Centre
de services scolaire
des Sommets
Québec

DIRECTIVE

DIRECTIVE SUR LES RÔLES ET RESPONSABILITÉS EN CAS D'INCIDENTS DE CONFIDENTIALITÉ

N° de directive :	**Adoptée le :**	**Entrée en vigueur le :**
DIR-SG-01	2023-12-12	2023-12-12
Responsable : Secrétariat général		

1. CADRE JURIDIQUE

La présente directive découle des articles 63.8 à 63.11 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, ci-après « LAI »).

La présente directive doit être lue en concordance avec les différents encadrements du Centre de services scolaire des Sommets (ci-après « CSSDS ») concernant la protection des renseignements personnels.

2. BUT ET OBJECTIFS DE LA DIRECTIVE

Le but de la directive est d'assurer la mise en œuvre des obligations du CSSDS découlant de la LAI en lien avec les incidents de confidentialité.

Les objectifs de la directive sont les suivants :

- Énoncer les principes sur lesquels repose la protection des renseignements personnels recueillis, utilisés, communiqués et conservés dans le cadre de l'exercice des fonctions du CSSDS;
- Établir un processus de déclaration des incidents de confidentialité pouvant survenir dans le cadre des fonctions du CSSDS;
- Informer les membres du personnel et autres personnes du CSSDS sur la gestion des incidents de confidentialité;
- Déterminer les rôles et responsabilités des personnes visées par la présente directive.

3. CHAMP D'APPLICATION

La présente directive s'applique à l'ensemble du personnel du CSSDS (écoles, centres, services).

Elle s'applique également aux membres du conseil d'administration, aux membres des conseils d'établissements et aux membres des différents comités du CSSDS.

La présente directive n'a pas pour effet de limiter les responsabilités du CSSDS découlant de la *Politique sur la sécurité de l'information du Centre de services scolaire des Sommets* adoptée en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03), ainsi que des encadrements qui en découlent.

4. DÉFINITIONS

Les termes utilisés dans la présente directive sont ceux de la LAI et des autres encadrements légaux applicables, sauf indication contraire. Pour faciliter la compréhension de la présente directive, on entend par :

Comité sur l'accès	Le comité sur l'accès à l'information et la protection des renseignements personnels du CSSDS
CAI	Commission d'accès à l'information
Déclarant	Personne qui a connaissance d'un possible incident de confidentialité
Direction	Direction de l'unité administrative concernée (l'établissement, le centre ou le service) à qui le Déclarant signale l'incident de confidentialité
Incident de confidentialité	• L'accès non autorisé par la loi à un renseignement personnel • L'utilisation non autorisée par la loi d'un renseignement personnel • La communication non autorisée par la loi d'un renseignement personnel • La perte d'un renseignement personnel • Toute autre atteinte à la protection d'un tel renseignement
Personne	Une personne visée par le champ d'application de la présente directive agissant au nom du CSSDS ou dans le cadre de ses fonctions
Responsable présumé	Personne à l'origine d'un incident de confidentialité allégué
Renseignement personnel	Renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier
RPRP	Personne désignée comme responsable de la protection des renseignements personnels du CSSDS

5. PRINCIPES GÉNÉRAUX

5.1 Une Personne doit recueillir uniquement les renseignements personnels nécessaires aux fonctions du CSSDS.

5.2 Une Personne a accès uniquement aux renseignements personnels qui sont nécessaires à l'exercice de ses fonctions.

5.3 Une Personne ne peut communiquer des renseignements personnels sans le consentement de la personne concernée, de son représentant, ou dans les cas prévus par la loi.

5.4 Une Personne qui a connaissance d'un incident de confidentialité doit le déclarer dans les plus brefs délais en conformité de la présente directive.

6. PROCESSUS LORS D'UN INCIDENT DE CONFIDENTIALITÉ

6.1. Déclaration d'un incident de confidentialité

6.1.1. Le Déclarant doit, sans délai, informer la Direction de tout événement pouvant laisser croire qu'il s'est produit un incident de confidentialité.

6.1.2. Sans délai, la Direction doit informer le RPRP et le directeur du Service de l'informatique de l'événement qui lui a été dénoncé.

6.1.3. Dès que possible, la Direction collecte les informations suivantes relativement à l'incident de confidentialité, remplit le *Formulaire de déclaration d'un incident de confidentialité* et le transmet au RPRP et au directeur du Service de l'informatique :

- Le contexte et les circonstances entourant l'événement (date, description des faits survenus, etc.);
- La nature des renseignements personnels concernés (par exemple : noms, adresse, courriel, code permanent, etc.);
- Le fait que ces renseignements étaient ou non protégés par un mot de passe ou un code d'accès, par exemple;
- Le nombre de personnes concernées par les renseignements personnels;
- L'identité et le nombre de personnes ou l'organisme qui ont reçu les renseignements personnels, le cas échéant;
- Les mesures immédiates prises, le cas échéant;
- Toute autre information pertinente.

La direction peut évidemment communiquer, lorsque possible, avec le Responsable présumé pour obtenir ces informations.

