PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Procédure

A fait l'objet d'une consultation auprès du comité permanent sur l'accès à l'information et sur la protection des renseignements personnels de l'Université TÉLUQ le 21 juin 2023

Adopté par la responsable de l'accès à l'information et la protection des renseignements personnels de l'Université TÉLUQ le 15 septembre 2023

Entrée en vigueur le 22 septembre 2023

Table des matières

1 INTRODUCTION....2

1.1 PRÉAMBULE....2

1.2 OBJET....2

1.3 CADRE NORMATIF....2

1.4 CHAMP D'APPLICATION....3

1.5 DÉFINITIONS....3

1.6 RESPONSABILITÉ DE L'APPLICATION....5

2 PROCESSUS DE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ....5

2.1 LE SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ....6

2.2 INTERVENTION IMMÉDIATE....6

2.3 ANALYSE DE LA RECEVABILITÉ (EST-CE UN INCIDENT DE CONFIDENTIALITÉ?) 6

2.4 LA FICHE D'INCIDENT DE CONFIDENTIALITÉ....7

2.5 ÉQUIPE RESPONSABLE DU TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ....7

2.6 ÉVALUATION DU RISQUE POUR LA PERSONNE CONCERNÉE....9

2.7 NOTIFICATION DE L'INCIDENT....9

2.8 CARTOGRAPHIE....11

3 REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ....11

4 RESPONSABILITÉS....11

ANNEXES....12

1 Introduction

1.1 Préambule

Comme le prévoit ses *Règles de gouvernance en matière de protection des renseignements personnels*, l'Université TÉLUQ (« l'Université ») reconnaît l'importance de protéger les renseignements personnels qu'elle détient. C'est pourquoi elle met en œuvre les moyens administratifs et technologiques nécessaires afin que ceux-ci soient correctement traités tout au long de leur cycle de vie.

Afin de s'acquitter de ses obligations en la matière, l'Université met en place des mesures de sécurité raisonnables pour protéger les renseignements personnels qu'elle traite, peu importe leur support. Malgré les précautions prises, un incident de confidentialité est toujours possible. C'est pourquoi l'Université se dote de la présente procédure pour gérer les éventuels incidents de confidentialité et limiter ainsi leurs éventuelles conséquences néfastes pour les personnes concernées et pour l'Université.

1.2 Objet

La présente procédure a pour objet de :

- Définir les rôles et responsabilités des parties prenantes;
- Décrire la démarche à suivre en cas d'incident de confidentialité;
- Rappeler l'obligation de notification et ses modalités.

1.3 Cadre normatif

La présente procédure s'inscrit dans un contexte régi notamment par :

- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c. A-2.1), plus spécifiquement ses articles 63.8 à 63.11;
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, SQ 2021, c. 25 (la « Loi 25 », sanctionnée le 22 septembre 2021);
- Le *Code civil du Québec* (LQ, c. CCQ-1991);
- La *Charte des droits et libertés de la personne* (RLRQ, c. C-12);
- Lorsqu'applicable, le *Règlement général sur la protection des données* (RGPD) de l'Union européenne (UE), Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données;
- La politique *Sécurité de l'information*;
- Les *Règles de gouvernance en matière de protection des renseignements personnels;*
- La *Politique de confidentialité;*
- La directive *Utilisation des renseignements personnels, gestion des communications électroniques et confidentialité.*

1.4 Champ d'application

La présente procédure s'applique :

- À tous les membres de la communauté universitaire ayant connaissance d'un incident de confidentialité impliquant des renseignements personnels traités au sein de l'Université;
- Aux tiers traitant des renseignements personnels pour le compte de l'Université et ayant connaissance d'un tel incident en lien avec ces renseignements.

1.5 Définitions

Aux fins de la présente procédure, on entend par :

Comité : Le comité permanent sur l'accès à l'information et la protection des renseignements personnels de l'Université TÉLUQ.

Conseil : Le conseil d'administration de l'Université TÉLUQ.

Cycle de vie : L'ensemble des étapes que franchit un renseignement personnel et qui vont de sa collecte, en passant par son utilisation, sa communication, sa conservation et sa destruction ou anonymisation.

