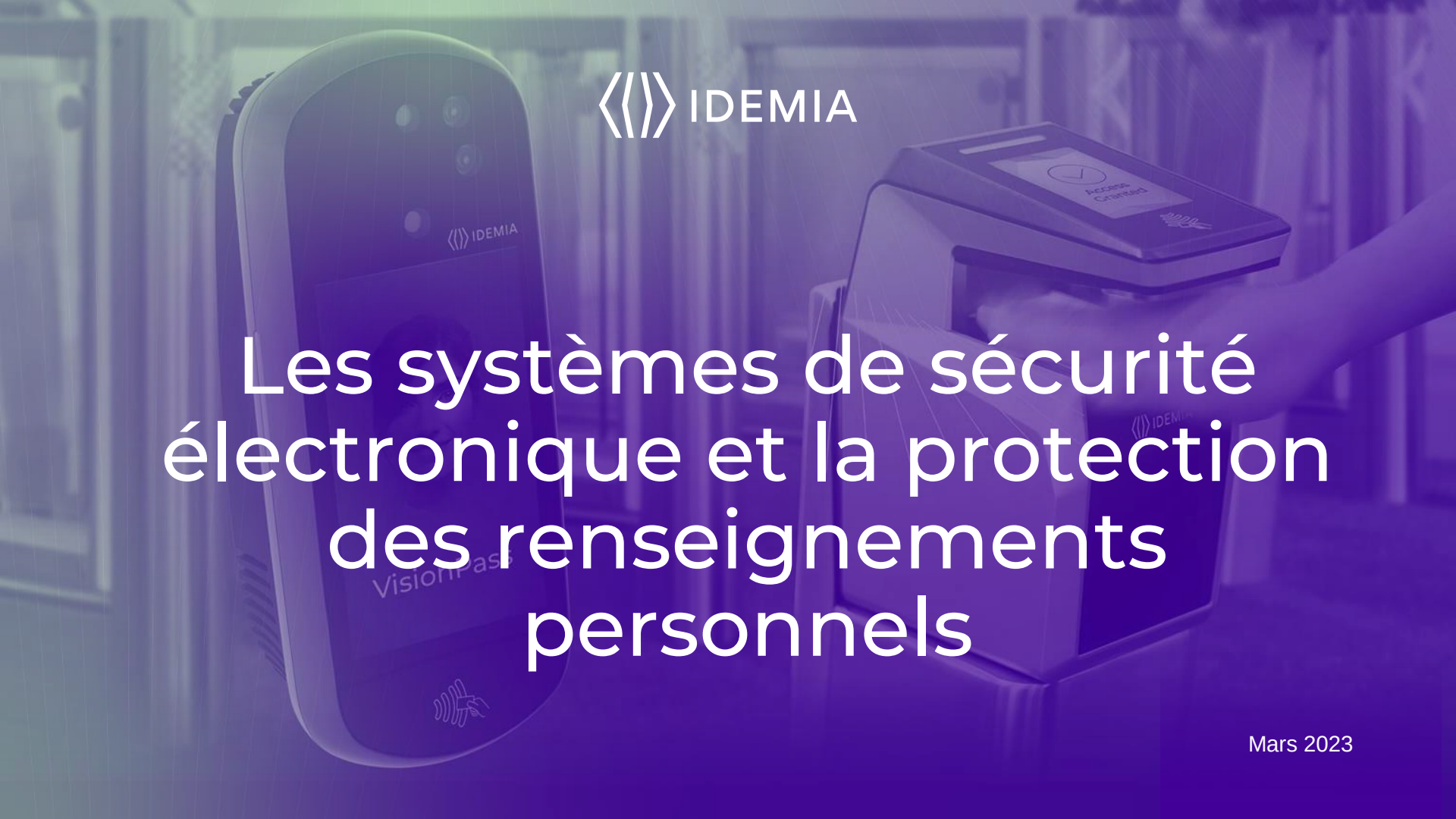


Les systèmes de sécurité électronique et la protection des renseignements personnels

Mars 2023

Nos commanditaires

Commanditaires Or

AREA SYSTÈME DE SÉCURITÉ

Securitas

Commanditaires Argent

Stantec

Consultants techniques TECHNILOGIC Spécialiste en systèmes de sécurité

AUTOMATIC SYSTEMS

Concordia UNIVERSITY

Genetec

Convergint TECHNOLOGIES

PROTECT IP SOLUTIONS GLOBALES

IDEMIA augmented identity

AXIS

GARDAWORLD

ALLIED UNIVERSAL

MIRADES

Mission ASIS Province de Québec

Offrir aux membres de la communauté montréalaise de la sécurité un lieu de rencontre favorisant le réseautage et le perfectionnement professionnel, tout en leur fournissant des outils d'information et de formation leur permettant de demeurer à l'avant-garde des meilleures pratiques, et favoriser la professionnalisation et la reconnaissance des métiers de la sécurité au sein de la communauté des affaires du Québec.