6.1.4. Dès que possible, la Direction doit, avec le soutien du RPRP et de la direction du Service informatique, agir avec prudence et diligence afin de mettre en place les mesures immédiates nécessaires à la diminution du risque qu'un préjudice soit causé (rappel d'un courriel, téléphone, etc.)

6.2. Procédure de traitement d'incident de confidentialité

6.2.1. Analyse de la situation

Le RPRP et, le cas échéant, le directeur du Service de l'informatique, analysent la situation déclarée et, au besoin, obtiennent des informations supplémentaires.

S'il y a lieu, le directeur du Service de l'informatique statue sur la situation et détermine si la situation doit être déclarée au Centre opérationnel en Cyberdéfense (COCD).

Le RPRP statue sur la situation et détermine s'il s'agit d'un incident de confidentialité.

S'il détermine qu'il ne s'agit pas d'un incident de confidentialité, mais qu'il juge qu'une intervention est tout de même nécessaire auprès des personnes impliquées dans l'événement, il communique avec la Direction afin qu'elle prenne, le cas échéant, les mesures appropriées.

6.2.2. Traitement d'un incident de confidentialité

Le RPRP et, le cas échéant, le directeur du Service de l'informatique s'assurent que les gestes ou les mesures, qui sont susceptibles de diminuer les risques qu'un préjudicie soit causé aux personnes dont les renseignements personnels sont concernés par l'incident de confidentialité, soient mis en œuvre en tenant compte de ceux qui ont été posés par la Direction.

À titre d'exemple, les mesures suivantes pourraient être recommandées par le RPRP et le directeur du Service de l'informatique :

- Obtenir des personnes, à qui ont été communiqués par erreur des renseignements personnels, une confirmation de destruction des renseignements personnels obtenus;
- Obtenir des personnes, à qui ont été communiqués par erreur des renseignements personnels, un engagement de non-divulgation des renseignements personnels obtenus;
- Selon la nature de l'incident de confidentialité, informer le Service des ressources humaines pour qu'il puisse évaluer la nécessité de tenir une enquête disciplinaire ou administrative.

Le RPRP évalue le risque de préjudice sérieux de l'incident de confidentialité en considérant notamment la sensibilité du renseignement, les conséquences appréhendées

de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. Pour ce faire, il utilise la *Grille d'évaluation d'un préjudice lors d'un incident de confidentialité*.

Si l'incident de confidentialité présente un risque de préjudice sérieux, le RPRP doit :

- Aviser la Commission d'accès à l'information avec diligence, de la manière et en fournissant les informations requises par le *Règlement sur les incidents de confidentialité* (RLRQ, c. A-21, r. 3.1), à l'aide du *Formulaire de déclaration d'un incident de confidentialité* de la CAI ;
- Aviser toute personne dont les renseignements personnels sont concernés par l'incident de confidentialité de la manière et en fournissant les informations requises par le *Règlement sur les incidents de confidentialité* ;
- Aucun avis aux personnes visées n'est nécessaire si un tel avis avait pour effet d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois;
- Aviser toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux (ministère, police, etc.) en ne communiquant que les renseignements personnels nécessaires à cette fin et inscrire cette communication au registre des communications en vertu de la LAI.

Dans tous les cas, le RPRP inscrit l'incident au registre des incidents de confidentialité, établi conformément au *Règlement sur les incidents de confidentialité*.

6.2.3 Mesures à prendre pour éviter qu'un incident de confidentialité de même nature se reproduise

Une fois les mesures immédiates accomplies, le RPRP, le directeur du Service de l'informatique et toute direction concernée déterminent si d'autres mesures devraient être appliquées pour éviter que d'autres incidents de même nature ne se reproduisent. Ces recommandations sont ensuite transmises à la direction générale pour évaluation.

À titre d'exemples, les mesures suivantes peuvent être recommandées :

- La modification des accès informatiques ;
- La suppression de renseignements personnels ;
- La mise en place de formation ou autres mesures de sensibilisation ;
- La révision de processus internes (logiciels, méthodes de travail, etc.)

Dans tous les cas, le RPRP transmet à la direction générale les recommandations reçues de la Commission d'accès à l'information à la suite de la déclaration d'un incident de confidentialité.

7. COMITÉ SUR L'ACCÈS

7.1.1. Le RPRP peut en tout temps consulter le Comité sur l'accès dans l'analyse et le traitement d'une situation pouvant être un incident de confidentialité.

7.1.2. Le RPRP fait rapport annuellement au Comité sur l'accès des incidents de confidentialité survenus et des mesures mises en place.

8. INFORMATION ET DIFFUSION

8.1.1. Le RPRP s'assure de la diffusion de la présente directive auprès des différentes unités administratives.

8.1.2. Au besoin, en collaboration avec les directions d'unités administratives, le RPRP s'assure qu'une formation adéquate soit disponible et offerte aux membres du personnel.

9. ENTRÉE EN VIGUEUR

9.1.1. La présente directive a été approuvée par le Comité sur l'accès le 24 novembre 2023.

9.1.2. La présente directive a été adoptée par la directrice générale le 12 décembre 2023 et entre en vigueur à la même date.