Le 13 octobre 2022

[redacted]

**Objet : Demande d'accès du 16 septembre 2022**
**N/D : 226356DAJ**

Maître,

En réponse à votre demande d'accès reçue à nos bureaux le 16 septembre dernier, vous trouverez ci-joint une copie de la « *Procédure en cas d'incident de confidentialité* » détenue par la Commission des normes, de l'équité, de la santé et de la sécurité du travail.

Nous devons vous informer que vous pouvez demander à la Commission d'accès à l'information de réviser cette décision. Nous joignons une note explicative concernant l'exercice de ce recours.

Espérant le tout à votre satisfaction, veuillez agréer, Maître, nos salutations distinguées.

La substitut de la responsable de l'accès aux documents et
de la protection des renseignements personnels,

Signature numérique de Paméla Bélanger Lapointe
DN : cn=Paméla Bélanger Lapointe, o=CNESST, ou, email=pamela.belangerlapointe@cnesst.gouv.qc.ca, c=CA
Date : 2022.10.13 13:19:31 -04'00'

Paméla Bélanger Lapointe, Avocate
*Pamela.BelangerLapointe@cnesst.gouv.qc.ca*
*Tél. : 418 266-4900, poste* [redacted]
*Téléc. : 418 528-7245*

PBL/cb

p. j.

## AVIS DE RECOURS EN RÉVISION

## RÉVISION

### a) Pouvoir

L'article 135 de la Loi prévoit qu'une personne peut, lorsque sa demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels ou dans le cas où le délai prévu pour répondre est expiré, demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

**QUÉBEC**

Commission d'accès à l'information
Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9

Tél : (418) 528-7741
Téléc : (418) 529-3102

**MONTRÉAL**

Commission d'accès à l'information
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4

Tél : (514) 873-4196
Téléc : (514) 844-6170

### b) Motifs

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

### c) Délais

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

# PROCÉDURE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

Commission des normes, de l'équité, de la santé et de la sécurité du travail

Septembre 2022

# PROCÉDURE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

## PRÉAMBULE

La Commission des normes, de l'équité, de la santé et de la sécurité du travail (ci-après la « CNESST ») accorde une grande importance à la protection des renseignements personnels et confidentiels qu'elle détient, tel qu'en fait foi son engagement à cet égard dans sa déclaration de services. Conséquemment, elle met en œuvre des moyens physiques, technologiques et administratifs afin d'assurer le caractère confidentiel des renseignements détenus et veille à ce que leur traitement soit fait dans le respect des droits des travailleurs, des employeurs et des tiers, de même qu'en conformité aux exigences du cadre légal en vigueur. Divers moyens de prévention et de détection en place à la CNESST sont destinés à prévenir les incidents de confidentialité.

Toutefois, la CNESST communiquant des millions de documents et de renseignements à caractère confidentiel annuellement, notamment aux travailleurs, aux employeurs, à leurs représentants et aux instances administratives et judiciaires, le risque que survienne un incident de confidentialité demeure toujours présent. En effet, aucune mesure de prévention et de sécurité ne saurait garantir une étanchéité exempte de toute erreur ou malversation.

Il importe donc que la CNESST se dote d'une stratégie d'intervention en cas d'incident de confidentialité afin d'en limiter les conséquences. Une intervention efficace et l'instauration de mesures correctives sont alors de mises pour éviter l'aggravation et la reproduction de l'incident de confidentialité.

## OBJET ET PORTÉE

La présente procédure vise à mettre en place une stratégie d'intervention en cas d'incident de confidentialité. Elle définit le rôle des intervenants impliqués et énonce les principes et la procédure devant guider les interventions de la CNESST en cas d'incident de confidentialité. Elle doit s'interpréter en harmonie avec la gestion des incidents prévue par le nouveau processus de gestion des menaces, des vulnérabilités et des incidents ainsi que par le *Processus de gestion des incidents de sécurité de l'information* (https://intranet.cnesst.qc/cnesst/securite-de-linformation/processus-de-securite-et-architecture/).

