

PAR COURRIEL

Québec, le 7 août 2025

N/Réf. : 2025-12467

OBJET: ***Votre demande en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)***

Madame,

Nous faisons suite à votre demande d'accès reçue le 21 juillet 2025, visant à obtenir « *pour tous services, logiciels ou technologies liés à la surveillance, y compris sans s'y limiter : a) Les drones b) Les caméras portatives c) Les technologies de reconnaissance automatique des plaques d'immatriculation d) Les technologies de reconnaissance biométrique (faciale, d'empreintes digitales, oculaire, vocale et autre) e) Les caméras de surveillance (incluant les ententes avec la compagnie Ring) f) Les intercepteurs d'IMSI (IMSI-Catchers) g) Les bases de données des compagnies de télécommunications h) Toutes autres technologies de surveillance, les documents suivants* » :

Concernant le point h), le 24 juillet dernier, vous avez apporté cette précision : *toutes technologies qui permettent de surveiller, de guetter, de profiler, de collecter des informations sur les individus, les groupes d'individus, leurs comportements, et leurs activités, notamment leurs comportements et leurs activités en ligne* ».

1. *Tout contrat, appel d'offres, devis, facture ou entente entre le ministère de la Sécurité publique et un fournisseur de ces services, logiciels ou technologies.*
2. *Tout document contenant de l'information sur les politiques internes, l'utilisation ou la formation à l'utilisation de ces services, logiciels ou technologies* ».

Le ministère de la Sécurité publique (MSP) n'a repéré aucun document visé par votre demande. Pour votre information, le MSP n'effectue aucune surveillance de

...2

la population. Celle-ci est plutôt orientée vers des territoires, des systèmes et des personnes contrevenantes assujetties à une ordonnance du Tribunal. En application de l'article 1 de la Loi sur l'accès, nous sommes dans l'impossibilité de donner suite à votre demande.

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez, en vertu de la section III du chapitre IV de cette loi (articles 135 et suivants), faire une demande de révision à l'égard de cette décision en vous adressant à la Commission d'accès à l'information dans les 30 jours suivant la date de la présente décision. À cet effet, vous trouverez joint à la présente le document intitulé Avis de recours.

Veuillez agréer, Madame, nos salutations distinguées.

La responsable de l'accès aux documents,

Original signé

Nadine Léveillé

p. j. Article de la loi et avis de recours en révision

Chapitre A-2.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

CHAPITRE I **APPLICATION ET INTERPRÉTATION**

1. La présente loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers.

Elle s'applique quelle que soit la forme de ces documents: écrite, graphique, sonore, visuelle, informatisée ou autre.

1982, c. 30, a. 1.

AVIS DE RECOURS EN RÉVISION

Avis de recours à la suite d'une décision rendue par le ministère de la Sécurité publique en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Révision par la Commission d'accès à l'information

a) Pouvoir : l'article 135 de la Loi prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision. La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec

Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal

Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

b) Motifs : les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais : les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

PAR COURRIEL

Québec, le 13 août 2025

N/Réf. : 2025-12467

OBJET: Votre demande en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1)

Madame,

Nous faisons suite à votre demande d'accès reçue le 21 juillet 2025, visant à obtenir « *pour tous services, logiciels ou technologies liés à la surveillance, y compris sans s'y limiter : a) Les drones b) Les caméras portatives c) Les technologies de reconnaissance automatique des plaques d'immatriculation d) Les technologies de reconnaissance biométrique (faciale, d'empreintes digitales, oculaire, vocale et autre) e) Les caméras de surveillance (incluant les ententes avec la compagnie Ring) f) Les intercepteurs d'IMSI (IMSI-Catchers) g) Les bases de données des compagnies de télécommunications h) Toutes autres technologies de surveillance, les documents suivants* » :

Concernant le point h), le 24 juillet dernier, vous avez apporté cette précision : *toutes technologies qui permettent de surveiller, de guetter, de profiler, de collecter des informations sur les individus, les groupes d'individus, leurs comportements, et leurs activités, notamment leurs comportements et leurs activités en ligne* ».

1. *Tout contrat, appel d'offres, devis, facture ou entente entre le ministère de la Sécurité publique et un fournisseur de ces services, logiciels ou technologies.*

2. *Tout document contenant de l'information sur les politiques internes, l'utilisation ou la formation à l'utilisation de ces services, logiciels ou technologies* ».