ASIS Certification

Certified Protection Professional (CPP®)
The Certified Protection Professional (CPP) is considered the "gold standard" for security management professionals. This certification validates your knowledge in all areas of security management. Eligibility requirements include 5-7 years of security experience and 3 years in responsible charge of a security function.

Professional Certified Investigator (PCI®)
The Professional Certified Investigator (PCI) certification provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. Requirements include 3-5 years of investigations experience, with at least two years in case management.

Associate Protection Professional (APP)
The Associate Protection Professional (APP) designation provides the first "rung" on the security manager's career ladder. It is for those with 1-3 years of security management experience and measures the professional's knowledge of security management fundamentals, business operations, risk management, and response management.

Physical Security Professional (PSP®)
The Physical Security Professional (PSP) demonstrates your knowledge in physical security assessments, application, design, and integration of physical security systems, and implementation of security measures. Eligibility requirements include 3-5 years of experience in the physical security field.

Qu’est-ce qu’un «renseignements personnels»

Selon la Commission d’accès a l’information du Québec:

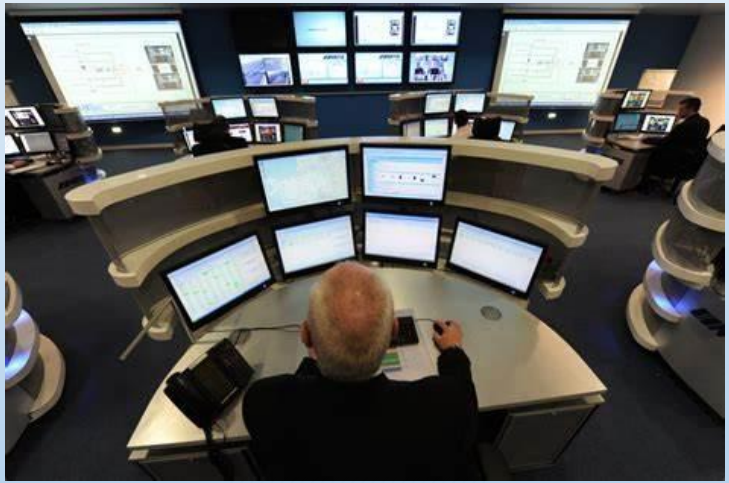
«Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l’identifier. Ils sont confidentiels. Sauf exceptions, ils ne peuvent être communiqués sans le consentement de la personne concernée».

Date de naissance,
Age,
No d’assurance sociale,
No d’employé,
Origine ethnique,
Sexe,
Religion,
État matrimoniaux,

Taille, poids,
Groupe sanguin,
ADN,
Antécédents médicaux,
Antécédents professionnels,
Éducation,
Revenus,
Habitudes de consommation,

Adresse,
Adresse ip,
Adresse Courriel,
Message courriel,
No de téléphone,
Solvabilité,
Renseignements bancaires,
Données biométriques,