La *Loi sur l'accès à l'information* définit « incident de confidentialité » comme étant l'accès, l'utilisation ou la communication d'un renseignement personnel qui n'est pas autorisé par la loi. Il peut également s'agir de la perte d'un renseignement personnel ou tout autre atteinte à la protection des renseignements personnels.[1] La CNESST accorde

[1] Art. 63.8 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

une grande importance à tous les documents contenant des renseignements confidentiels, aussi la présente politique s'applique également à l'égard de ceux-ci. Une situation d'incident de confidentialité peut survenir sans égard au support sur lequel l'information est divulguée (papier, électronique, communication orale, etc.). Un incident de confidentialité peut être intentionnel ou accidentel et être le fait d'un membre du personnel de la CNESST ou d'un tiers. Toute divulgation de renseignements personnels ou confidentiels non autorisée par la loi ou par la personne concernée par ces renseignements constitue une divulgation illégale.

Les incidents de confidentialité doivent être traités avec diligence et efficacité, et ce, dans les meilleurs délais. À titre d'illustration, des exemples de situations constituant des incidents de confidentialité sont présentés à l'Annexe 1 de la présente procédure.

## INTERVENANTS

### CHEF DÉLÉGUÉ DE LA SÉCURITÉ DE L'INFORMATION (VPTN)

Le chef délégué de la sécurité de l'information assume, sous le lien fonctionnel du chef gouvernemental de la sécurité de l'information, les responsabilités décrites dans la *Directive gouvernementale sur la sécurité de l'information*. Il doit entre autres mettre en œuvre un cadre de gouvernance qui regroupe plusieurs domaines, dont la cybersécurité, l'éthique, la sécurité physique et la protection des renseignements personnels.

(ci-après « **CDSI** »)

### COORDINATEUR ORGANISATIONNEL DES MESURES DE SÉCURITÉ DE L'INFORMATION (VPTN)

Le coordonnateur organisationnel des mesures de sécurité de l'information assume les responsabilités décrites dans le processus de gestion des menaces, des vulnérabilités et des incidents (PGMVI), conformément à ce que prévoit la *Politique relative à l'accès, la protection et la sécurité de l'information* de la CNESST. Le **COMSI** est identifié dans le *Registre d'autorités sur la sécurité de l'information et la protection des renseignements personnels*. Ces deux documents sont disponibles sur le site intranet de la CNESST, sous la rubrique « Sécurité de l'information » (http://intranet.cnesst.qc/cnesst/securite-de-linformation/politiques-cadres-directives-et-orientations/).

(ci-après « **COMSI** »)

### INTERVENANT DE LA CNESST

Tous les membres du personnel de la CNESST, incluant les membres de la Commission, sont considérés comme des **intervenants** aux fins de la présente procédure. Ils doivent contribuer au respect et à la mise en application de la présente procédure en signalant tout incident de confidentialité dont ils ont connaissance et en respectant les instructions du **répondant** et, le cas échéant, de l'**Unité dédiée** et du **COMSI**.

(ci-après « **intervenant** »)

## RÉPONDANT EN MATIÈRE D'ACCÈS À L'INFORMATION ET EN PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le répondant en matière d'accès aux documents et de protection des renseignements personnels est responsable de la résolution des incidents de confidentialité de son unité administrative. Il assure un rôle de contact principal entre son unité administrative, la **responsable de l'accès** et le **COMSI**. Les **répondants** de chaque unité administrative sont identifiés dans la liste des répondants. Cette liste est disponible sur le site intranet de la CNESST, via le lien suivant :

« https://intranet.cnesst.qc/fileadmin/Intranet/employe/repondants/acces-doc-protection-renseignements/li_rep_acc_info.pdf ».

(ci-après « r**épondant** »)

## RÉPONDANT EN ÉTHIQUE (DGRH)

Le répondant en éthique est responsable d'assister et conseiller le **répondant** relativement aux aspects éthiques liés aux incidents de confidentialité. Il est désigné par le dirigeant d'organisme conformément à l'article 11 de la Directive gouvernementale sur la sécurité de l'information.

