Université du Québec à Rimouski

TITRE :	**PROCEDURE RELATIVE A LA GESTION DES INCIDENTS DE CONFIDENTIALITE IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS** **C3-D110**
APPROUVEE :	SECRETARIAT GENERAL ET VICE-RECTORAT A LA VIE ETUDIANTE
EN VIGUEUR :	LE 5 OCTOBRE 2022
RESPONSABILITE :	SECRETARIAT GENERAL ET VICE-RECTORAT A LA VIE ETUDIANTE

TABLE DES MATIÈRES

§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§

1. PRÉAMBULE

L'Université du Québec à Rimouski (UQAR) est responsable des renseignements personnels qu'elle traite dans le cadre de ses activités et est responsable de veiller à leur protection. Par le fait même, l'UQAR est responsable de mettre en place un protocole de gestion advenant un incident de sécurité impliquant ce type de renseignements. Cette procédure s'inscrit dans la foulée des actions prises par l'UQAR pour assurer la protection des renseignements personnels.

2. OBJECTIF

La présente procédure permet de définir ce qu'est un incident de confidentialité et prescrit la marche à suivre lorsque survient un tel incident. Elle identifie également les rôles et responsabilités des différentes personnes intervenant dans le processus.

Elle a pour objectif de préciser la prise en charge de ces incidents, en plus d'en réduire le nombre et leur impact.

3. DÉFINITIONS

« Confidentialité » : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et qui n'est divulguée qu'à celles-ci.

« Incident de confidentialité » : Accès non autorisé par la Loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection. Sont notamment considérés comme des incidents de confidentialité :

- Un membre du personnel consulte ou utilise des renseignements personnels non nécessaires à l'exercice de ses fonctions;
- Un pirate informatique s'infiltre dans un système et a accès à des renseignements personnels;
- Une communication contenant des renseignements personnels est transmise par erreur à la mauvaise personne;
- Une personne perd ou se fait voler des documents contenant des renseignements personnels;
- Une personne s'immisce dans une banque de données contenant des renseignements personnels;
- Une personne accède à un lieu physique sans autorisation et a accès à des renseignements personnels dans les documents y étant présents;
- Une personne vole un document contenant des renseignements personnels.

« Préjudice sérieux » : Est déterminé suivant l'analyse de la sensibilité des renseignements personnels concernés, l'éventualité d'utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables.

« Renseignement personnel » : Un renseignement concernant une personne et permettant de l'identifier.

4. CADRE NORMATIF

Cette procédure relève de la *Politique établissant le cadre de gouvernance en matière de protection des renseignements personnels* (à venir) et de :

- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c.25;
- *Politique de la sécurité de l'information*;
- *Cadre de gestion de la sécurité de l'information*;
- Règlement sur les incidents de confidentialité (édiction à venir).

5. CHAMP D'APPLICATION

Cette procédure s'applique à toutes les personnes membres du personnel de l'UQAR et vise tous les incidents impliquant la confidentialité de l'information, que celle-ci soit sur support numérique ou papier, comportant des renseignements personnels qui sont collectés, conservés, utilisés, communiqués ou détruits par l'UQAR. Cette procédure s'applique également à tout accès non autorisé à des locaux ou lieux physiques susceptibles d'avoir une incidence sur la confidentialité des documents y étant contenus.

6. RÔLES ET RESPONSABILITÉS

La personne responsable de l'accès aux documents et à la protection des renseignements personnels à l'UQAR :

- Assure la prise en charge de tout incident de confidentialité;
- Procède à l'analyse de la nature du préjudice suivant la déclaration d'un incident de confidentialité;
- Coordonne l'application des mesures de mitigation du préjudice;
- Assure le suivi, l'évaluation et la mise à jour des étapes de prise en charge d'un incident de confidentialité.

À l'UQAR, la personne responsable de l'accès aux documents et de la protection des renseignements personnels est le secrétaire général et vice-recteur à la vie étudiante.

Le Comité sur l'accès à l'information et la protection des renseignements personnels (ci-après « Comité ») participe, en collaboration avec la personne responsable de l'accès aux documents et de la protection des renseignements personnels, au suivi et à l'amélioration de la prise en charge d'un incident de confidentialité impliquant des renseignements personnels. Le comité peut, le cas échéant, proposer toute modification à la présente procédure.

Le comité participe également, conformément à l'article 8 de la présente procédure, aux démarches de prévention des incidents de confidentialité impliquant des renseignements personnels.

7. PROTOCOLE EN CAS D'INCIDENT

7.1 Toute personne qui détecte un incident impliquant la confidentialité de l'information, quelle que soit sa nature, ou qui a des motifs de croire qu'un incident s'est produit doit immédiatement déclarer celui-ci via l'un des moyens suivants :

- Ouvrir un billet « Incident de sécurité informatique » à travers le Système de gestion des demandes de service (SGDS/Octopus) disponible à l'adresse suivante : https://sgds.uqar.ca;
- Communiquer avec le Centre de service TI par téléphone en composant le poste 1717 à partir d'un poste interne ou encore d'un des numéros téléphoniques principaux de l'UQAR;
- Communiquer avec le Centre de service TI (CSTI) en transmettant un courriel à l'adresse csti@uqar.ca;
- Communiquer avec le Secrétariat général et vice-rectorat à la vie étudiante en transmettant un courriel à l'adresse : prp@uqar.ca.