Communication de masse



Rapport d’incident

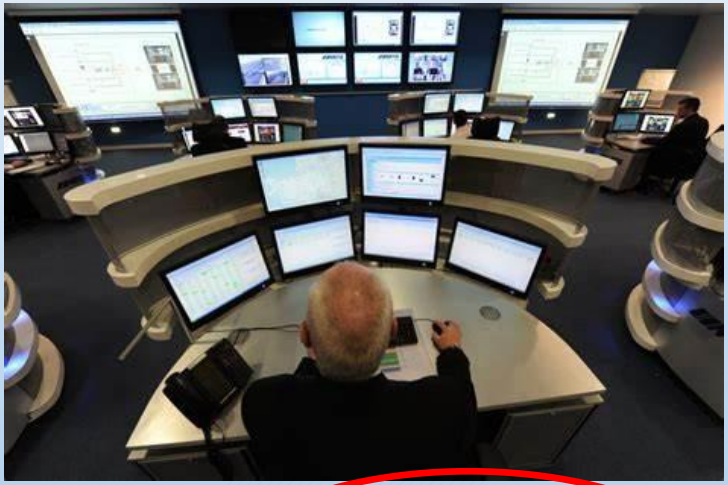
Contrôle d’accès

Vérifications routinières

Détection d’intrusion

Gestion des visiteurs

Communication de masse



Rapport d’incident

Contrôle d’accès

Vérifications routinières

Détection d’intrusion

Gestion des visiteurs

Contrôle d’accès

Protéger les renseignements personnels

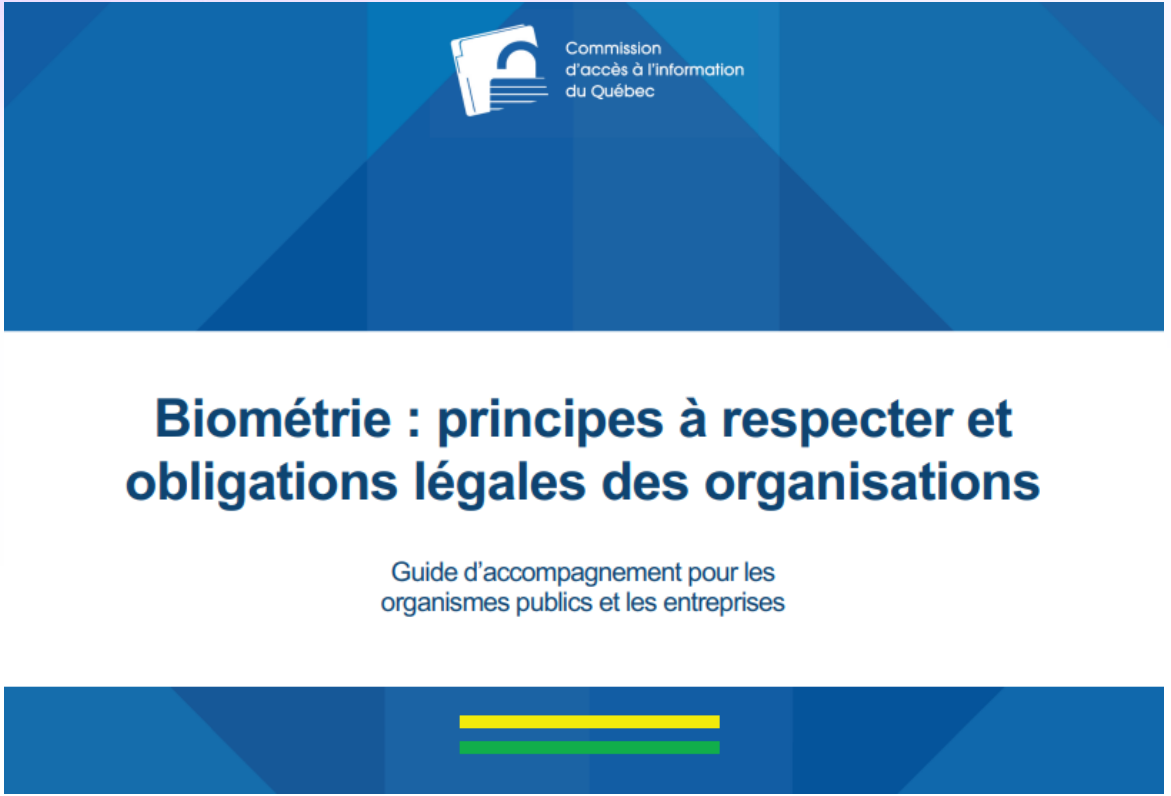
- Ne conserver que les renseignements requis dans la base de donnée du système de contrôle d’accès.
- Droit a l’oublie
- Assurer un contrôle étroit de l’accès aux renseignements personnel (et aux données historiques).

Augmenter le niveau de sécurité de l’information

- Utiliser des technologies de carte sécuritaire
- Activer la communication certifiée (TLS 1.2)
- Éviter la communication Wiegand

Contrôle d’accès biométrique

[Biométrie : principes à respecter et obligations légales des organisations (gouv.qc.ca)]



Contrôle d’accès biométrique

- Consentement explicite
- Alternative
- Droit a l’oublie
- Dépôt du formulaire de déclaration a la CAI 60 jours avant la mise en service
- Évaluation des facteurs relatif a la vie privée (Privacy Impact assement, PIA)

Notez qu’à partir du 22 septembre 2023, il sera obligatoire de procéder à une évaluation des facteurs relatifs à la vie privée pour tout projet d’acquisition, de développement et de refonte d’un système d’information ou de prestation électronique de services impliquant la collecte, l’utilisation, la communication, la conservation ou la destruction de renseignements personnels. La Commission offre déjà un guide d’accompagnement à cette démarche.