(ci-après « r**épondant en éthique** »)

## RESPONSABLE DE L'ACCÈS AUX DOCUMENTS ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (DGAJ)

La personne responsable de l'accès aux documents et de la protection des renseignements personnels assume les responsabilités que lui attribuent diverses lois et directives gouvernementales, notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après la « LAI »), la *Politique relative à l'accès, la protection et la sécurité de l'information* de la CNESST et son *Cadre de gestion relatif à l'accès, la protection et la sécurité de l'information*. La responsable de l'accès est identifiée dans le *Registre d'autorités sur la sécurité de l'information et la protection des renseignements personnels*. Ces trois derniers documents sont disponibles sous la rubrique « Sécurité de l'information » dans l'intranet de la CNESST(https://intranet.cnesst.qc/cnesst/securite-de-linformation/politiques-cadres-directives-et-orientations//). Elle peut s'adjoindre un **substitut de la responsable**, sauf exception, relativement aux démarches prévues à la présente procédure dont elle a la responsabilité de veiller à son application.

(ci-après « **responsable de l'accès** »)

## SUBSTITUTS DE LA RESPONSABLE DE L'ACCÈS AUX DOCUMENTS ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (DGAJ)

Les substituts de la **responsable de l'accès** sont des avocats faisant partie de l'**unité dédiée**. Ils œuvrent à titre conseillers juridiques et représentants pour la CNESST en matière d'accès à l'information et de protection des renseignements personnels. Ils exercent également les pouvoirs et responsabilités octroyées à la **responsable de l'accès** par LAI. Dans certains cas, le rôle du substitut relatif à la présente procédure peut être effectué par un autre avocat de la DGAJ.

(ci-après « **substitut de la Responsable** »)

## UNITÉ DÉDIÉE EN MATIÈRE D'ACCÈS À L'INFORMATION (DGAJ)

L'unité dédiée en matière d'accès à l'information fait partie de la Direction générale des affaires juridiques (DGAJ). Elle œuvre dans le domaine de l'accès à l'information et de la protection des renseignements personnels. Elle assiste la r**esponsable de l'accès** dans l'exécution de ses responsabilités attribuées par la LAI. Elle est composée de personnels juridiques, incluant notamment des avocats agissant à titre de **substituts de la responsable**. L'**unité dédiée** fait partie de la Direction des affaires juridiques Est et Accès à l'information (DAJ SST Est et Accès à l'information).

(ci-après « **unité dédiée** »)

# PROCÉDURE À SUIVRE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

## 1. Dénonciation de l'incident de confidentialité par l'intervenant

Un **intervenant**, lorsqu'il a connaissance d'une situation pouvant constituer un incident de confidentialité, doit immédiatement en aviser le **répondant** de son unité administrative.

Que l'incident soit accidentel ou intentionnel, cette obligation demeure même si :

- L'incident présumé est survenu dans un dossier qui n'est pas sous sa responsabilité ;
- L'incident présumé est survenu dans un dossier d'une autre direction ;
- L'incident présumé ne découle pas d'une de ses actions, mais de celle d'un autre intervenant ;
- La problématique présumée à l'origine de l'incident a déjà été corrigée.

Par ailleurs, l'i**ntervenant** doit dénoncer toutes les situations pour lesquelles il a des motifs raisonnables de croire qu'un incident de confidentialité est survenu. Il appartiendra par la suite au **répondant** et à l'**unité dédiée** de déterminer s'il s'agit effectivement d'un incident de confidentialité au sens de la présente procédure.

## 2. Signalement de l'incident de confidentialité par le répondant

Le **répondant**, lorsqu'il reçoit la dénonciation d'un incident de confidentialité, doit agir rapidement afin de le signaler à l'**unité dédiée**. Pour ce faire, le formulaire *Déclaration d'incident de confidentialité* doit être complété et transmis à l'**unité dédiée** dans les meilleurs délais. Cette déclaration est disponible sur l'intranet à l'adresse suivante : https://intranet.cnesst.qc/employe/repondants/repondants-acces-aux-documents-et-protection-des-renseignements-personnels/).