...2

Depuis la transmission de la première réponse le 7 août dernier, nous avons repéré de nouveaux documents. La présente vise donc à vous en informer d'une part, puis de vous les communiquer. Vous constaterez qu'un seul passage a été masqué en vertu de l'article 29 de la Loi sur l'accès. Si révélé, l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne pourrait être réduit.

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez, en vertu de la section III du chapitre IV de cette loi (articles 135 et suivants), faire une demande de révision à l'égard de cette décision en vous adressant à la Commission d'accès à l'information dans les 30 jours suivant la date de la présente décision. À cet effet, vous trouverez joint à la présente le document intitulé Avis de recours.

Veuillez agréer, Madame, nos salutations distinguées.

La responsable de l'accès aux documents,

Original signé

Nadine Léveillé

p. j. Article de la loi et avis de recours en révision

Chapitre A-2.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

CHAPITRE II

ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

SECTION II

RESTRICTIONS AU DROIT D'ACCÈS

§ 4. — *Renseignements ayant des incidences sur l'administration de la justice et la sécurité publique*

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi. Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

1982, c. 30, a. 29; 2006, c. 22, a. 16.

AVIS DE RECOURS EN RÉVISION

Avis de recours à la suite d'une décision rendue par le ministère de la Sécurité publique en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Révision par la Commission d'accès à l'information

a) Pouvoir : l'article 135 de la Loi prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision. La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec

Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal

Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

b) Motifs : les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais : les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

POLITIQUE SUR L'UTILISATION DE CAMÉRAS DE SURVEILLANCE

AU SIÈGE SOCIAL DU

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE

Novembre 2011

TABLE DES MATIÈRES

1. Objet	3
2. Champ d'application	3
3. Cadre de référence	3
4. Principes.....	4
5. Plan de surveillance par caméras	4
6. Gestion des renseignements	5
7. Avis apposé aux endroits sous surveillance	5
8. Formation du personnel	6
9. Délai de conservation des enregistrements	6
10. Révision de la politique	6
11. Date d'entrée en vigueur	6
Annexe - Lexique.....	7

1. Objet

Le siège social du ministère de la Sécurité publique (MSP) est équipé d'un système de surveillance par caméras vidéo dont les images peuvent être enregistrées et conservées.

Cette politique définit les principes et les modalités d'installation du système de surveillance par caméras de surveillance ainsi que les règles de conservation et de consultation des renseignements produits par ce système.

2. Champ d'application

Cette politique s'applique au siège social du ministère de la Sécurité publique situé au 2525, boulevard Laurier, Québec. Elle porte sur l'accès aux enregistrements qui sont produits par le système de surveillance par caméras.

3. Cadre de référence

Cette politique s'appuie sur le cadre légal et administratif suivant :

- Charte des droits et libertés de la personne (art. 5);
- Code civil du Québec (art. 35 et art. 36);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- Loi sur les archives (L.R.Q., c. A-2.1.1);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (c. A-2.1, r. 0.2);
- Règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics (Commission d'accès à l'information du Québec, juin 2004, 7 pages);
- Directive en matière d'examen administratifs et d'enquêtes (<http://www.int.msp.gouv.qc.ca/index.php?id=443>);
- Politique ministérielle sur la sécurité de l'information (<http://www.int.msp.gouv.qc.ca/index.php?id=202>);

- Calendrier de conservation des documents
(http://www.int.msp.gouv.qc.ca/fileadmin/documents/Directives_et_politiques/Bureau_sous_ministre/gestion_documentaire/calendrier_conservation_documents.pdf).

4. Principes

Le droit au respect de la vie privée

Le droit à la vie privée d'un employé peut s'étendre à son lieu de travail. Dans ce cas, son droit, qui n'est pas absolu, est subordonné au droit de l'employeur de protéger ses biens, ses informations ainsi que la sécurité des autres employés.

Les images enregistrées sont considérées comme des documents contenant des renseignements personnels. Conséquemment, la conservation et la consultation des enregistrements se font en conformité avec les règles prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Les moyens de surveillance doivent correspondre aux besoins de protection

Le système mis en place pour la surveillance par caméras est proportionné aux besoins en matière de sécurité des personnes, des informations et des biens. Les endroits surveillés et les moments durant lesquels se fait la surveillance doivent présenter des risques suffisants pour justifier le recours à ce moyen de protection en tenant compte des autres mesures de sécurité en place.