Dirigeant : Toute personne embauchée à titre de cadre supérieur selon les termes du Protocole des cadres supérieurs (annexe 6-A) de l'Université du Québec.

À titre indicatif, au 1er juin 2023, ces personnes sont : la directrice générale; le directeur de l'enseignement et de la recherche; la directrice des services administratifs et la directrice des affaires externes et secrétaire générale.

Gestionnaire : Toute personne embauchée à titre de cadre supérieur ou cadre, et toute directrice, directeur de département, d'unité ou de chaire de recherche.

Incident de confidentialité (ou incident) : Ttoute utilisation ou communication, ou tout accès non autorisé par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection ou à son caractère confidentiel.

Membre de la communauté universitaire : Membres du personnel, incluant le personnel cadre supérieur, le personnel cadre et le corps professoral, les personnes tutrices, les personnes chargées d'encadrement, la communauté étudiante (active ou non), les personnes stagiaires, les équipes, unités, centres et chaires de recherche. Sont également considérés comme des membres de la communauté universitaire : les membres de la commission des études et du conseil d'administration, les membres de tous les comités créés par l'une ou l'autre des instances administratives de l'Université, et les diplômés et diplômées de l'Université.

Membres du personnel : Toutes les personnes employées et membres du personnel, sous-traitants ou employés, employées temporaires et les tiers travaillant pour ou agissant pour le compte de l'Université, incluant à titre de bénévole ou de stagiaire. Les administratrices et administrateurs de l'Université sont considérés comme des membres du personnel aux fins de la présente procédure.

Mesures correctrices : Mesures de mitigation des risques mises en place pour faire cesser un incident de confidentialité et en réduire les conséquences.

Mesures préventives : Mesures de mitigation des risques mises en place pour éviter qu'un incident de confidentialité ne se reproduise.

Personne concernée : Personne physique concernée par un ou plusieurs renseignements personnels.

Renseignements personnels (ou RP) : Toute information relative à une personne physique et qui permet de l'identifier :

- directement, c'est-à-dire par le recours à cette seule information;
- indirectement, c'est-à-dire par le recoupement avec d'autres informations ou par inférence.

Renseignement personnel non confidentiel : Renseignement personnel auquel la loi ne confère pas un caractère de confidentialité.

Responsable de la protection des renseignements personnels au sein de l'Université : La secrétaire générale, le secrétaire général ou toute autre personne désignée à ce titre auprès de la commission d'accès à l'information.

Responsable du traitement des incidents de confidentialité : Personne désignée par le ou la responsable de la protection des renseignements personnels au sein de l'Université pour recevoir et traiter un incident de confidentialité au premier niveau. On peut joindre le ou la responsable à incidentdeconfidentialite@teluq.ca.

La ou le responsable de la protection des renseignements personnels au sein de l'Université peut également désigner plusieurs personnes à ce titre, lesquelles sont conjointement désignées comme l'**équipe d'intervention en protection des renseignements personnels (PRP)**. L'équipe d'intervention PRP exerce alors les fonctions du ou de la responsable du traitement des incidents de confidentialité.

L'**équipe d'intervention PRP** se désigne une personne répondante et la majorité de ses membres peut agir seule.

Tiers/sous-traitant : Toute personne ou entité extérieure à la communauté universitaire et traitant des renseignements personnels pour le compte de l'Université.

Université : Université TÉLUQ, incluant tous ses services, départements, unités ou chaires de recherche.

1.6 Responsabilité de l'application et de la divulgation

Chaque membre du personnel a une responsabilité dans la collecte, l'utilisation, la communication, la protection, la conservation ou la destruction des renseignements personnels auxquels il a accès.

Chaque gestionnaire a une responsabilité dans la collecte, l'utilisation, la communication, la protection, la conservation ou la destruction des renseignements personnels auxquels ses employés ont accès.

Chaque membre du personnel a une responsabilité de divulguer un incident de confidentialité dont il est témoin.

Tous les membres du personnel doivent connaître et suivre la présente procédure. Ils doivent, en présence d'un incident de confidentialité, le signaler au ou à la responsable du traitement des incidents de confidentialité conformément au processus décrit à l'article 2.