Le **répondant** est responsable de la gestion de l'incident de confidentialité et il doit mettre en œuvre la présente procédure. Il est responsable de faire remplir ce formulaire convenablement par la personne qu'il juge appropriée. Cette personne devra indiquer tous les renseignements pertinents afin de permettre à l'**unité dédiée** de bien comprendre et évaluer la situation. Le **répondant** peut également compléter lui-même ce formulaire à l'aide des renseignements qu'il a obtenus.

Une fois le formulaire convenablement complété, le **répondant** doit en transmettre une copie électronique à l'**Unité dédiée** par le biais de la boîte courriel AR Accès (aracces@cnesst.gouv.qc.ca).

## 2.1 Signalement d'un incident concernant une autre direction

Il peut arriver qu'un **intervenant** constate et dénonce un incident de confidentialité relatif à une autre direction. À titre d'exemple :

> *Un fournisseur offrant des services à plusieurs directions avise un **intervenant** qu'il a reçu des renseignements personnels d'un travailleur pour lequel il n'offre pas de services. Après avoir été avisé de l'incident, le **répondant** constate que le dossier du travailleur n'est pas traité par sa direction, mais plutôt par la direction voisine.*

Si le **répondant** constate que l'incident lui ayant été dénoncé concerne un dossier d'une autre direction, il doit immédiatement transmettre un courriel au **répondant** de la direction concernée en lui fournissant l'ensemble des renseignements pertinents qu'il détient relativement à cette situation. Il doit mettre la boîte courriel AR Accès (aracces@cnesst.gouv.qc.ca) en copie conforme de cette communication. Il appartiendra alors au **répondant** de la direction concernée d'entreprendre les démarches prévues à la présente procédure, dont celle de remplir le formulaire de *Dénonciation d'un incident de confidentialité*.

## 2.2 Signalement d'un incident concernant plusieurs directions

Il peut arriver qu'un incident de sécurité concerne plusieurs directions. À titre d'exemple :

> *Lors de l'ouverture d'un dossier, une erreur est commise dans l'inscription de l'employeur au dossier. Ainsi, tout au long du traitement du dossier, des communications sont transmises au mauvais employeur. Aucun **intervenant** ne constate cette situation. Le dossier est ensuite transféré dans une autre direction. L'erreur dans l'inscription de l'employeur n'est toujours pas corrigée et de nouvelles communications sont transmises au mauvais employeur par la nouvelle direction. Un **intervenant** de la nouvelle direction constate alors la problématique et la dénonce immédiatement à son **répondant**.*

Si le **répondant** constate que l'incident lui ayant été dénoncé a été reproduit par sa direction, il sera responsable du traitement des incidents survenus alors que le dossier était dans sa direction, de même que tout autre incident précédent. La responsabilité du traitement de l'ensemble de l'incident incombera ainsi au **répondant** de la dernière direction ayant reproduit l'incident. Il devra alors s'assurer que l'incident soit traité conformément à la présente procédure, autant pour la portion touchant sa direction que la portion en touchant une autre. Le **répondant** de la direction ayant initialement commis l'incident de confidentialité se doit de collaborer avec le **répondant** de la direction qui est responsable du traitement de cet incident de confidentialité. Il doit donc répondre à ses questions et lui fournir toutes les informations nécessaires pour régler l'incident en question.

Inversement, si le **répondant** constate que l'incident lui ayant été dénoncé n'a pas été reproduit par sa direction, il se trouvera alors dans une situation similaire à celle décrite à la section 2.1 (Signalement d'un incident concernant une autre direction) de la présente procédure et devra ainsi aviser le **répondant** de la direction concernée de l'incident en s'assurant que la boîte courriel AR Accès (aracces@cnesst.gouv.qc.ca) soit en copie conforme.

## 3. Démarches de résolution de l'incident de confidentialité par le répondant

Dès que le **répondant** reçoit la dénonciation d'un incident de confidentialité, il doit immédiatement entreprendre des démarches afin d'en minimiser l'impact et en limiter les conséquences. Le **répondant** est responsable de s'assurer que les actions nécessaires à cette fin soient effectuées.

