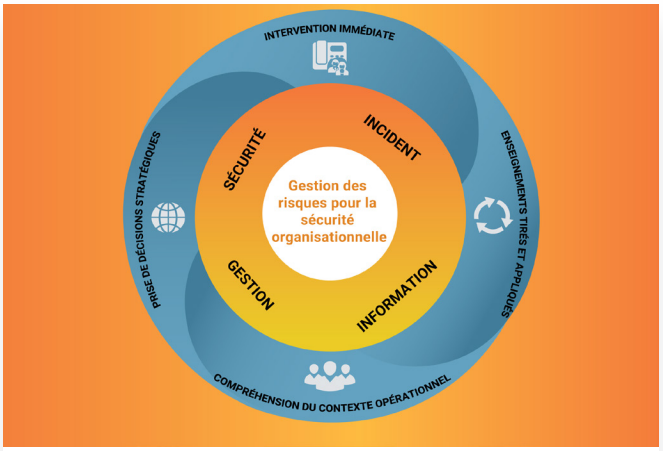
Gestion des incidents de sécurité

PRÊT à l'emploi Guide Mobile

Apprenez comment les organisations peuvent efficacement gérer les informations relatives aux incidents de sûreté et de sécurité.



Qu'est-ce que la gestion des informations relatives aux incidents de sûreté et de sécurité ?

Pourquoi est-il indispensable pour les organisations de gérer l'information sur les incidents ?

Il existe plusieurs raisons pour lesquelles il est indispensable que les organisations gèrent les informations relatives aux incidents de sécurité et de sûreté.

- Réduire l'impact d'un incident sur l'organisation et sur ses employés.
- Améliorer la capacité d'une organisation à prévenir de futurs incidents.
- Améliorer la capacité d'une organisation à se préparer à futurs incidents et à atténuer leur impact.
- Permettre à une organisation de s'acquitter de son devoir de diligence et de protection à l'égard de ses employés et des autres en renforçant leur sûreté et leur sécurité.
- Soutenir une bonne prise de décision en matière de programme, de sûreté et de sécurité, de ressources humaines, de finances et de plaidoyer.
- Fournir des renseignements utiles qui facilitent l'accès d'une organisation aux populations dans le besoin.

Qu’est-ce qu’un incident ?

L’organisation doit définir clairement ce qu’est un incident avant de pouvoir gérer de façon constructive les informations qui s’y rapportent.

Définition

Le terme « incident » désigne un ou plusieurs évènements au cours desquels :

- la sûreté ou la sécurité des employés est compromise ;
- une personne dépendante ou un tiers est blessé ou lésé au cours des activités de l’organisation ;
- des biens ou des actifs de l’organisation sont volés, endommagés ou mis en danger ;
- il y a perturbation de la programmation et des opérations ;
- l’indépendance de l’action de l’organisation est compromise ;
- la réputation de l’organisation est menacée ou entachée.

Interne vs externe

Un incident peut toucher directement une organisation et ses employés, ou une personne qui ne fait pas partie de l’organisation.

Gravité

Les incidents peuvent être critiques et non-critiques :

- Un **incident critique** exige qu’une organisation réponde en utilisant divers moyens et mesures supplémentaires qui vont au-delà de ses procédures courantes (par exemple : enlèvement, décès).
- Un **incident non critique** est celui qu’il est possible de traiter en suivant les procédures courantes de l’organisation (par exemple : accident de voiture sans blessure ni dommage grave).

La gravité d’un incident est souvent mesurée par le niveau de l’impact qu’il a sur l’organisation.

Impact

Un incident peut avoir un impact sur :

- la sécurité et le bien-être des employés ;
- la capacité d'une organisation à :
  - mener ses opérations
  - fournir de l'aide et des services
  - atteindre ses objectifs

Accident ou acte intentionnel

Un incident peut être un accident ou un acte intentionnel :