Les tiers et les sous-traitants doivent, en présence d'un incident de confidentialité alors qu'ils agissent pour le compte de l'Université, le signaler au ou à la responsable du traitement des incidents de confidentialité conformément au processus décrit à l'article 2.

Tous les autres membres de la communauté universitaire sont invités, en présence d'un incident de confidentialité, à le signaler au ou à la responsable du traitement des incidents de confidentialité conformément au processus décrit à l'article 2.

2 Processus de traitement d'un incident de confidentialité

2.1 Le signalement d'un incident de confidentialité

Être en présence d'un incident de confidentialité signifie :

- Avoir une connaissance directe de l'incident;
- Avoir un motif de croire en la survenance d'un incident;
- Ou même soupçonner la survenance d'un incident.

Et ce, à la lumière d'informations dont on a connaissance.

Un membre du personnel, un tiers ou un sous-traitant agissant pour le compte de l'Université doit, en présence d'un incident de confidentialité, le signaler sans délai au ou à la responsable du traitement des incidents de confidentialité en écrivant à incidentdeconfidentialite@teluq.ca.

Il doit aussi en informer son supérieur immédiat ou sa supérieure immédiate, sauf si cette personne est impliquée dans l'incident.

Tout autre membre de la communauté universitaire ou tiers est invité, en présence d'un tel incident, à le signaler sans délai à la même adresse.

En cas d'urgence et en dehors des heures de bureau, le membre du personnel peut contacter son supérieur immédiat ou sa supérieure immédiate, sauf si cette personne est impliquée dans l'incident, ou le secrétaire général ou la secrétaire générale pour rapporter l'incident.

2.2 Intervention immédiate

Lorsque cela est possible, l'auteur, auteure du signalement prend le plus rapidement possible les mesures adéquates afin de contenir l'incident et d'en limiter les torts ou dommages. Il prend également les mesures adéquates pour préserver la preuve de l'incident. Il prend les **mesures correctives (mesures de mitigation immédiates)** demandées par le ou la responsable du traitement des incidents de confidentialité, le cas échéant.

2.3 Analyse de la recevabilité (est-ce un incident de confidentialité?)

Le ou la responsable du traitement des incidents de confidentialité ou la personne répondante de l'équipe d'intervention PRP détermine s'il s'agit bien d'un incident de confidentialité.

Pour ce faire, il ou elle utilise la *Grille d'aide à la décision* jointe en annexe.

Si l'une des réponses aux questions est négative, il ne s'agit pas d'un incident de confidentialité et le signalement est clos. Les membres de l'équipe d'intervention PRP sont informés des résultats de l'analyse et peuvent en demander la révision par l'ensemble de l'équipe.

Même si la réponse s'avère négative, la collecte d'informations et l'analyse sont documentées.

Si les réponses aux questions sont affirmatives, le processus se poursuit et une *Fiche d'incident de confidentialité* est remplie par le répondant.

2.4 La Fiche d'incident de confidentialité

2.4.1 Remplir la Fiche d'incident de confidentialité

Le ou la responsable du traitement des incidents de confidentialité ou la personne répondante de l'équipe d'intervention PRP recueille, collige et résume les informations et documents en lien avec l'incident de confidentialité signalé.

Pour ce faire, elle ou il utilise la *Fiche d'incident de confidentialité* jointe en annexe.

La collecte d'informations et l'analyse sont documentées.

2.4.2 Partage de la Fiche d'incident de confidentialité

Dans les meilleurs délais et dans les deux (2) jours ouvrables, la personne répondante convoque l'équipe d'intervention PRP pour une rencontre et lui transmet la fiche et les documents afférents.

Si certaines informations demandées dans la fiche ne sont pas immédiatement disponibles, dès lors qu'elles ne sont pas indispensables pour traiter rapidement l'incident, celui-ci peut être traité. Les documents complémentaires seront récupérés ultérieurement.

2.5 Équipe responsable du traitement des incidents de confidentialité

2.5.1 Le ou la responsable du traitement des incidents de confidentialité ou l'équipe d'intervention PRP (3 membres) doit :

- Vérifier qu'il s'agit bien d'un incident de confidentialité imputable à l'Université;
- S'assurer que les **mesures correctives (mesures de mitigation immédiates)** sont prises; dans le cas contraire, il donne des instructions pour y remédier.