7.2 Toute personne visée à l'article 7.1 doit également aviser la personne supérieure immédiate.

7.3 À la déclaration d'un incident, un billet d'incident est créé afin d'assurer la gestion et le suivi de l'incident.

7.4 La personne responsable de l'accès aux documents et de la protection des renseignements personnels, ou toute autre personne qu'elle désigne pour assurer la prise en charge de l'incident, sera chargée dès la réception de la déclaration de l'incident :

- D'établir sommairement les circonstances de l'incident;
- D'identifier l'information et, le cas échéant, les renseignements personnels concernés par l'incident;
- D'identifier les personnes visées par l'incident.

7.5 Dès la déclaration de l'incident, les personnes impliquées dans la prise en charge peuvent poser tout geste de mitigation afin de diminuer les risques qu'un préjudice soit causé, amplifié ou qu'il ne se reproduise.

7.6 La personne responsable de la protection des renseignements personnels, en collaboration avec toute personne de son choix, détermine la nature du préjudice. À cet effet, la personne responsable de la protection des renseignements personnels tient compte, notamment :

- De la sensibilité des renseignements concernés;
- Des conséquences appréhendées;
- De la probabilité de l'utilisation à des fins préjudiciables.

7.7 S'il y a absence d'un préjudice ou que celui-ci est mineur, la personne responsable de la protection des renseignements personnels peut, si les mesures de mitigation entreprises en vertu de l'article 7.5 ne sont pas suffisantes, mettre en œuvre toute autre mesure en vue de régler l'incident.

7.8 S'il y a un préjudice sérieux ou si le préjudice est à risque de le devenir, la personne responsable de la protection des renseignements personnels doit :
- Aviser la Commission d'accès à l'information;
- Aviser les personnes concernées, sauf si l'avis est susceptible d'entraver une enquête;
- Aviser avec discrétion les personnes ou organismes susceptibles de diminuer le préjudice et ne communiquer que les renseignements nécessaires;
- Inscrire cette communication dans le registre des incidents de confidentialité de l'UQAR.

7.9 L'avis à la Commission d'accès à l'information prévu à l'article 7.8 est fait par écrit conformément à ce qui est prévu à l'Annexe 2:

7.10 La Commission d'accès à l'information peut, lorsqu'un incident de confidentialité est porté à son attention conformément à l'article 7.8, ordonner à toute personne, après lui avoir fourni l'occasion de présenter ses observations, l'application de toute mesure visant à protéger les droits des personnes concernées par la présente procédure pour le temps et aux conditions qu'elle détermine. Elle peut notamment ordonner la remise des renseignements personnels impliqués à l'UQAR ou leur destruction.

7.11 La personne visée par une ordonnance sans qu'elle en ait été informée au préalable parce que, de l'avis de la Commission d'accès à l'information, il y a urgence ou danger de causer un préjudice irréparable, peut, dans le délai indiqué dans l'ordonnance, présenter ses observations pour en permettre le réexamen par la Commission d'accès à l'information.

7.12 L'avis aux personnes concernées par l'incident de confidentialité prévu à l'article 7.8 contient :
- 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;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

- Une brève description des mesures que l'UQAR a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
- Les mesures que l'UQAR suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- Les coordonnées de la personne responsable de l'accès aux documents et de la protection des renseignements personnels permettant à la personne concernée de se renseigner davantage relativement à l'incident.

7.13 La personne responsable de la protection des renseignements personnels inscrit l'incident de confidentialité au registre des incidents de confidentialité conformément à ce qui est prévu à l'Annexe 3.

7.14 Pour tout incident de nature à avoir des incidences sur la sécurité de l'information, la personne responsable de l'accès aux documents et de la protection des renseignements personnels s'assure de s'adjoindre des personnes nécessaires auprès du Service des technologies de l'information, le tout conformément aux règlements, politiques et directives applicables en la matière. De même, pour tout incident impliquant le vol de documents ou un accès non autorisé à des locaux ou à tout lieu physique, la personne responsable de l'accès aux documents et de la protection des renseignements personnels s'assure de s'adjoindre des personnes nécessaires auprès du Service des terrains, bâtiments et de l'équipement.

7.15 L'incident de confidentialité est considéré comme réglé lorsque les mesures entreprises en vertu de l'article 7.5 ou celles mises en application subséquemment ont eu les impacts jugés satisfaisants par la personne responsable de l'accès aux documents et de la protection des renseignements personnels et qu'elles permettent d'atténuer les risques qu'un incident similaire ne se reproduise.