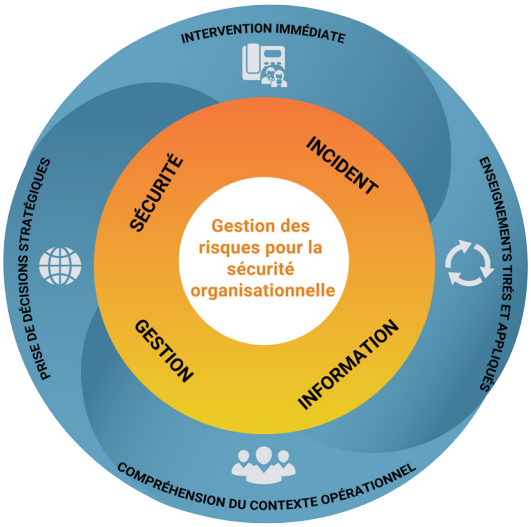
- **Incident touchant à la sûreté** = accident
- **Incident touchant à la sécurité** = évènement intentionnellement causé par un tiers afin de nuire à une organisation ou à un autre intervenant, ou de porter atteinte à des activités d'aide prévues. Les actes intentionnels qui, sans viser directement l'organisation, l'ont néanmoins affectée, elle ou ses employés, relèvent également des incidents de sécurité.

Classification

Les organisations doivent utiliser un système rigoureux de classification qui définisse clairement les différents types d'incidents.

Qu’est-ce que la gestion de l’information relative aux incidents de sécurité ?

La gestion des informations relatives aux incidents de sûreté et de sécurité (SIIM en anglais) correspond au processus de collecte et d’utilisation de ce type d’information. Elle vise principalement à accroitre la sûreté, la sécurité et la capacité générale d’une organisation à accéder aux communautés et à leur fournir de l’aide. Le moyen d’y parvenir est de veiller à ce que toute information utile résultant des incidents soit mise à profit pour éclairer la prise de décision à tous les niveaux organisationnels. Toutes les activités liées à la SIIM doivent privilégier la dimension humaine et respecter la diversité et les différents besoins des personnes touchées par les incidents.



Intervention immédiate

Signaler un incident afin de rapidement réagir et aider les individus affectés.

Enseignements tirés et appliqués

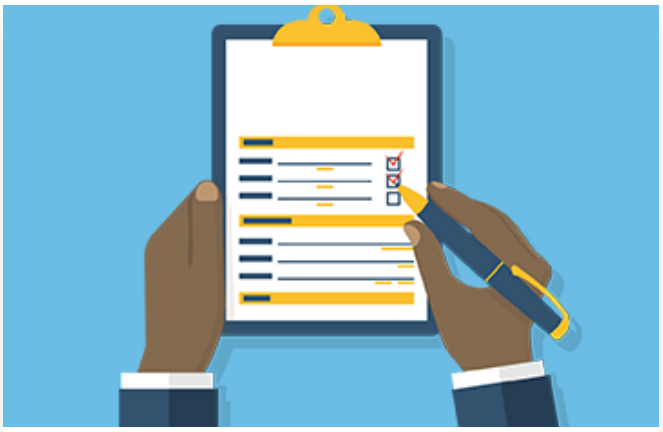
Après un incident, exploiter les informations recueillies de sorte à en tirer des enseignements qui permettront aux organisations de mieux **prévenir** les incidents futurs et de mieux **s’y préparer**.

Compréhension du contexte opérationnel

Afin d’éclairer la prise des décisions opérationnelles, il convient de dégager les tendances et mieux comprendre le contexte en exploitant les données internes et externes des incidents.

Prise de décisions stratégiques

Exploiter les données d’incidents de sorte à éclairer la prise de décisions utiles concernant les activités organisationnelles touchant à la sécurité et la sûreté, aux programmes, aux finances, aux ressources humaines et au plaidoyer.



Gestion des informations relatives aux incidents

Gestion des informations relatives aux incidents

La gestion des informations relatives aux incidents de sûreté et de sécurité implique un cycle d'apprentissage continu. La réponse et l'analyse d'un incident doivent informer la réponse et l'analyse des incidents futurs. Or, pour gérer les informations relatives aux incidents, les organisations et les employés doivent se conformer à certaines étapes clés. L'ordre de ces étapes et la personne responsable de chaque activité peuvent varier selon la situation et l'organisation. Pour cela, il est essentiel que chaque organisation fournisse à tous ses employés des directives et des procédures claires et précises à suivre lors de la gestion des informations relatives aux incidents de sûreté et de sécurité.