Le **répondant** peut s'adjoindre, dans la réalisation de ces démarches, toute personne permettant une résolution efficace de l'incident. Le **répondant** demeure toutefois responsable de la bonne exécution des démarches nécessaires et du traitement conforme de l'incident de confidentialité.

### 3.1. Identification et résolution de la cause de l'incident

Il est primordial, dès le signalement d'un incident de confidentialité, que le **répondant** tente d'en identifier la cause. En effet, le premier objectif de la présente procédure est d'assurer que les incidents de confidentialité ne se reproduisent pas.

Le gestionnaire de l'unité administrative, en collaboration avec le **répondant,** devra s'assurer que la problématique ayant causé l'incident soit identifiée et convenablement corrigée.

Par exemple :

- Si une lettre est transmise à la mauvaise personne dans un dossier, s'assurer que ses coordonnées soient retirées du dossier pour éviter que d'autres lettres ne lui soient transmises ;
- Si une lettre est transmise à l'ancienne adresse d'une personne, s'assurer que l'adresse soit modifiée pour l'ensemble du dossier pour éviter que d'autres lettres ne soient transmises à la mauvaise adresse.

Il appartient donc au gestionnaire de l'unité administrative, en collaboration avec le **répondant**, de s'assurer que ces démarches soient effectuées avec succès pour éviter une répétition du même incident, notamment par la mise en place ou l'amélioration des mesures administratives.

### 3.2. Résolution des conséquences de l'incident

Une fois l'étape de l'identification de la cause de l'incident complétée, il sera nécessaire pour le **répondant** de s'assurer que des démarches soient entreprises afin de minimiser et limiter les conséquences de l'incident. Les actions pertinentes à cette fin peuvent varier selon les circonstances et devront être adaptées pour chaque cas d'espèce. Or, deux principales démarches devront être effectuées dans la quasi-totalité des situations.

D'abord, dans le cas d'incidents de confidentialité touchant des documents physiques, le **répondant** devra obtenir la restitution des documents concernés dans l'incident auprès du tiers. S'il n'est pas possible d'en obtenir la restitution, le **répondant** devra s'assurer que ceux-ci soient détruits de façon sécuritaire. Ce sera également le cas si les documents ont été transmis de façon électronique. La destruction sécuritaire fait référence à l'utilisation d'un procédé permettant de détruire de manière irréversible les renseignements confidentiels. Ainsi, les documents papier doivent être déchiquetés avant d'être jetés au rebut ou acheminés pour recyclage ou incinération. Les documents électroniques et leurs supports (disquettes, cédéroms, cartouches, rubans magnétiques, cassettes audio ou vidéo, disques durs, etc.) doivent être effacés selon un procédé qui ne permet pas d'en reconstituer le contenu. Ils peuvent aussi être physiquement détruits par déchiquetage ou broyage. Évidemment, dans le cas de renseignements communiqués oralement au tiers, il sera impossible d'en obtenir la restitution ou la destruction.

Ensuite, le **répondant** devra transmettre au tiers une attestation de confidentialité appropriée à la situation. Plusieurs modèles d'attestation de confidentialité sont disponibles sur l'intranet (https://intranet.cnesst.qc/employe/repondants/repondants-acces-aux-documents-et-protection-des-renseignements-personnels/). Le **répondant** devra s'assurer de sélectionner le modèle approprié et de compléter les informations manquantes (en jaune). Il devra ensuite transmettre l'attestation de confidentialité ainsi complétée en format PDF et s'assurer d'obtenir sa signature par le tiers. Dès la réception de l'attestation de confidentialité signée par le tiers, l'**intervenant** qui l'a reçu doit compléter la « Section réservée à la Commission ». Il devra ensuite la transmettre au **répondant**, lequel doit en fournir une copie à l'**unité dédiée** par le biais de la boîte courriel AR Accès (aracces@cnesst.gouv.qc.ca) ou au **substitut de la responsable** ayant été assigné afin de l'assister dans ce dossier, le cas échéant.

Dans tous les cas, si le **répondant** éprouve des difficultés à compléter les démarches ci-dessus décrites, il peut communiquer avec le substitut de la responsable de l'accès aux documents mandaté.

