilés obtenus par l'Institut](#) énonce les conditions à satisfaire et la marche à suivre pour obtenir l'autorisation du directeur général pour une telle communication, et elle précise les modalités de contrôle et de suivi de l'utilisation des renseignements ainsi communiqués.

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant la Politique de communication en vertu des articles 27 et 28 de la Loi sur l'Institut de la statistique du Québec de renseignements individuels relatifs aux entreprises ou assimilés obtenus par l'Institut, vous pouvez communiquer avec [Camille Courchesne](#).

L'exploitation des fichiers de microdonnées des enquêtes de l'Institut

Pour l'aider à exploiter les données qu'il détient et pour en tirer toute la connaissance scientifique qui peut être dégagée de cette information statistique, l'Institut peut retenir les services de personnes ne faisant pas partie de son personnel. Le directeur général peut ainsi embaucher des analystes et des chercheurs externes, dans les organismes publics et le milieu universitaire, pour l'aider dans sa fonction d'analyse et de recherche.

La **Politique relative à l'exploitation des fichiers de microdonnées des enquêtes de l'ISQ** précise les modalités de cette collaboration. Par exemple, elle prévoit que toutes ces personnes sont soumises aux mêmes engagements de confidentialité que les employés de l'Institut et qu'elles doivent, notamment, signer un engagement à la confidentialité. Cette politique stipule également que les mandats confiés à ces personnes font l'objet d'ententes ou de contrats prévoyant de façon très explicite des garanties de confidentialité et des mesures administratives, physiques et technologiques propres à assurer la sécurité de l'information qui leur est confiée. La Politique prévoit également que toute demande d'exploitation d'un tel fichier est soumise à un comité d'examen.

Les données d'enquête que l'Institut met ainsi à la disposition de ces analystes et de ces chercheurs sont soumises à des techniques de masquage inspirées des meilleures pratiques en ce domaine dans le monde. Grâce à ce masquage, l'Institut peut mettre à la disposition des analystes et des chercheurs externes des fichiers de microdonnées d'enquête comportant un potentiel analytique élevé, tout en minimisant les possibilités d'identification indirecte des répondants. Les données ainsi masquées sont présentées dans un fichier appelé « Fichier aux fins d'analyse ou de recherche externe » (FARE).

Vous avez des questions, des commentaires?

Pour toute question ou tout commentaire concernant l'exploitation des fichiers de microdonnées de l'Institut, vous pouvez communiquer avec **Julie Blackburn**.

Lexique

Authentification

Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

Actifs informationnels

Ensemble des informations textuelles et chiffrées consignées dans les systèmes informatiques de l'Institut, ainsi que les systèmes qui soutiennent cet ensemble. L'actif informationnel de l'Institut peut comprendre une banque de données, un système d'information, une technologie de l'information ou une installation, ou encore un ensemble de ces éléments, acquis ou constitués par l'Institut.

Cryptage

Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Crypter

Transformer une information en un cryptogramme, de manière à la rendre inintelligible à toute personne non autorisée et à en assurer ainsi la confidentialité.

Cryptogramme

Message rendu inintelligible grâce au chiffrement, qui ne peut être compris et utilisé que par les seules personnes en possession de la clé permettant de le déchiffrer.

Disponibilité de l'information

Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Intégrité de l'information

Propriété d'une information ou d'une technologie de l'information de n'être modifiée, ni détruite sans autorisation.

Renseignement d'identité

Tout renseignement permettant d'identifier une personne physique ou morale. Par exemple : nom, numéro d'assurance sociale.