Une fois un incident de confidentialité constaté, le ou la responsable du traitement des incidents de confidentialité ou l'équipe d'intervention PRP doit :

- Établir les circonstances de l'incident ;
- Cibler les renseignements personnels et les personnes concernées ;
- Déterminer les **mesures correctives (mesures de mitigation)** afin de faire cesser l'incident, incluant le recours à toute personne susceptible de diminuer le préjudice, et s'assurer de leur application ;
- Déterminer les **mesures préventives (mesures de mitigation supplémentaires)** afin de faire en sorte que l'incident ne se reproduise pas, et s'assurer de leur application ;
- Inscrire l'incident aux registres concernés ;
- Réviser les processus en continu.

Le ou la responsable du traitement des incidents de confidentialité ou l'équipe d'intervention PRP évalue le degré du risque de préjudice sérieux par une évaluation des facteurs relatifs à la vie privée (EFVP) au moins sommaire.

Pour ce faire, elle ou il utilise l'*Évaluation des facteurs relatifs à la vie privée (EFVP) sommaire* jointe en annexe.

2.5.2 Équipe d'intervention PRP élargie (5 membres)

Selon le degré de gravité, le ou la responsable du traitement des incidents de confidentialité ou l'équipe d'intervention PRP avise le ou la responsable de la protection des renseignements personnels au sein de l'Université et le directeur du Service des technologies de l'information. Il ou elle collabore avec ces

nouveaux intervenants pour trouver les solutions à la gestion de l'incident de confidentialité et les appliquer.

L'équipe d'intervention PRP élargie détermine les :

- **Mesures correctives (mesures de mitigation immédiates)** afin de contenir l'incident et d'en limiter les torts ou les dommages, et s'assure de leur application ;
- **Mesures correctives (mesures de mitigation)** afin de faire cesser l'incident, incluant le recours à toute personne susceptible de diminuer le préjudice, et s'assure de leur application ;
- **Mesures préventives (mesures de mitigation supplémentaires)** afin de faire en sorte que l'incident ne se reproduise pas.

2.5.3 Équipe d'urgence PRP (7 membres)

Selon le degré de gravité, le ou la responsable de la protection des renseignements personnels au sein de l'Université avise les personnes dirigeantes de l'Université et la direction du Service des communications et des affaires publiques. Il ou elle collabore avec ces nouveaux intervenants pour trouver les solutions à la gestion de l'incident de confidentialité et les appliquer.

L'équipe d'urgence PRP est composée des intervenants suivants :

- les personnes dirigeantes de l'Université;
- le ou la responsable de la protection des renseignements personnels au sein de l'Université;
- la direction du Service des technologies de l'information;
- la direction du Service des communications et des affaires publiques;
- un membre de l'équipe d'intervention PRP désigné par le ou la responsable de la protection des renseignements personnels au sein de l'Université;
- Toute autre personne requise par l'équipe d'urgence.

L'équipe d'urgence PRP doit déterminer les :

- **Mesures correctives (mesures de mitigation immédiates)** afin de contenir l'incident et d'en limiter les torts ou dommages, et s'assure de leur application;
- **Mesures correctives (mesures de mitigation)** afin de faire cesser l'incident, incluant le recours à toute personne susceptible de diminuer le préjudice, et s'assure de leur application;
- **Mesures préventives (mesures de mitigation supplémentaires)** afin de faire en sorte que l'incident ne se reproduise pas.

Selon le degré de gravité, l'équipe d'urgence PRP doit :

- Faire intervenir les intervenants et les autorités externes pour trouver les solutions à la gestion de l'incident de confidentialité et les appliquer (policiers, assureurs, spécialistes, etc.);

- Coordonner les communications internes et externes, dont les avis publics, et notifier l'incident à la Commission d'accès à l'information (CAI), à la personne concernée et, au besoin, au ministère concerné, en utilisant l'avis public;
- Mettre en place les mesures visant à réduire les impacts d'un incident de confidentialité sur la réputation de l'Université.