Contrôle d'accès biométrique

Faites l'analyse préliminaire
(nécessité et proportionnalité)

- Réalisez si possible une évaluation des facteurs relatifs a la vie privée
  (Obligatoire a compter de septembre 2023)

Déclarez a la Commission au moyen du formulaire prévue a cet effet

- Tout procédé permettant de saisir des caractéristiques biométriques a des fins d'indentification avant de l'utiliser.
- La création d'une banque de caractéristique ou de mesure biométriques au moins 60 jours avant sa mise en service

Respectez vos obligations

- Consentement exprès
  (voir le formulaire type)
- Autre moyen d'identification (alternative)
- Respect de la finalité de la collecte
- Mesures de confidentialité et sécurité
- Destruction sécuritaire et définitive
- Droit d'accès et de rectification

Gestion des dossiers d’incident

- Ne conserver que les renseignements requis
- Droit a l’oublie
- Évaluation des facteurs relatif a la vie privée (Privacy Impact assement, PIA)

Notez qu’à partir du 22 septembre 2023, il sera obligatoire de procéder à une évaluation des facteurs relatifs à la vie privée pour tout projet d’acquisition, de développement et de refonte d’un système d’information ou de prestation électronique de services impliquant la collecte, l’utilisation, la communication, la conservation ou la destruction de renseignements personnels. La Commission offre déjà un guide d’accompagnement à cette démarche.

Gestion des Visiteurs

- Ne conserver que les renseignements requis
- Droit a l'oublie
- Évaluation des facteurs relatif a la vie privée (Privacy Impact assement, PIA)

Notez qu'à partir du 22 septembre 2023, il sera obligatoire de procéder à une évaluation des facteurs relatifs à la vie privée pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. La Commission offre déjà un guide d'accompagnement à cette démarche.

Vidéo Surveillance

[VIDEOSURVEILLANCE_CAI.indd (gouv.qc.ca)]

Document en cours de révision

Commission d'accès à l'information du Québec

LA VIDÉOSURVEILLANCE

Conseils pratiques à l'intention des organismes publics et des entreprises

photo : www.istockphoto.com

INTRODUCTION

Le but de ce document est de sensibiliser les organismes publics et les entreprises du Québec aux enjeux de protection des renseignements personnels que soulève le recours à la vidéosurveillance. Bien que la vidéosurveillance soit de plus en plus répandue, son utilisation doit respecter les dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[1] dans le cas d'un organisme public ou celles de la Loi sur la protection des renseignements personnels dans le secteur privé[2] dans le cas d'une entreprise. En effet, l'image d'une personne identifiable qui se trouve sur un support constitue un renseignement personnel[3]. Cette image peut avoir été captée par une caméra de surveillance, un drone ou toute autre technologie de cette nature.

Le présent document vise à proposer de bonnes pratiques en la matière. Il peut être utilisé pour évaluer un système de vidéosurveillance existant ou pour guider un projet impliquant l'utilisation de caméras dans des lieux publics ou privés afin d'enregistrer des images avec ou sans son.

PREMIÈRE ÉTAPE : PUIS-JE RECOURIR À LA VIDÉOSURVEILLANCE?

Avant de recourir à la vidéosurveillance, un organisme public ou une entreprise devrait s'interroger sur la nécessité[4] de recueillir des images au sujet d'individus par le biais de cette technologie en répondant aux questions suivantes :

- Pourquoi recourir à la vidéosurveillance? Quel est le but poursuivi par l'installation d'un tel système?
- Cet objectif est-il légitime, important, urgent et réel?
- Si oui, l'atteinte au droit fondamental à la vie privée que constitue la collecte d'images d'individus est-elle proportionnelle à l'objectif poursuivi[5]?

De plus, certains organismes publics[6] ont l'obligation de consulter le comité sur l'accès à l'information et la protection des renseignements personnels qui relève du sous-ministre ou du dirigeant de l'organisme au sujet des mesures à respecter. Celles-ci doivent comprendre notamment une évaluation de la nécessité de recourir à cette technologie et une évaluation de la conformité de l'utilisation de cette technologie par rapport au droit au respect de la vie privée[7].

1 Quel est le but poursuivi par l'installation d'un tel système?

Pour évaluer si vous pouvez recueillir des renseignements personnels au moyen de la vidéosurveillance, il faut d'abord vous demander quel est l'objectif poursuivi. Quelle situation ou quels problèmes voulez-vous résoudre? Pourquoi recueillir des renseignements personnels par vidéosurveillance? Soyez précis.