L'utilisation d'un système de surveillance par caméras doit être réévaluée périodiquement pour tenir compte des changements apportés à l'ensemble des systèmes de protection et de l'évolution des risques en matière de sécurité.

5. Plan de surveillance par caméras

Le responsable de la sécurité rédige un plan de surveillance par caméras qui vise à réduire les risques et les dangers en matière d'ordre public et de sécurité des personnes, des informations et des biens malgré les mesures de sécurité déjà en place.

Le plan de surveillance par caméras comprend notamment :

- ✓ une analyse des risques et des dangers en matière d'ordre public et de sécurité des personnes, des informations et des biens en tenant compte des systèmes de sécurité existants;
- ✓ la localisation des caméras de surveillance et l'indication de leur champ de vision;

- ✓ les périodes d'enregistrement des images;
- ✓ les mesures prises afin de protéger les données enregistrées.

Le plan de surveillance par caméras est soumis au comité ministériel chargé de la protection des renseignements personnels avant son approbation. Ce dernier rend une opinion sur la nécessité de recourir à la surveillance par caméras et sur la conformité de l'utilisation de ces caméras au droit au respect de la vie privée.

Le personnel est consulté sur le plan de surveillance par caméras avant qu'il ne soit adopté. La consultation se fait par l'intermédiaire des comités ministériels des relations professionnelles (CMRP).

Le responsable ministériel de la sécurité autorise la mise en application du plan de surveillance après avoir pris connaissance des opinions découlant des consultations.

6. Gestion des renseignements

Seul le personnel chargé du fonctionnement et de l'entretien du système de surveillance par caméras peut visionner les enregistrements. La liste de ces personnes est consignée dans un registre.

Toute personne a droit de visionner les enregistrements personnels qui la concerne. La demande de visionnement doit être adressée au responsable ministériel de l'accès aux documents et de la protection des renseignements personnels. Ce dernier rend un avis en se basant sur les règles d'accès aux renseignements personnels.

Les enregistrements peuvent être utilisés aux fins d'enquête administrative selon les modalités prévues par la Directive en matière d'examen administratifs et d'enquêtes.

Les enregistrements qui ont été consultés ainsi que les dates et les motifs de consultation sont consignés dans un registre.

7. Avis apposé aux endroits sous surveillance

Un avis doit être apposé aux endroits où les caméras sont installées afin d'informer le personnel et les visiteurs qu'ils vont pénétrer dans une zone sous surveillance par caméras. Cet avis indique les coordonnées où joindre la personne responsable de la gestion des caméras.

Lorsqu'une caméra est installée à proximité d'une aire de travail, l'avis doit préciser son champ de vision.

8. Formation du personnel

Le personnel qui assure le fonctionnement des appareils, ou qui les utilise, y compris le personnel engagé à contrat, doit avoir reçu une formation appropriée portant sur les règles en matière de protection des renseignements personnels et de la vie privée.

9. Délai de conservation des enregistrements

Les renseignements personnels recueillis et enregistrés dans une base de données informatisée sont conservés pendant une période maximale de 30 jours puis détruits de façon systématique. Cependant, lorsque des enregistrements sont utilisés aux fins d'une enquête, ils sont conservés pendant la durée de cette enquête et détruits à la fin des procédures.

10. Révision de la politique

La présente politique est révisée au besoin.

11. Date d'entrée en vigueur

Cette politique entre en vigueur le 1^{er} novembre 2011.

Annexe - Lexique

Comité ministériel chargé de la protection des renseignements personnels : Comité mis sur pied en vertu du deuxième alinéa de l'article 2 du Règlement sur la diffusion de l'information et de la protection des renseignements personnels (c. A-2.1, r. 0.2).

Renseignements personnels : Tout renseignement qui concerne une personne physique et qui permet de l'identifier. Toute donnée, toute image ou tout son enregistré qui permet d'identifier une personne représente un renseignement personnel.

Système de surveillance vidéo : Système ou dispositif mécanique, électronique ou numérique qui permet l'enregistrement vidéo continu ou périodique, l'observation ou la surveillance de renseignements personnels relatifs à un individu.

Personnel : Personne à l'emploi du ministère de la Sécurité publique possédant le statut de régulier, temporaire, contractuel, étudiant, stagiaire ou sous-traitant.

Plan de surveillance par caméras : Document qui décrit le système de surveillance par caméras, localise les endroits où sont installées les caméras, leurs champs de vision, les périodes d'enregistrement ainsi que les mesures de sécurité mises en place pour protéger les renseignements recueillis par ce système.