8. PRÉVENTION

8.1 La personne responsable de l'accès aux documents et de la protection des renseignements personnels fait rapport au Comité, annuellement, des incidents de confidentialité pris en charge, des mesures mises en œuvre et des impacts de celles-ci dans une perspective d'amélioration par l'établissement de moyens ou mécanismes permettant de prévenir la survenance d'incidents de confidentialité.

8.2 La présente procédure peut être revue, au besoin, afin de refléter tout changement législatif ou tout moyen de prévention adopté en vertu de l'article 8.1.

Annexe 1 - Procédure en cas d'incidents de confidentialité

	Incidents de cybersécurité	**Autres incidents (vol de documents, accès non autorisé à des locaux, etc.)**
	Toute personne qui a un motif de croire qu'un incident de confidentialité s'est produit doit le déclarer via le Système de gestion des demandes de service, à csti@uqar.ca ou à prp@uqar.ca . Cette personne doit également aviser sa personne supérieure immédiate.	Toute personne qui a un motif de croire qu'un incident de confidentialité s'est produit doit le déclarer à prp@uqar.ca . Cette personne doit également aviser sa personne supérieure immédiate .
Étape 1	Si la demande est traitée par le CSTI, le service doit contacter la personne responsable de la protection des renseignements personnels si elle n'est pas déjà au courant. Cette dernière personne doit : - établir sommairement les circonstances de l'incident; - identifier l'information et, le cas échéant, les renseignements personnels concernés par l'incident; - identifier les personnes visées par l'incident.	La demande est traitée par la personne responsable de la protection des renseignements personnels qui doit : -contacter le Service des terrains, des bâtiments et de l'équipement (STBÉ); - établir sommairement les circonstances de l'incident; - identifier l'information et, le cas échéant, les renseignements personnels concernés par l'incident; - identifier les personnes visées par l'incident.
Étape 2	Analyser et si possible, poser des actions visant à diminuer les risques qu'un préjudice soit causé ou se reproduise (mesures de mitigation immédiates).	Analyser et si possible, poser des actions visant à diminuer les risques qu'un préjudice soit causé ou se reproduise (mesures de mitigation immédiates).

	Incidents de cybersécurité	**Autres incidents (vol de documents, accès non autorisé à des locaux, etc.)**
Étape 3	La personne responsable de la protection des renseignements personnels, en collaboration avec le CSTI, détermine la nature du préjudice. **Absence** d'un risque de préjudice sérieux : d'autres mesures de mitigation peuvent être mises en place afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise. Risque d'un **préjudice sérieux** : 1 La personne responsable de la protection des renseignements personnels doit aviser la Commission d'accès à l'information (article 63.8 de la Loi); 2 Aviser les personnes concernées (sauf si l'avis est susceptible d'entraver une enquête); 3 Aviser avec discrétion les personnes ou organismes susceptibles de diminuer le préjudice (communication des renseignements nécessaires) 4 Inscrire cette communication dans un registre (responsable de la protection des renseignements personnels).	La personne responsable de la protection des renseignements personnels, en collaboration avec le STBÉ, détermine la nature du préjudice. **Absence** d'un risque de préjudice sérieux : d'autres mesures de mitigation peuvent être mises en place afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise. Risque d'un **préjudice sérieux** : 1 La personne responsable de la protection des renseignements personnels doit aviser la Commission d'accès à l'information (article 63.8 de la Loi); 2 Aviser les personnes concernées (sauf si l'avis est susceptible d'entraver une enquête); 3 Aviser avec discrétion les personnes ou organismes susceptibles de diminuer le préjudice (communication des renseignements nécessaires) 4 Inscrire cette communication dans un registre (responsable de la protection des renseignements personnels).
Étape 4	Appliquer d'autres mesures de mitigation afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise.	Appliquer d'autres mesures de mitigation afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise.
Étape 5	La personne responsable de la protection des renseignements personnels inscrit l'incident de confidentialité au registre.	La personne responsable de la protection des renseignements personnels inscrit l'incident de confidentialité au registre.

Annexe 2 – L'avis à la Commission d'accès à l'information en cas de préjudice sérieux

L'avis à la Commission d'accès à l'information qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, est fait par écrit et doit contenir les renseignements suivants :

1. le nom de l'organisation ayant fait l'objet de l'incident de confidentialité;
2. le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident;
3. 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;
4. une brève description des circonstances de l'incident et, si elle est connue, sa cause;
5. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
6. la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
7. le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;
8. une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telle que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
9. les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 63.8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;
10. les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;
11. le cas échéant, une mention précisant qu'une personne 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.

Annexe 3 - Registre des incidents de confidentialité

Le registre des incidents de confidentialité doit contenir les éléments suivants :

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; une brève description des circonstances de l'incident;
2. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
3. la date ou la période au cours de laquelle l'UQAR a pris connaissance de l'incident;
4. le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
5. une description des éléments qui amènent l'UQAR à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées;
6. si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;
7. une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.