Étape 1 : Signalement de l'incident et intervention immédiate

Signaler l'incident

Il faut que les organisations aient un cadre en place leur permettant de :

- signaler immédiatement les incidents graves en suivant les procédures de signalement de l'organisation (par téléphone ou radio) ;
- transmettre les renseignements essentiels pour la réponse immédiate, notamment :
  - ✓ qui est impliqué
  - ✓ ce qui s'est passé
  - ✓ où l'incident s'est produit
  - ✓ quand l'incident s'est produit
  - ✓ quelles mesures ont déjà été prises
  - ✓ quelle aide est nécessaire
- fournir des mises à jour pour les incidents en cours, au besoin.

Conseils pour le compte-rendu immédiat

- Se limiter aux faits. Éviter de porter un jugement ou de se focaliser sur les raisons qui ont conduit à l'incident.
- Garder confidentielles les informations relatives à l'incident.
- Suivre des mécanismes de signalement spécifiques aux cas sensibles tels que les agressions sexuelles (le cas échéant).

Réagir à l'incident

Les organisations ayant reçu un rapport initial d'incident doivent :

- faire en sorte que les personnes touchées par l'incident reçoivent l'aide et le soutien nécessaires ;
- s'assurer que le délai d'intervention correspond à la gravité et à l'impact de l'incident ;
- prioriser l'assistance aux personnes touchées, et protéger ces personnes et d'autres contre de nouveaux préjudices ;
- prendre en compte toute particularité personnelle (ethnicité, statut personnel, identité de genre) pouvant nécessiter une démarche personnalisée en matière de réponse.

Remplir un compte-rendu officiel d'incident

Après avoir apporté la réponse initiale à un incident, les organisations doivent faire le nécessaire pour qu'un compte-rendu officiel de l'incident soit rempli et enregistré dans un système prévu à cet effet.

Il est possible que le compte-rendu nécessite la collecte d'informations supplémentaires sur l'incident.

Les organisations devraient appliquer les procédures de rapport suivantes :

- utiliser un système simple de compte-rendu d'incident pour consigner les informations connexes ;
- fournir au personnel des modèles faciles à utiliser, et le former de manière à prévenir le manque de précision dans les comptes-rendus ;
- former le personnel sur la façon de consigner les incidents directement dans le système ou affecter un membre du personnel à la saisie des comptes-rendus dans le système ;
- expliquer clairement au personnel ce qui se passe avec les informations relatives à l'incident à la suite d'un compte-rendu ;
- assurer la confidentialité afin de protéger les personnes touchées par l'incident.

Conseils pour les comptes-rendus officiels d'incidents

- Se conformer aux procédures de l'organisation.
- En fonction de la gravité de l'incident, envisager de ne pas discipliner le personnel s'il reconnait avoir enfreint les règles de l'organisation.
- Inclure les informations personnelles (origine ethnique, statut, identité de genre) de sorte que la réponse à l'incident et l'analyse de ce dernier puissent tenir compte de la diversité du personnel. Ne recueillir ces informations que si l'organisation peut assurer leur confidentialité et garantir que les employés concernés ne risquent pas de subir d'autres dommages.
- Ne partager les comptes-rendus qu'avec les collègues appropriés, et ce dans le respect des règles de confidentialité.

Étape 2 : Analyse de l'incident et enseignements tirés

Assurer le suivi

Les organisations doivent assurer le suivi d'un compte-rendu d'incident.

Le personnel responsable devrait :

- obtenir toute information supplémentaire qui, tout en étant requise pour l'analyse, ne figure pas dans le compte-rendu initial de l'incident ;
- effectuer un debriefing avec la ou les personnes touchées par l'incident pour tirer des enseignements de ce qui s'est produit ;
- trouver un juste équilibre entre le fait de récompenser le personnel pour avoir signalé les défaillances et l'application des procédures disciplinaires ;
- tenir compte des besoins individuels des membres du personnel impliqués dans ce debriefing et s'assurer que le processus soit adapté à leurs besoins, notamment les contraintes linguistiques ou d'accès aux services de soutien psychologique ou médical.

Conseils pour le debriefing

- Se limiter aux faits.
- Utiliser le debriefing pour tirer des enseignements de l'incident qui soient applicables à l'ensemble de l'organisation.
- Ne pas laisser un debriefing factuel dégénérer en debriefing émotionnel.
- Éviter de critiquer les personnes impliquées dans l'incident.

Analyser l'incident

Le membre compétent du personnel analyse les informations recueillies dans le compte-rendu officiel de l'incident pour déterminer les causes de celui-ci. Il est essentiel de comprendre les causes de l'incident, qu'il s'agisse d'une attaque par des tiers ou du non-respect des procédures par un employé, pour prévenir des incidents futurs et s'y préparer.