Visiteur : Personne effectuant une courte visite dans les locaux du ministère pour des raisons d'affaires ou personnelles.

Zone de travail : Secteur dont l'accès est limité aux employés et aux visiteurs autorisés.

DIRECTIVE ADMINISTRATIVE

	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

1. BUT

Cette directive encadre l'utilisation et la gestion des systèmes de contrôle des accès et de vidéosurveillance permettant d'assurer la sécurité et le maintien de l'ordre dans les palais de justice sous la responsabilité de la Direction de la sécurité dans les palais de justice (DSPJ) et a pour objectif d'en prôner un usage professionnel et éthique, dans le respect des lois et règlements en vigueur.

2. CADRE LÉGAL, RÉGLEMENTAIRE ET RÉFÉRENCES

Charte des droits et libertés de la personne (LRQ, c. C-12);

Code civil du Québec (CCQ-1991);

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, c. A-2.1);

Loi sur les archives (LRQ, c. A-21.1);

Loi concernant le cadre juridique des technologies de l'information (LRQ, c. C-1.1);

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (LRQ, c. A-2.1, r.2);

Règlement sur les incidents de confidentialité (LRQ, c. A-2.1, r.3.1);

Règlement sur l'éthique et la discipline dans la fonction publique (LRQ, c. F-3.1.1, r.3);

Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics, Commission d'accès à l'information du Québec (juin 2004);

Ministère de la Sécurité publique, notamment les documents :

- Politique ministérielle sur la protection des renseignements personnels;

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 1 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

 Sécurité publique Québec	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

- Politique ministérielle de sécurité de l'information;
- Politique sur l'utilisation des caméras de surveillance au siège social;
- Directive ministérielle sur la gestion des accès au siège social;
- Directive en matière d'examens administratifs et d'enquêtes;

Assemblée nationale du Québec – Instruction 10.01 – Utilisation du système de vidéosurveillance.

3. DÉFINITIONS

Les termes utilisés dans les directives de la Direction générale de la sécurité de l'État (DGSE) sont définis dans le document d'information générale intitulé « Lexique des termes utilisés dans les directives » disponible dans l'Intranet.

4. PRINCIPES DIRECTEURS

4.1 Les informations et images recueillies par les systèmes de contrôle d'accès et de vidéosurveillance sont des renseignements personnels. Elles sont confidentielles et protégées conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

4.2 La DSPJ, dans le cadre de ses obligations et conformément aux dispositions prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, doit s'assurer de la gestion, de la protection, de la conservation et de la disposition de certains renseignements à caractère sensible recueillis par un système de gestion des accès et de vidéosurveillance.

4.3 Comme la DSPJ est responsable de l'ensemble des renseignements qu'elle recueille, utilise, conserve, élimine et communique, elle doit s'assurer de former et sensibiliser son personnel aux règles visant le respect de la vie privée ainsi qu'en matière de protection des renseignements personnels recueillis par vidéosurveillance.

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 2 sur 8
---	----------------------	--------------

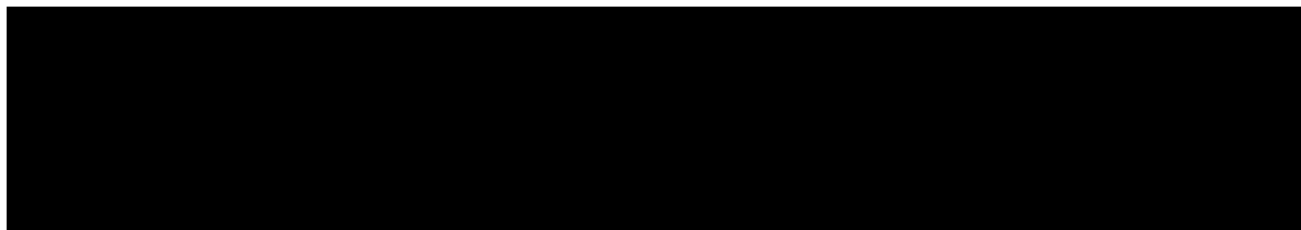
DIRECTIVE ADMINISTRATIVE

	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

4.4 Les différents postes de gestion des accès et de vidéosurveillance doivent être situés dans une zone sécurisée. En conséquence, afin d'assurer la protection des équipements de surveillance et des renseignements personnels s'y retrouvant, seules les personnes autorisées par la DSPJ peuvent y accéder. Lorsque non utilisés, ces postes doivent être verrouillés au moyen d'un mot de passe.