## 4. Rôle du substitut dans les incidents particuliers

Lorsqu'un **substitut de la responsable** est assigné à un dossier d'incident de confidentialité, il doit prendre connaissance de la situation à l'aide du formulaire de *Déclaration d'un incident de confidentialité* et des autres commentaires ou documents pouvant avoir été fournis. Il peut également requérir des renseignements supplémentaires au **répondant** et à tous autres **intervenants** afin de bien comprendre la situation.

### 4.1 Détermination des incidents de confidentialité majeurs

Après avoir analysé la situation, le **substitut de la responsable** doit déterminer si elle constitue un incident de confidentialité majeur. Un incident de confidentialité est majeur lorsque son impact peut notamment être qualifié par l'un (ou plusieurs) des éléments suivants :

- Augmente rapidement ;
- Touche une grande partie de la clientèle ;
- Entraîne un risque de médiatisation ;
- Conduit à une plainte (ou intention de plainte) auprès de la CNESST ou de toute autre instance gouvernementale ou légale;
- Demande l'intervention des forces de l'ordre ;
- Affecte d'autres ministères ou organismes (incidence à portée gouvernementale);
- Menace l'intégrité physique ou psychique d'une personne.

Dans ces situations, le **substitut de la responsable** doit aviser le **COMSI** en lui transmettant les renseignements pertinents relatifs à l'incident. Le **COMSI** assure alors la reddition de comptes relative à l'incident de confidentialité majeur, en informant :

- Le *Chef délégué de la sécurité de l'information* ;
- Le(s) d*étenteur(s) adjoint(s)* de l'information concernée ;
- La *Direction des communications et des relations publiques* à l'adresse suivante : relationsmedias@cnesst.gouv.qc.ca.

En plus des intervenants à informer en cas d'incident de confidentialité majeur, lorsque l'incident de confidentialité a une incidence à portée gouvernementale, le **COMSI** informe également :

- Le(s) *Détenteur(s)* de l'information concernée ;
- Le *Bureau de la présidente-directrice générale* ;
- Le *CERT/AQ*[2] et le *Chef gouvernemental de la sécurité de l'information*.

Le **substitut de la responsable** avise également le responsable en éthique afin d'évaluer l'opportunité d'informer les personnes concernées par l'incident.

Un incident de confidentialité devient à portée gouvernementale lorsque celui-ci produit un impact sur d'autres ministères ou organismes, ou qu'il implique des données leur appartenant.

[2] Computer Emergency Response Team / Administration Québécoise: Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise

Soulignons que la qualification d'incident majeur ou à portée gouvernementale est évolutive, de sorte qu'un incident qui ne l'était initialement pas peut le devenir en cours de traitement, et inversement.

Le niveau d'impact des préjudices potentiels ou avérés est déterminé selon différentes grilles prévues au processus de gestion des menaces, des vulnérabilités et des incidents (PGMVI).

S'il y a lieu, le **substitut de la responsable** avise le **COMSI** de la recommandation du **responsable en éthique** quant à l'opportunité d'informer les personnes concernées par l'incident avant d'y donner son approbation.

### 4.2 Détermination des incidents de confidentialité présentant un risque de préjudice sérieux

Après avoir analysé la situation, le **substitut de la responsable** doit déterminer si elle constitue un incident de confidentialité présentant un risque de préjudice sérieux au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.* Cette évaluation se fait notamment en considérant la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables tel que le vol d'identité.

Dans ces situations, le **substitut de la responsable** doit aviser :

- La Commission d'accès à l'information;
- La **responsable de l'accès**;
- La personne dont un renseignement est visé par un incident présentant un risque de préjudice sérieux, s'il y a lieu.

Le **substitut de la responsable** doit également aviser au besoin le **COMSI** en lui transmettant les renseignements pertinents relatifs à l'incident. Le **COMSI** assure alors la reddition de comptes relative à l'incident de confidentialité présentant un risque de préjudice sérieux auprès des autorités de la CNESST. Le **COMSI** informe également au besoin :

- Le *Chef délégué de la sécurité de l'information* ;
- Le(s) d*étenteur(s) adjoint(s)* de l'information concernée ;
- La *Direction des communications et des relations publiques* à l'adresse suivante : relationsmedias@cnesst.gouv.qc.ca.