Dans leur analyse d'un incident, les organisations doivent :

- prendre en compte les conséquences et les causes de l'incident ;
- déterminer si des incidents similaires se sont déjà produits ;
- vérifier si les procédures organisationnelles ont été suivies ;
- analyser l'efficacité de l'intervention de gestion de l'incident ;
- prendre en considération toute caractéristique personnelle des personnes impliquées dans l'incident (genre, religion, origine ethnique) qui pourrait être un facteur ou un motif de l'incident.

Mettre à profit les enseignements tirés

Après l'analyse de l'incident, les responsables et les décideurs de l'organisation doivent :

- définir et mettre en œuvre des mesures nouvelles ou améliorées pour prévenir des incidents similaires ou s'y préparer ;
- demander l'élaboration d'un plan d'action visant à faire en sorte que les mesures recommandées soient mises en œuvre.

Étape 3 : Analyse du contexte, des caractéristiques et des tendances

Enregistrer les incidents

Les organisations doivent enregistrer les incidents dans une base de données réservée à cet effet. Lorsque les membres du personnel sont appelés à déposer eux-mêmes leurs comptes-rendus d'incidents directement dans la base de données, les organisations devraient fournir des directives claires ainsi qu'une formation visant à garantir la cohérence des comptes-rendus.

Une base de données sur les incidents :

- est un système logiciel ou un document tableur genre Excel spécialement mis en place pour la gestion des informations relatives aux incidents de sûreté et de sécurité ;
- utilise une technologie qui correspond à la taille et aux besoins de l'organisation ;
- préserve la confidentialité des informations enregistrées afin de protéger la vie privée des personnes concernées ;
- dispose de clés d'accès définissant qui peut consulter l'information et à quelles fins ;
- suit des procédures cohérentes pour l'établissement des comptes-rendus ;
- permet l'analyse d'incidents multiples.

Accéder à des informations externes sur les incidents

Les organisations ont intérêt à comparer leurs tendances en matière d'incidents à celles d'organisations similaires. Les informations externes sur les incidents peuvent servir à enrichir l'analyse. Elles peuvent être obtenues soit à partir de sources ouvertes, soit par le biais d'abonnements auprès de fournisseurs commerciaux ou d'accords de partage de données sur les incidents.

Lors de l'analyse d'information externe sur un incident, les organisations doivent :

- faire entrer en ligne de compte la **fiabilité de la source** (cette source est-elle réputée pour son authenticité, sa fiabilité et sa compétence ?) ;
- examiner la **validité de l'information** (cette information concorde-t-elle avec d'autres données pertinentes et est-elle confirmée par des sources indépendantes ?).

Communiquer aux acteurs extérieurs des informations relatives aux incidents

En acceptant de communiquer à d'autres organisations leurs données sur les tendances clés, les organisations peuvent obtenir des informations supplémentaires à partir des données d'incidents externes. Les données anonymisées sont diffusées directement sur des forums ou via des bases de données communes. Notons toutefois que les différences entre les catégories d'incidents peuvent compliquer la mise en commun des données et l'analyse de celles-ci.

Exemples de ressources externes pour la communication des données d'incidents :

- le projet Aid in Danger, de Insecurity Insight ;
- la base de données sur la sécurité des travailleurs humanitaires AWSD ;
- International NGO Safety Organisation (INSO) ;
- le cadre « Sauver des vies ensemble ».

Analyser les données d'incidents multiples

L'analyse de multiples incidents internes et externes peut aider les organisations à mieux comprendre le contexte opérationnel en dégageant des caractéristiques et des tendances, ainsi que des variations subtiles de l'environnement opérationnel qui risqueraient autrement de passer inaperçues. L'analyse du contexte peut faciliter l'accès et la mise en œuvre d'une stratégie d'acceptation.

L'analyse de données d'incidents multiples :

- est une approche structurée destinée à analyser des incidents multiples (internes et externes) ;
- compare les données de tendances propres à une organisation avec des données externes sur les incidents de sécurité et de sécurité (provenant de sources publiques ou communiquées par d'autres organisations) ;
- compare les incidents d'une organisation avec les données d'organisations similaires ;
- tient compte de la façon dont le manque de précision dans les comptes-rendus peut affecter les données.

