Conseil scolaire du NORD-OUEST
4 Rue Bouchard, CP 1220 | St-Isidore (AB) | T0H 3B0
780.624.8855
www.csno.ab.ca

Système d'information des élèves (SIS : Student information System)

PRÉAMBULE

La Conseil a signé une entente avec Alberta Education qui exige que le Conseil réponde à des exigences spécifiques en matière de la sécurité des renseignements sur les élèves. Le texte intégral de l'accord peut être obtenu auprès de la direction générale du Conseil.
Le but de cette annexe est de se mettre en conformité avec l'accord en documentant les étapes mises en place pour gérer de manière acceptable le risque de perte de données sur les étudiants dans le système d'information sur les étudiants (SIS).
Cette annexe est conforme à des sections ou clauses spécifiques de l'accord.

PASI Security Controls pour les autorités scolaires

Le conseil scolaire doit mettre en œuvre les contrôles de sécurité suivants d'ici le 1er janvier 2020 ou la date à laquelle l'autorité scolaire se connecte pour la première fois au PASI via son SIS, selon la première éventualité.
1. « Un document de politique de sécurité de l'information doit être approuvé par la direction générale, publié et communiqué à tous les employés et aux parties externes concernées. »
1.1. Ce document servira de réponse au contrôle de sécurité A.5.1.1.
1.2. Ce document sera revu et édité annuellement par la direction générale et la secrétaire du Conseil.
1.3. Ce document et les exigences de sécurité qu'il contient seront communiqués à toutes les parties prenantes.
2. « Les exigences relatives aux accords de confidentialité ou de non-divulgation reflétant les besoins du Conseil scolaire en matière de protection de l'information doivent être identifiées et régulièrement examinées. »
2.1. Le Conseil a un accord général de confidentialité qui doit être accepté par tout le personnel du Conseil. Annexe A
2.2. L'accord d'utilisation du réseau du personnel a été modifié en mettant l'accent sur la confidentialité des informations des étudiants.

DIRECTIVES GÉNÉRALES

1. Tous les renseignements personnels recueillis par le Conseil seront conservés et protégés contre tout accès non autorisé.
2. Les dispositifs de stockage portables ne doivent pas être utilisés pour stocker des renseignements personnels à moins d'y être autorisés par la direction générale. Les informations doivent être cryptées et protégées par mot de passe. Les informations personnelles sur les appareils portables doivent être temporaires et supprimées à la fin de la tâche.
3. L'administrateur du système d'information doit s'assurer que la sauvegarde et la récupération des données/informations sont en place et examinées périodiquement, concernant les informations stockées dans le réseau du Conseil.
4. Le personnel du Conseil doit signaler toute atteinte à la sécurité des informations, à la confidentialité ou à l'abus des services cloud, qu'ils soient réels ou suspectés, à leur superviseur immédiat pour enquête. Les superviseurs doivent contacter l'administrateur du système d'information pour obtenir de l'aide.
5. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par l'enseignant, l'évaluation des risques liés à l'application et au stockage dans le cloud (formulaire A) sera complétée par l'enseignant et soumise à la direction.
6. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par l'école, l'évaluation des risques liés à l'application et au stockage dans le cloud (formulaire A) sera remplie par le directeur et soumise à l'administrateur des systèmes d'information.
7. Pour les applications ou le stockage basés sur le cloud pour lesquels un accord est conclu par la division, l'évaluation des risques liés aux applications et au stockage en nuage (formulaire A) sera complétée par l'administrateur du système d'information.
8. Lorsqu'une violation ou un acte d'abus se produit, aucune mesure ne devrait être prise par l'enseignant ou l'école qui pourrait entraver une enquête jusqu'à ce que la direction générale l'ordonne.
    a. Aucune donnée ou information de compte ne doit être supprimée tant que la direction générale en fait la demande ou l'approuve.
    b. Les parents, les élèves ou les autres membres du personnel ne doivent pas être informés de la violation ou de l'abus avant d'y être dirigé par la direction générale.

9. L'utilisation d'applications ou de stockage basés sur le cloud par le personnel doit respecter les principes de « citoyenneté numérique ». De plus, le personnel est tenu de respecter ce qui suit lorsqu'il est en ligne :
    a. Pour les professionnels, le code de conduite propre à leur profession;
    b. Pour le personnel de soutien, les mêmes principes de conduite qui seraient attendus hors ligne;
    c. Pour tout le personnel, assurez-vous de ne pas publier ou partager d'informations liées au travail qui seraient considérées comme confidentielles; et
    d. Pour tout le personnel, comprenez que vos actions à la fois en ligne et hors ligne en dehors du travail peuvent affecter votre relation de travail avec le Conseil scolaire.
10. Les atteintes à la vie privée doivent être signalées au coordonnateur FOIP.

Référence: Article 11, 31, 33, 52, 53, 196, 197, 222 Education Act
Freedom of Information and Protection of Privacy Act Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education
ATA Code of Professional Conduct