Pour agir, l'équipe d'urgence PRP peut recommander l'octroi d'un contrat de gré à gré, en conformité avec l'article 13, par. 1 LCOP.

2.6 Évaluation du risque pour la personne concernée

Si elle considère qu'il s'agit bien d'un incident de confidentialité imputable à l'Université, le ou la responsable du traitement des incidents de confidentialité ou l'équipe d'intervention PRP évalue le risque pour la personne concernée par le fait de l'incident. À cette fin, le ou la responsable du traitement des incidents de confidentialité ou l'équipe PRP établit le niveau du préjudice, en considérant notamment :

- La sensibilité des renseignements personnels en cause;
- L'impact potentiel de l'incident sur la personne concernée;
- Le potentiel de survenance du préjudice;
- La vulnérabilité des personnes en cause.

Le ou la responsable du traitement des incidents de confidentialité ou l'équipe PRP détermine si la personne concernée court, ou non, un risque de préjudice sérieux.

2.7 Notification de l'incident

2.7.1 En présence d'un risque de préjudice sérieux

Le ou la responsable de la protection des renseignements personnels au sein de l'Université signale la survenance d'un incident et des mesures correctives prises pour y remédier en diffusant les avis suivants.

2.7.1.1 L'avis à la Commission d'accès à l'information du Québec (CAI)

L'avis à la CAI doit être fait avec diligence. Le ou la responsable de la protection des renseignements personnels au sein de l'Université formule l'avis à la CAI et lui transmet.

Le contenu de l'*Avis à la CAI* se trouve en annexe.

2.7.1.2 L'avis à la personne concernée

L'avis à la personne concernée doit être fait avec diligence. Le ou la responsable de la protection des renseignements personnels au sein de l'Université formule l'avis à la personne concernée et lui transmet.

Le contenu de l'*Avis à la personne concernée* se trouve en annexe.

Cet avis se fait par tout moyen adéquat. Il peut s'agir d'un courriel ou d'une lettre postale. Toutefois, lorsqu'il est très difficile de joindre la personne directement, ou si l'on estime que l'avis direct à la personne concernée lui causerait un préjudice trop élevé, il est possible de recourir à un avis public. Le but est que la personne concernée ait ainsi indirectement connaissance de l'incident.

Le cas échéant, le ou la responsable de la protection des renseignements personnels au sein de l'Université rédige et publie cet avis.

Le ou la responsable de la protection des renseignements personnels au sein de l'Université n'est pas tenu d'aviser la personne concernée aussi longtemps que cet avis est susceptible d'entraver une enquête menée par un organisme chargé de prévenir, de détecter ou de réprimer une infraction aux lois.

2.7.1.3 L'avis à d'autres autorités

Dans certains cas particuliers d'incident impliquant des personnes concernées résidant hors du Québec, il est possible qu'une autre autorité régulatrice (au Canada ou à l'étranger) doive être informée de l'incident.

Si l'incident constitue un crime, le ou la responsable de la protection des renseignements personnels au sein de l'Université en informe le service de police compétent.

2.7.2 En l'absence d'un risque de préjudice sérieux

Le ou la responsable de la protection des renseignements personnels au sein de l'Université détermine s'il est pertinent d'informer de l'incident la personne concernée. Il peut choisir de le faire pour des raisons de transparence ou de gestion des affaires. Ces raisons sont documentées dans le registre des incidents de confidentialité.

Si l'incident constitue un crime, le ou la responsable de la protection des renseignements personnels au sein de l'Université en informe le service de police compétent.

2.7.3 Documenter les avis

Le ou la responsable du traitement des incidents de confidentialité ou l'équipe PRP documente les procédures menant à l'émission d'avis en vertu de la présente section.

2.7.4 Prise en charge de l'incident par l'assureur

Au besoin, le ou la responsable de la protection des renseignements personnels au sein de l'Université collabore avec l'assureur de l'Université pour la prise en charge de l'incident conformément à la police d'assurance.

2.8 Cartographie

Afin d'en faciliter la compréhension, le *Processus de traitement d'un incident de confidentialité* a été cartographié en annexe.

