COMPLEXE MULTI-DISCIPLINAIRE LES ESTACADES

Annexe 2	TITRE
Date d'entrée en vigueur: 9 juin 2020	**PROCÉDURES D'ACCÈS DES ACTIFS INFORMATIONNELS**

1. OBJECTIFS GÉNÉRAUX

Les présentes procédures visent à encadrer l'accès, l'utilisation, la surveillance et la protection des actifs informationnels du **Complexe Multi-Disciplinaire les Estacades (CMDE)**, afin de :

- Prévenir les accès non autorisés, les pertes, les vols ou les atteintes à l'intégrité des actifs informationnels;
- Assurer la protection des renseignements personnels conformément à la **Loi sur la protection des renseignements personnels dans le secteur privé (Loi 25)**;
- Définir clairement les responsabilités des utilisateurs et des gestionnaires.

Les actifs informationnels incluent notamment : les systèmes informatiques, les comptes utilisateurs, les bases de données, les courriels, les images de vidéosurveillance et tout renseignement personnel ou confidentiel.

2. SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

2.1 Objectif

Empêcher tout accès physique non autorisé, tout dommage, toute intrusion ou tout incident pouvant compromettre la sécurité des personnes, des locaux et des actifs informationnels du CMDE.

2.2 Mesures

- Le contrôle des accès aux portes d'entrée principales est assuré par des moyens technologiques appropriés, incluant des **caméras de surveillance**;
- La surveillance est effectuée dans un objectif de sécurité et de prévention, sous la responsabilité du personnel d'accueil et du gestionnaire des technologies de l'information;
- Les équipements sensibles (serveurs, postes administratifs, archives) sont situés dans des zones à accès restreint.

3. CONTRÔLE D'ACCÈS AUX ACTIFS INFORMATIONNELS

3.1 Accès aux équipements et systèmes

- L'accès aux ordinateurs administratifs est contrôlé par des **mécanismes physiques sécurisés** (clés ou dispositifs équivalents) à diffusion restreinte;
- L'accès aux systèmes d'information est protégé par un **identifiant unique** et un **mot de passe confidentiel**;
- Les accès sont accordés selon le principe du **besoin de savoir** et retirés dès qu'ils ne sont plus requis.

3.2 Responsabilités des utilisateurs

Tout utilisateur doit :

- Garder confidentiels son identifiant et son mot de passe;
- Ne jamais partager ses accès avec une autre personne;
- Ne pas consigner ses mots de passe sur un support accessible à autrui;
- Aviser sans délai le gestionnaire des technologies de l'information ou le responsable de la protection des renseignements personnels en cas de soupçon de compromission.

3.3 Responsabilités du gestionnaire des technologies de l'information

Le gestionnaire des technologies de l'information est responsable de :

- La gestion des identifiants et des accès aux serveurs, incluant **Active Directory** et le serveur de courrier électronique;
- La mise en place et l'application des politiques de mots de passe;
- La révocation rapide des accès lors du départ ou du changement de fonctions d'un utilisateur.

4. ACCÈS AUX IMAGES CAPTÉES PAR LE SYSTÈME DE VIDÉOSURVEILLANCE

4.1 Objectif

Encadrer l'accès, le visionnement, l'archivage et la diffusion des images captées par les systèmes de caméras du CMDE, dans le respect de la vie privée et des obligations prévues à la Loi 25.

4.2 Principes

- Les caméras de surveillance sont utilisées exclusivement à des fins de sécurité, de prévention, de gestion des incidents et de protection des personnes et des biens;
- L'accès aux images est strictement limité aux personnes autorisées;
- Toute consultation ou diffusion d'images doit être justifiée, proportionnelle et documentée au besoin.

4.3 Responsabilités et autorisations

Directeur général

- Autorise toute transmission d'images ou de vidéos à l'externe (autorités, assureurs, conseillers juridiques, etc.).

Directions-/Directions adjointes de services

- Peuvent visionner des images en différé liées à des événements relevant de leurs secteurs;
- Autorisent la transmission d'images à la direction de l'école lors d'événements impliquant des élèves ou des membres du personnel scolaire;
- Peuvent autoriser les gestionnaires intermédiaires à visionner des images en différé pour leur secteur.

Coordonnateur – Dekhockey

- Peuvent visionner des images en différé afin de valider des décisions de jeu pouvant mener à des sanctions;
- Assurent l'archivage des captures liées à des événements pouvant avoir des impacts sur des individus ou sur le CMDE.

Réceptionnistes, préposés aux installations et préposés à l'opération de la surfaceuse

- Peuvent visionner les images **en temps réel uniquement**, lorsque requis dans l'exercice de leurs fonctions.

Gestionnaire des technologies de l'information

- Assure la gestion technique du système de vidéosurveillance;
- Contrôle et autorise l'accès aux images archivées;
- Effectue ou supervise l'archivage des images pertinentes;
- Transmet des images ou extraits vidéo aux autorités compétentes **sur autorisation du directeur général**.

5. CONSERVATION, ARCHIVAGE ET DESTRUCTION DES IMAGES

- Les images sont conservées pour une durée limitée, proportionnelle aux finalités pour lesquelles elles ont été collectées;
- Les images non pertinentes sont détruites de façon sécuritaire;
- Les images liées à un incident, une enquête ou un litige sont conservées selon les délais légaux applicables.

6. MANQUEMENTS ET INCIDENTS DE CONFIDENTIALITÉ

Tout accès non autorisé, usage abusif ou incident impliquant des actifs informationnels ou des renseignements personnels doit être signalé sans délai. Des mesures correctives et disciplinaires peuvent être appliquées selon la gravité de la situation.

7. ENTRÉE EN VIGUEUR

Les présentes procédures entrent en vigueur à la date de leur adoption et demeurent applicables jusqu'à leur modification ou leur remplacement.

Le genre masculin est utilisé sans discrimination et uniquement dans le but d'alléger le texte.