2 Cet objectif est-il légitime, important, urgent et réel?

Une fois le but poursuivi par le recours à la vidéosurveillance déterminé et circonscrit, évaluez si cet objectif justifie la collecte de renseignements personnels qui sera faite par les caméras. Cet objectif doit être légitime, c'est-à-dire justifié et fondé en droit ou en équité.

Posez-vous les questions suivantes :

- L'utilisation de la vidéosurveillance telle que projetée est-elle contraire à la Charte des droits et libertés de la personne[8] ou interdite par d'autres dispositions légales?
- Dans le cas d'un organisme public : quel est le lien entre l'objectif poursuivi et ses attributions ou un mandat dont il a la gestion?

Vidéo Surveillance

Première étape: Puis-je recourir a la vidéo surveillance

1. **Quel est le but poursuivi par l'installation d'un tel système**

2. **Cet objectif est-il légitime, important, urgent et réel?**

   L'utilisation de la vidéosurveillance telle que projetée est-elle contraire à la Charte des droits et libertés de la personne ou interdite par d'autres dispositions légales?

   Dans le cas d'un organisme public : quel est le lien entre l'objectif poursuivi et ses attributions ou un mandat dont il a la gestion ?

3. **Si oui, l'atteinte au droit fondamental à la vie privée que constitue la collecte d'images d'individus est-elle proportionnelle à l'objectif poursuivi?**

   Doit être nettement plus utile à l'organisme ou à l'entreprise que préjudiciable aux personnes dont les images sont captées.

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

1. Adoptez une politique concernant la vidéosurveillance et désignez une personne qui en est responsable
2. Informez le public ou les personnes concernées de la présence de caméras et de la collecte de renseignements personnels les concernant
3. Limitez la portée de la vidéosurveillance
4. Assurez la sécurité des images recueillies
5. Limitez l’accès aux images recueillies et leur utilisation
6. Détruisez de manière sécuritaire les images dès qu’elles ne sont plus nécessaires

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

7. Prévoyez l’accès aux images par les personnes concernées

8. Consultez le comité sur l’accès à l’information et la protection des renseignements personnels si vous êtes un organisme public assujetti au Règlement sur la diffusion

9. Réévaluez périodiquement la nécessité de la vidéosurveillance et la politique

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

1. Adoptez une politique concernant la vidéosurveillance et désignez une personne qui en est responsable

    - Préciser pourquoi vous avez recours à la vidéosurveillance
    - Définir les règles d'installation et d'utilisation des caméras et des autres appareils
    - Définir les mesures de sécurité qui s'appliqueront aux renseignements personnels collectés et leur durée de conservation
    - Déterminer qui, au sein de l'organisme ou de l'entreprise, aura accès aux images ainsi captées
    - Circonscrire l'utilisation permise des images recueillies
    - Établir un cadre de gestion des demandes d'accès aux renseignements personnels conservés par vidéosurveillance
    - Désigner une personne responsable de la gestion de la vidéosurveillance et des demandes d'accès aux renseignements

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

2. Informez le public ou les personnes concernées de la présence de caméras et de la collecte de renseignements personnels les concernant

    - Afin d'informer les personnes concernées que vous recueillez des renseignements personnels à leur sujet, avisez-les de la présence de caméras et de la collecte de renseignements personnels qui en découle. Cela peut se faire par le biais d'affiches bien en vue dans les endroits visés par la vidéosurveillance.

    - L'ajout du numéro de téléphone où une personne responsable peut être jointe en cas de question constitue une pratique encouragée.

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

3. Limitez la portée de la vidéosurveillance

- À la lumière de la réflexion que vous avez faite à l'étape 1, planifiez soigneusement le nombre de caméras requises, les endroits où elles seront installées et leur mode de fonctionnement afin de ne recueillir que les images nécessaires pour solutionner le problème ciblé. Rappelez-vous d'éviter les endroits où l'expectative de vie privée et d'intimité est très élevée

- Déterminez seulement les moments où les caméras doivent être en fonction pour atteindre l'objectif visé