3 Registre des incidents de confidentialité

Le registre des incidents permet de documenter tous les incidents de confidentialité survenus, même ceux qui n'en sont pas après analyse de leur recevabilité. Outre son rôle essentiel lors d'un éventuel audit de conformité, ce registre permet de bonifier les plans de résilience, d'orienter au besoin l'offre de formation et de sensibilisation à l'équipe PRP et d'améliorer en continu la gestion des incidents.

Le registre répertorié est conforme aux dispositions de l'article 63.11 LAI.

4 Responsabilités

Outre les responsabilités dévolues au paragraphe 1.6 des présentes, le ou la responsable de la protection des renseignements personnels au sein de l'Université est responsable de la diffusion, de l'application et de la mise à jour de la présente procédure.

ANNEXES

Grille d’aide à la décision (paragraphe 2.3)

Fiche d’incident de confidentialité (paragraphe 2.4.1)

Évaluation des facteurs relatifs à la vie privée (EFVP) sommaire (paragraphe 2.5)

Contenu d’un avis à la Commission d’accès à l’information du Québec (paragraphe 2.7.1)

Contenu d’un avis à une personne concernée (paragraphe 2.7.2)

Processus de traitement d’un incident de confidentialité cartographié CAI (paragraphe 2.7.5)

Grille d'aide à la décision (paragraphe 2.3)

Le ou la responsable du traitement des incidents de confidentialité détermine s'il s'agit bien d'un incident de confidentialité.

Il ou elle doit pouvoir répondre successivement aux deux (2) questions suivantes :

1. Les informations et les objets de l'incident sont-ils des renseignements personnels et confidentiels?

2. Ces renseignements personnels ont-ils fait l'objet d'une :

    a) Consultation par une personne/entité non autorisée à en prendre connaissance;
    ou
    b) Transmission à une personne/entité non autorisée à les recevoir;
    ou
    c) Utilisation à des fins non autorisées par la Loi ou par la ou le titulaire de ces renseignements;
    ou
    d) Perte ou d'un vol dans des circonstances telles que l'hypothèse i), ii) ou iii) soit possible.

Si les réponses aux deux questions sont affirmatives, le processus se poursuit et une *Fiche d'incident de confidentialité* est remplie.

Si l'une des réponses aux deux questions est négative, il ne s'agit pas d'un incident de confidentialité et le processus est clos.

N. B. Il est important de documenter la démarche.

Fiche d'incident de confidentialité (paragraphe 2.4.1)

Fiche d'incident de confidentialité
(Articles 63.7 et suivants *Loi sur l'accès)*

Renseignements requis	Réponse	Commentaires / Informations complémentaires
Date de l'incident		
Date de signalement de l'incident		
Type/nature de l'incident : - **Accès non autorisé** - **Utilisation non autorisée** - **Communication non autorisée** - **Perte**		
Description de l'incident		
Renseignements personnels impliqués		
Nombre de personnes affectées		
Nombre d'informations (ou fichiers) impliquées		
Date d'échange avec l'équipe d'intervention PRP		
Degré de sensibilité du renseignement		
Conséquences possibles de l'utilisation du renseignement		
Probabilité d'utilisation du renseignement à des fins préjudiciable		
Niveau de préjudice global*		
Mesures de mitigation visant à diminuer le préjudice ou le risque de préjudice		
Mesures de mitigation visant à éviter la répétition du risque		
Le RP est-il « critique » (59 LAI)? **L'incident crée-t-il un risque de « préjudice sérieux » (63.9 LAI)?** - **Avis à la CAI** - **Avis aux personnes affectées** - **Avis public**		
Soutien aux personnes affectées		
Date de fin des mesures de mitigation		

* Selon l'évaluation des facteurs relatifs à la vie privée (EFVP) sommaire

Évaluation des facteurs relatifs à la vie privée (EFVP) sommaire (paragraphe 2.5)

Évaluation des facteurs relatifs à la vie privée (EFVP) sommaire
(Articles 63.7 et suivants *Loi sur l'accès)*