Lorsque l'incident de confidentialité a une incidence à portée gouvernementale, le **COMSI** doit, en plus des intervenants précédemment énumérés, informer :

- Le(s) *Détenteur(s)* de l'information concernée ;
- Le *Bureau de la présidente-directrice générale* ;

- Le *CERT/AQ*[3] et le *Chef gouvernemental de la sécurité de l'information*.

Un incident de confidentialité devient à porter gouvernemental lorsque celui-ci produit un impact sur d'autres ministères ou organismes, ou qu'il implique des données leur appartenant.

Soulignons que la qualification d'incident présentant un risque de préjudice sérieux ou à portée gouvernementale est évolutive, de sorte qu'un incident qui ne l'était initialement pas peut le devenir en cours de traitement, et inversement.

Le niveau d'impact des préjudices potentiels ou avérés est déterminé selon différentes grilles prévues au PGMVI.

Dans le cas d'un tel incident, le **substitut de la responsable** doit aviser les personnes concernées par l'incident.

### 4.3 Rôle du substitut dans les démarches de résolution de l'incident

Le **substitut de la responsable** doit fournir les conseils juridiques pertinents au traitement de l'incident de confidentialité. Il doit travailler en collaboration avec le **répondant** afin d'identifier les démarches appropriées relativement à la résolution de l'incident et s'assurer qu'elles soient exécutées. Il peut également émettre des recommandations en vue d'empêcher la survenance de nouveaux incidents de confidentialité et d'améliorer la sécurité des renseignements détenus par la CNESST. Dans cette optique, un suivi doit être fait par le **substitut de la responsable** pour vérifier l'application et l'impact de ses recommandations, le cas échéant. Si des mesures correctives recommandées n'ont pas été implantées, le **substitut de la responsable** doit en informer le **COMSI**. Finalement, le **substitut de la responsable**, peut s'il le juge opportun, aviser le **responsable en éthique** qu'un incident de confidentialité s'est produit.

Lorsque le **substitut de la responsable** considère que des démarches de résolution de l'incident suffisantes ont été posées afin d'en minimiser les impacts et d'en empêcher la répétition, il avise le **répondant** de la fermeture du dossier. Il doit ensuite inscrire les renseignements pertinents relatifs à l'incident au *Registre des incidents de confidentialité*. Le dossier pourra également être fermé de la même façon après avoir communiqué avec le **COMSI** si des mesures correctives recommandées n'ont pas été implantées.

## 5. Procédure particulière pour l'unité dédiée

Dans la situation où un incident de confidentialité impliquant directement un membre de l'unité dédiée serait dénoncé, l'incident devra, exceptionnellement, être signalé à la **responsable de l'accès** par le biais de l'adresse courriel RAIPRP@cnesst.gouv.qc.ca.

[3] Voir note 2

Afin d'éviter toute apparence de conflit d'intérêts dans le traitement d'un tel incident, un avocat ne faisant pas partie de la DAJ SST Est et Accès à l'information sera désigné pour exercer les rôles normalement attribués à l'**unité dédiée** et au **substitut de la responsable** en vertu de la présente procédure. Le traitement de l'incident devra être fait en respect de la présente procédure, compte tenu des adaptations nécessaires.

## 6. Reddition de comptes relative aux incidents de confidentialité

La **responsable de l'accès** doit faire une reddition de comptes à la *Présidente-directrice générale* et à la *Directrice générale des affaires juridiques* toutes les années. Pour ce faire, une copie du *Registre des incidents de confidentialité* de l'année précédente doit leur être transmise au plus tard le 1er avril de chaque année.

Si des mesures de suivis devaient être prises de façon plus spécifique au cours de l'année, la **responsable de l'accès** peut avec les intervenants concernés mettre en place des mesures permettant de limiter les incidents de confidentialités.