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

4. Assurez la sécurité des images recueillies

- Assurez-vous que les locaux où se trouvent les équipements qui permettent de visionner les images de vidéosurveillance sont verrouillés et protégés.
- Limitez le nombre de personnes qui peuvent avoir accès au local et à l'équipement contenant les enregistrements à celles dont les tâches requièrent qu'elles aient accès à ces renseignements. Il peut y avoir un registre d'accès aux locaux et aux images.
- Protégez l'accès aux équipements d'enregistrement par des mots de passe ou d'autres moyens efficaces. Les images peuvent aussi être cryptées pour plus de sécurité.
- Sensibilisez les personnes autorisées aux règles visant le respect de la vie privée et la protection des renseignements personnels recueillis par vidéosurveillance

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

4. Assurez la sécurité des images recueillies

- Faites signer des engagements à la confidentialité aux personnes qui ont accès aux appareils et aux renseignements.
- Ayez un plan (politique, directive ou autre) pour agir rapidement en cas d'incident de sécurité impliquant les renseignements personnels recueillis par vidéosurveillance.

Vous pouvez vous référer à l'aide-mémoire de la Commission à l'intention des organismes et des entreprises Quoi faire en cas de perte ou de vol de renseignements personnels? sur le site de la Commission: www.cai.gouv.qc.ca

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

5. Limitez l’accès aux images recueillies et leur utilisation

- Précisez qui, au sein de votre organisme ou de votre entreprise, peut avoir accès aux enregistrements et dans quelles situations, en lien avec ses fonctions

- Prévoyez également à quelles fins les images enregistrées peuvent être utilisées (celles-ci devraient être compatibles avec les utilisations envisagées lors de la collecte).

- Assurez-vous que les enregistrements ne seront pas communiqués à des tiers, sauf avec les autorisations requises. Le cas échéant, prévoyez les modalités d’ententes avec les fournisseurs ou les opérateurs de services en vidéosurveillance quant à leurs obligations et à leurs responsabilités

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

6. Détruisez de manière sécuritaire les images dès qu'elles ne sont plus nécessaires

Établissez un calendrier de conservation des enregistrements selon vos besoins en gardant à l'esprit qu'ils devraient être détruits dès que possible. Assurez-vous de respecter ces délais.

- La conservation des images pour une durée de 30 jours est un délai généralement suffisant et recommandé.
- Prévoyez des moyens sécuritaires pour détruire de manière irréversible les enregistrements. Vous pouvez vous référer à la fiche d'information : La destruction des documents contenant des renseignements personnels sur le site de la Commission: www.cai.gouv.qc.ca

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

7. Prévoyez l’accès aux images par les personnes concernées

   - Puisque les personnes présentes sur les enregistrements ont le droit d’avoir accès aux renseignements personnels qui les concernent, prévoyez comment et à qui une telle demande doit être faite.

   - Assurez-vous de ne pas révéler des renseignements personnels au sujet d’autres personnes à moins que la loi ne le permette

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

8. Consultez le comité sur l'accès à l'information et la protection des renseignements personnels si vous êtes un organisme public assujetti au Règlement sur la diffusion

   - Si vous êtes un organisme public assujetti au Règlement sur la diffusion, évaluez la conformité de l'utilisation de la vidéosurveillance par rapport au droit au respect de la vie privée.

   - Informez le comité sur l'accès à l'information et la protection des renseignements personnels des résultats de cette évaluation

Vidéo Surveillance

Seconde étape: Autre exigences de protection des renseignements personnels

9. Réévaluez périodiquement la nécessité de la vidéosurveillance et la politique

- Refaites l'évaluation prévue à l'étape 1 du présent document de manière périodique
- Cessez l'utilisation de la vidéosurveillance dès qu'elle n'est plus nécessaire

Vidéo Surveillance

DÉCISIONS DE LA COMMISSION

- Coopérative d'habitation de la Solidarité Cartierville, 100 52 83, 29 août 2017
- Ville de Québec, 101 18 20, 6 mars 2017
- Apple Canada inc. (Apple Store du Carrefour Laval), 100 88 19, 29 novembre 2016
- Garderie Excelsiori Daycare inc., 11 17 56, 5 octobre 2016
- Corporation immobilière Omers, 100 95 57, 16 mars 2016
- Coopérative d'habitation Chung Hua, 100 49 29, 16 mars 2016
- Star Bar (9142-1891 Québec inc.), 100 64 26, 9 mars 2015
- Bronzage Soleil autour du monde, 100 74 83, 24 novembre 2014
- Garderie Cœur d'enfant inc., 08 02 72, 31 mars 2014
- Revenu Québec, 1015611-S, 23 novembre 2018.

CONTACT

Denis Bourget
Vice-President Strategic Account
Biometric Devices

denis.bourget@idemia.com

+1 438-998-6204

Join us on

www.idemia.com