EFVP

DEGRÉ DE GRAVITÉ ➔➔➔				
	Équipe d'intervention PRP ***Équipe d'intervention PRP bonifiée*** ***Équipe d'urgence PRP***			
	NIVEAU 4	***NIVEAU 4***	***NIVEAU 4***	***NIVEAU 5***
	NIVEAU 3	***NIVEAU 3***	***NIVEAU 4***	***NIVEAU 4***
	NIVEAU 2	***NIVEAU 3***	***NIVEAU 3***	***NIVEAU 3***
	NIVEAU 1	***NIVEAU 1***	***NIVEAU 1***	***NIVEAU 1***
	DEGRÉ DE GRAVITÉ ➔➔➔			

CRITÈRES D'ÉVALUATION

Les RP sont non critiques - ***Données personnelles de base*** ***Les RP sont critiques*** - ***Données financières relatives à un paiement*** - ***Données financières autres*** ***Les RP sont critiques*** - ***Données personnelles relatives à l'intimité ou à la vie personnelle*** ***Les RP affectent 1 personne*** ***Les RP affectent 2 à 100 personnes*** ***Les RP affectent plus de 100 personnes*** ***Les RP affectent plus de 10 000 personnes*** ***Risque mitigé de réutilisation du RP*** ***Risque important de réutilisation du RP*** ***Impact mitigé sur la vie personnelle ou professionnelle*** ***Impact important sur la vie personnelle ou professionnelle*** ***Illégalité à la base de l'incident*** ***Impact réputationnel mitigé sur l'Université TÉLUQ*** ***Impact réputationnel sur l'Université TÉLUQ*** ***Incident nécessitant un avis aux personnes concernées (risque de préjudice grave)*** ***Incident nécessitant un avis public*** ***Incident nécessitant un avis à la CAI***	***NIVEAU 1*** ***Tous les critères sont en vert*** ***Aucune autre couleur*** ***NIVEAU 2*** ***Tous les critères sont en vert*** ***Un critère peut être en jaune*** ***NIVEAU 3*** ***Plus d'un critère est en jaune*** ***Aucun critère n'est en rouge*** ***NIVEAU 4*** ***Tous les critères sont en vert ou jaune*** ***Un critère peut être rouge*** ***NIVEAU 5*** ***Tous les critères sont en vert ou jaune*** ***Plus d'un critère est en rouge***

Contenu d'un avis à la Commission d'accès à l'information du Québec (paragraphe 2.7.1)

(Article 3, Règlement sur les incidents de confidentialité)

L'avis à la CAI qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, donné en application de l'article 63.8 de la Loi, est fait par écrit et doit contenir les informations suivantes :

1. Le nom de l'organisation ayant fait l'objet de l'incident de confidentialité.
2. Une brève description de la nature de l'atteinte et des circonstances de l'incident et, si elle est connue, sa cause.
3. Une description des catégories de renseignements personnels concernées ou, si cela n'est pas possible, la raison justifiant l'impossibilité de fournir une telle description.
4. Le nombre de personnes concernées et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'il n'est pas connu, une approximation de ce nombre.
5. Les mesures que l'organisme public a prises ou entend prendre afin d'aviser les personnes concernées dont un renseignement personnel est concerné par l'incident (art. 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels) ainsi que la date à laquelle les personnes concernées ont été avisées ou le délai envisagé pour les aviser.
6. Le nom et les coordonnées de la personne à contacter relativement à l'incident de confidentialité (la ou le chef d'équipe d'intervention ou le ou la responsable de la protection des renseignements personnels).
7. Les conséquences de l'incident de confidentialité, y compris une description des éléments qui amènent l'organisme public ou l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées (sensibilité des renseignements personnels concernés, différentes utilisations malveillantes possibles desdits renseignements personnels et probabilité de leur usage à des fins préjudiciables).
8. Les mesures prises pour remédier à l'incident de confidentialité et éviter que de nouveaux incidents de même nature ne se produisent, ainsi que le délai où les mesures ont été prises ou le délai d'exécution envisagé.
9. Toute information relative à l'incident de confidentialité, y compris notamment sa cause et ses circonstances, la date ou la période où l'incident a eu lieu, ou une approximation de cette période, la date ou la période au cours de laquelle l'organisme public a pris connaissance de l'incident.
10. Le cas échéant, une mention précisant qu'une personne, un organisme public ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