4.5 Seules les personnes autorisées par la DSPJ peuvent, dans le cadre de leurs fonctions, utiliser les systèmes de contrôle des accès et de vidéosurveillance et ce, qu'à des fins de sécurité exclusivement.

Note : Les différents clients ou propriétaires d'édifices ne doivent, en aucun temps, pouvoir accéder aux données ou images de ces systèmes.



4.7 Il est interdit de confirmer l'emplacement ou le champ de vision des caméras, leurs délais de rétention ou toute autre information relative aux systèmes de contrôle des accès et de vidéosurveillance ainsi que les composantes physiques en place et ce, en vertu de l'article 28 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

4.8 Les systèmes de contrôle d'accès et de vidéosurveillance doivent être utilisés avec éthique et professionnalisme :

4.8.1 On ne doit pas recourir à ces systèmes de manière à brimer la vie privée des occupants de l'édifice ou de toute autre personne se trouvant dans les environs des bâtiments sous protection de la DSPJ;

4.8.2 Ces systèmes ne doivent jamais servir à des fins de surveillance de la prestation de travail du personnel de la DSPJ ou celle de la clientèle dont elle assure la protection;

4.8.3 Aucun gros plan sur une personne ou groupe de personnes ne peut être fait sans un motif raisonnable de sécurité;

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 3 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

4.8.4 Il est interdit de se servir des caméras pour regarder des personnes ou des lieux à l'extérieur des édifices et terrains sous protection de la DSPJ sans un motif évident de sécurité.

4.9 Les angles de vision des caméras qui permettent de voir à l'intérieur d'autres édifices doivent être brouillés à l'aide d'une zone privée (zone de masquage).

4.10 Toute demande pour l'obtention de renseignements ou d'enregistrements vidéo contenus dans les systèmes de contrôle d'accès ou de vidéosurveillance doit, soit :

4.10.1 Être requise dans le cadre d'une enquête de la DSPJ, ou

4.10.2 Être requise en vertu d'une demande officielle d'un corps policier ou d'un autre organisme chargé d'application de la loi, ou

4.10.3 Effectuée en vertu d'une demande d'accès à l'information et autorisée par le responsable de l'accès à l'information du ministère de la Sécurité publique.

4.11 Lorsqu'un incident de confidentialité impliquant un renseignement personnel se produit, la DSPJ doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se reproduisent. Si l'incident présente un risque de préjudice sérieux, la DSPJ doit, conformément au Règlement sur les incidents de confidentialité :

- aviser la Commission d'accès à l'information;
- aviser toute personne dont un renseignement personnel est concerné par l'incident;
- l'inscrire au registre des incidents de confidentialité impliquant un renseignement personnel.

Note : Les éléments à considérer pour déterminer si un incident présente un risque de préjudice sérieux sont la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Le responsable de la protection des renseignements personnels doit également être consulté.

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 4 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

 Sécurité publique Québec	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

5. MODALITÉS DE VISIONNEMENT ET D'EXTRACTION

5.1 Le système d'enregistrement vidéo numérique permet la visualisation et l'enregistrement d'images captées par les caméras de surveillance. Les séquences vidéo sont conservées sur les disques durs pour une période de 30 jours. À noter que la période de conservation peut être moindre car les appareils d'enregistrement ne disposent pas tous de la même technologie.

5.2 L'officier de la DSPJ, responsable du secteur concerné, doit autoriser toutes extractions de données, images ou vidéos des systèmes de contrôle d'accès et de vidéosurveillance. Toutefois, dans le cadre d'une enquête, un constable-enquêteur peut procéder sans en aviser l'officier responsable. La personne qui extrait des séquences vidéo doit, en tout temps, consigner les détails de la demande dans le Registre de transmission d'enregistrement vidéo.

Note : L'extraction vidéo doit toujours être réalisée en présence d'un témoin.

5.3 À la suite de l'approbation du gestionnaire, l'extrait vidéo sera :

- Remis au demandeur, dans le cas d'une demande effectuée par un corps de police ou un autre organisme chargé d'application de la loi;
- Remis au responsable de l'accès à l'information du ministère de la Sécurité publique, dans le cas d'une demande d'accès à l'information.

5.4 Les demandes d'extraction d'enregistrements vidéo sont archivées dans un dossier numérique sécurisé ou un classeur sécurisé pour une période de 5 ans (formulaires et enregistrements).