## 7. Mise à jour de la présente procédure

La présente procédure doit être mise à jour lorsqu'une modification du droit applicable, qu'elle soit législative, règlementaire ou jurisprudentielle, a un impact relativement à la validité ou l'efficacité de la présente procédure. Il en est de même, si un délai de cinq ans s'est écoulé depuis sa dernière révision.

De la même façon, la présente procédure doit être mise à jour lorsqu'une modification administrative des mesures de sécurité devant être appliquées a un impact relativement à la validité ou l'efficacité de la présente procédure.

Dans ces situations, la mise à jour de la procédure doit être faite dans les six mois suivants, selon le cas, la modification du droit applicable ou l'échéance du délai de cinq ans.

La présente procédure peut également être modifiée par la **responsable de l'accès** à tout moment, si cette dernière le juge opportun.

La **responsable de l'accès** devant assurer la mise en application de la présente procédure, il lui appartient de s'assurer de la maintenir à jour. Par ailleurs, aucune modification ne peut être effectuée à la présente procédure sans avoir été préalablement approuvée par la **responsable de l'accès**.

## ANNEXE 1 : QUELQUES EXEMPLES D'INCIDENTS DE CONFIDENTIALITÉ

**Voici quelques exemples de situations constituant des incidents de confidentialité :**

- À la suite d'une erreur dans l'identification de l'employeur dans un dossier, une décision d'admissibilité devant être transmise à l'employeur est plutôt communiquée à un autre employeur au nom similaire ;
- Une copie de dossier est transmise à une travailleuse. Or, on réalise qu'à la suite d'une erreur humaine, un rapport médical concernant un autre travailleur avait été classé dans le dossier ;
- Un intervenant souhaite communiquer avec une salariée ayant récemment déposé une plainte en matière de harcèlement psychologique à l'encontre de son employeur. Lorsqu'il appelle au numéro de téléphone au dossier, la mère de la salariée décroche. L'intervenant discute donc du dossier avec celle-ci ;
- Une intervenante, aux prises avec un dossier particulièrement complexe, décide d'en faire une copie et l'amener à son domicile afin de pouvoir y travailler en soirée. Au retour du bureau, elle va acheter un café en prévision de sa longue soirée et elle laisse cette copie sur la banquette arrière de sa voiture. En sortant du café, elle réalise que sa voiture a été vandalisée et que son contenu a été volé ;
- Suivant une enquête en matière d'équité salariale, un préavis de décision est transmis à l'employeur visé par une plainte, un document identifiant les salariés ayant déposé les plaintes est joint au préavis. Les travailleurs n'ayant pas consenti à la levée de la confidentialité ont vent de cette transmission.
- Une note de consultation est transmise à la CNESST par le médecin traitant d'un travailleur s'étant cassé un bras au travail. La note est déposée au dossier du travailleur, lequel fait éventuellement l'objet d'une contestation au Tribunal administratif du travail. Lorsque des copies du dossier sont transmises à l'ensemble des parties, le travailleur réalise que cette note fait non seulement état de sa blessure au bras, mais également de ses problèmes de diabète, lesquels n'ont aucun lien avec son accident de travail ;
- Une décision d'admissibilité est transmise à un travailleur à l'adresse indiquée au dossier. Quelques jours plus tard, un tiers téléphone à la CNESST pour aviser qu'il a reçu la décision d'admissibilité à son domicile. On réalise alors que le travailleur a récemment déménagé et n'a pas avisé la CNESST de son changement d'adresse.

**Quelques autres exemples :**

- Vol ou perte de documents ou d'une tablette, d'un téléphone intelligent, d'un micro-ordinateur portable ou de toute unité de stockage (clé USB, disque dur, etc.) ;
- Dossiers de travailleurs se retrouvant dans les poubelles, dans des lieux publics à la suite d'une opération récupération-recyclage exécutée par un tiers ;
- Renseignements confidentiels se retrouvant sur le site Internet d'un tiers ;
- Accès non autorisé à des renseignements confidentiels par un employé de la CNESST ;
- Vente de renseignements personnels par un employé de la CNESST ou communication à un de ses proches ;
- Diffusion d'informations concernant le dossier d'un travailleur ou d'un employeur par un journaliste.