Contenu d'un avis à une personne concernée (paragraphe 2.7.2)

(Article 5, Règlement sur les incidents de confidentialité)

L'avis aux personnes concernées qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, donné en application de l'article 63.8 de la Loi, est fait par écrit et doit contenir les informations suivantes :

1. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2. Une brève description des circonstances de l'incident;
3. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette date ou période;
4. Une brève description des mesures que l'organisme public a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer le risque qu'un préjudice lui soit causé;
5. Les mesures que l'organisme public suggère aux personnes concernées afin de diminuer le risque qu'un préjudice leur soit causé ou afin d'atténuer un tel effet;
6. Les coordonnées permettant aux personnes concernées de se renseigner davantage relativement à l'incident.

Si, en raison du nombre de personnes concernées, il est disproportionnellement difficile d'en informer chacune d'elles, le ou la responsable de la protection des renseignements personnels au sein de l'Université doit prendre les mesures nécessaires pour s'assurer que les personnes concernées en sont informées, par avis public, en l'affichant sur le site web institutionnel et en utilisant des canaux appropriés et accessibles au public.

Processus de traitement d'un incident de confidentialité cartographié CAI (paragraphe 2.7.5)

PROCESSUS DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

PAR TOUT LE PERSONNEL

1. Protéger les renseignements personnels auxquels il a accès

▼
▼

2. Réviser annuellement la liste des renseignements personnels qui sont nécessaires à son travail

et

Informer son supérieur immédiat ou sa supérieure immédiate de ceux qui ne le sont pas

▼
▼

3. Découverte d'un incident de confidentialité ou d'un risque d'incident de confidentialité (incident = intervention, risque = prévention)

La découverte d'un incident de confidentialité signifie :

- avoir une connaissance directe de l'incident;
- avoir un motif de croire en la survenance d'un incident;
- ou même soupçonner la survenance d'un incident.

EXEMPLES

Avoir accès à un renseignement personnel auquel il n'a pas habituellement accès

Partager un renseignement personnel à une personne qui n'y a pas habituellement accès

▼
▼

4. Signaler l'incident de confidentialité au ou à la responsable au :
INCIDENTDECONFIDENTIALITE@teluq.ca

Et en informer sa supérieure immédiate ou son supérieur immédiat, sauf si cette personne est impliquée

5. Préserver les preuves de l'incident

6. Prendre les mesures correctives immédiates demandées par le ou la responsable

▼
▼

7. Collaborer au processus de gestion de l'incident de confidentialité

* **Incident de confidentialité** : Toute utilisation ou communication, ou tout accès non autorisé par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection ou à son caractère confidentiel.

PROCESSUS DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

PAR LE RESPONSABLE DU TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ

1. Recevoir le signalement

▼

▼

2. Analyser la recevabilité

Grille d'aide à la décision

▼

▼

3. Remplir la Fiche d'incident de confidentialité (circonstances de l'incident)

Fiche d'incident de confidentialité

▼

▼

4. Prendre les mesures correctives immédiates qui s'imposent

▼

▼

5. Faire une évaluation des facteurs relatifs à la vie privée (EFVP) sommaire (gravité de l'incident)

NIVEAU 1 : ACCEPTABLE (3 membres)
NIVEAU 2 : ACCEPTABLE, AVEC MESURES CORRECTIVES MINEURES (3 membres)
NIVEAU 3 : INACCEPTABLE, AVEC MESURES CORRECTIVES MAJEURES (5 membres)
NIVEAU 4 : INACCEPTABLE, SANS MESURE D'URGENCE (7 membres)
NIVEAU 5 : INACCEPTABLE, AVEC MESURE D'URGENCE (7 membres)

▼

▼

6. S'adjoindre les ressources associées prévues au processus, selon le besoin

▼

▼

7. Mettre en place le processus de gestion de l'incident de confidentialité

▼

▼

8. Appliquer les mesures correctrices et les mesures préventives

▼

▼

9. Inscription aux registres

9.1 des incidents de sécurité (TI)

9.2 des incidents de confidentialité (SG)

Processus de traitement d'un incident de confidentialité recommandé par la CAI (paragraphe 2.7.5)