6. RÔLE DES INTERVENANTS

6.1 Personnel utilisateur

6.1.1 Utiliser de manière professionnelle et éthique le système de vidéosurveillance afin d'observer les édifices et les terrains sous protection de la DSPJ.

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 5 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

6.1.2 Signaler toute utilisation inadéquate à son supérieur immédiat.

6.1.3 Transmettre les demandes d'extraction reçues à l'officier de la DSPJ responsable du secteur concerné via les voies hiérarchiques. Toute demande d'extraction doit demeurer confidentielle.

6.1.4 Signaler tout problème technique à la personne responsable de l'organisme ou du ministère propriétaire des équipements.

6.1.5 Consigner les bris ou problèmes techniques des équipements dans le rapport journalier des événements.

6.2 Officier responsable

6.2.1 S'assurer, auprès du propriétaire des équipements de sécurité et logiciels, que le système de vidéosurveillance est toujours en bon état de fonctionnement et qu'il dispose d'une capacité suffisante d'enregistrement des images.

6.2.2 Veiller à ce que les zones privées soient bien définies sur le système de vidéosurveillance.

6.2.3 Assurer le suivi des problèmes techniques, en lien avec le système de vidéosurveillance, avec le propriétaire des équipements de sécurité et logiciels. Au besoin, lorsqu'un service d'entretien approuvé est requis, passer préalablement un appel de service auprès du mandataire.

6.2.4 Transmettre à l'inspecteur-chef tout signalement concernant une utilisation inadéquate du système.

6.2.5 Traiter les demandes d'extraction reçues via le formulaire « Registre de transmission d'enregistrement vidéo ».

6.2.6 S'assurer que les enregistrements vidéo prélevés ne se rapportent qu'à l'incident ayant mené à la demande d'extraction.

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 6 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

 Sécurité publique Québec	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

6.2.7 Si une situation exige une extraction vidéo en urgence, il prend la responsabilité d'obtempérer à la demande sur-le-champ et fait en sorte que le directeur en soit informé subséquemment.

6.2.8 S'assurer que chaque document relatif à une demande d'extraction (formulaires et enregistrements) soit archivé de façon sécuritaire.

6.2.9 Veiller au respect de la présente directive.

6.3 Inspecteur-Chef

6.3.1 Recevoir toutes demandes d'accès à l'information provenant du Directeur de la DSPJ et désigner un officier responsable pour le traitement des demandes d'extraction.

6.3.2 Transmettre au Directeur de la DSPJ tout signalement concernant une utilisation inadéquate du système.

6.4 Directeur de la DSPJ

6.4.1 Veiller à ce que les personnes pouvant accéder au système d'accès et de vidéosurveillance aient pris connaissance de la présente directive et soient au fait des règles encadrant la protection de la vie privée et des renseignements personnels recueillis par vidéosurveillance.

6.4.2 À titre de responsable de la gestion des accès et de la vidéosurveillance ainsi que des demandes d'accès à l'information, il doit désigner la ou les personnes responsables du système d'accès et de vidéosurveillance.

6.4.3 S'assurer que toute personne chargée d'exploiter et d'assurer le bon fonctionnement des systèmes d'accès et de vidéosurveillance ait signé un engagement de confidentialité.

6.4.4 Analyser les demandes d'extractions vidéo ou les demandes émanant du système de contrôle d'accès et transmettre la réponse au demandeur.

6.4.5 Être responsable de l'acheminement ou de la rétention des extraits vidéo qui lui sont remis.

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 7 sur 8
---	----------------------	--------------

DIRECTIVE ADMINISTRATIVE

	Utilisation des systèmes de contrôle des accès et de vidéosurveillance	DIR-5.4.4
	Sécurité de l'État DSPJ	Dernière mise à jour 2024/10/11

6.4.6 Lorsqu'il est informé d'une utilisation inadéquate du système de vidéosurveillance, demander la tenue d'une enquête administrative.

6.4.7 S'assurer que des mesures raisonnables pour éviter les incidents de confidentialité impliquant un renseignement personnel soient en vigueur et respectées. De plus, dans l'éventualité que de tels incidents se produisent, prévoir la création d'un registre permettant d'y consigner ceux-ci.

FORMULAIRE

DSPJ2011-1136 Registre de transmission d'enregistrement vidéo

Signature du gestionnaire : Original signé par M. Martin Maranda	Date : 2024-10-15	Page 8 sur 8
---	----------------------	--------------