Étape 4 : Prise de décisions éclairées et élaboration de politique en toute connaissance de cause

Communiquer en interne les informations sur les incidents

Le partage et l'utilisation en interne des données d'incidents par les différents services et équipes apportent aux organisations des informations précieuses. Les organisations qui mettent en commun leurs données sont censées rendre celles-ci **anonymes** en supprimant toute information permettant d'identifier une personne, et ce afin de préserver **la confidentialité** et de protéger la vie privée des personnes touchées par les incidents. Les données relatives aux incidents permettent d'éclairer les décisions des divers services de l'organisation, notamment les programmes, les finances, les ressources humaines et le plaidoyer.

Les données relatives aux incidents peuvent être utilisées pour :

- l'analyse de contexte ;
- la mise au point de plans d'action ;
- l'accès et la planification des programmes ;
- les propositions de financement ;
- l'évaluation des risques ;
- les descriptions de postes relevant de domaines spécifiques.

Éclairer la prise des décisions opérationnelles

Une collecte et une analyse rigoureuses des données relatives aux incidents permettent aux responsables de prendre des décisions opérationnelles sur le terrain, ainsi qu'aux niveaux national, régional et international. Ces décisions peuvent porter sur :

- le lieu et la nature de l'intervention, y compris la façon de négocier l'accès
- les mesures à mettre en œuvre et celles à prioriser pour la gestion des risques de sécurité ;
- les activités et les ressources qui doivent être financées.

Conseils sur la façon de mettre l'analyse de l'information au service de la prise de décision opérationnelle

- Analyser l'impact réel ou potentiel des informations relatives à l'incident.
- Déterminer les services ou les collègues qui pourraient être touchés par ces informations ou en bénéficier.
- Définir le mécanisme et les modèles de communication de l'information entre plusieurs services afin de protéger la vie privée des personnes touchées.
- Transmettre les données d'incident anonymisées avec des recommandations de suivi aux différents services.

Informer la politique de l'organisation

Une collecte et une analyse rigoureuses des données relatives aux incidents permettent aux responsables de prendre des décisions stratégiques et de politiques organisationnelles. Ces décisions peuvent porter sur :

- le choix des pays où il convient d'intervenir ;
- les stratégies de sécurité à privilégier (acceptation, protection, ou dissuasion) ;
- les moyens de communication à utiliser pour informer les bénéficiaires, les donateurs, le public et les autres parties prenantes sur les programmes ;
- le moment d'utiliser les informations liées aux incidents à des fins de plaidoyer.

Les données relatives aux incidents peuvent constituer des preuves de :

- violence contre les travailleurs humanitaires ;
- perturbation de l'action humanitaire ;
- de restrictions à l'accès humanitaire ;
- de violence à l'encontre des populations locales ou difficultés rencontrées par celles-ci.

Ces informations peuvent donner lieu à des politiques liées à :

- l'amélioration de l'accès humanitaire ;
- la protection des travailleurs humanitaires ;
- le respect du droit international humanitaire ;
- la sensibilisation des donateurs, des parties prenantes et des autres acteurs aux contraintes opérationnelles et aux questions de sécurité ;
- la recherche de la justice pour les victimes de violations du droit pénal, humanitaire ou des droits de l'Homme.

Il ne faut en aucun cas faire mention d'individus ou de cas particuliers pour faire valoir une position politique. Les données collectives réduisent ce risque grâce à l'anonymat que confère la multiplicité.

Informer le personnel sur les décisions prises

Les hauts responsables doivent communiquer au personnel comment l'organisation a tiré des enseignements des incidents et pris des décisions à la lumière des informations recueillies. Cela peut contribuer à lutter contre le manque de précision dans les comptes-rendus d'incidents.

Cette démarche permettra aux membres du personnel de :

- mieux comprendre la gestion des informations relatives aux incidents ;
- faire davantage confiance au processus de signalement des incidents ;
- appliquer les enseignements tirés des incidents.

Classification des incidents

Classification des incidents

Les organisations utilisent des catégories pour décrire les différents types d'incidents qui peuvent arriver à l'organisation, ses employés, les communautés avec lesquelles elle travaille, et à tout autre tiers. Les organisations sont encouragées à utiliser des définitions normalisées pour faciliter l'analyse, l'échange de données et les comparaisons entre les organisations. Vous trouverez plus bas une liste de définitions proposées. Les organisations ne sont pas obligées d'utiliser toutes les catégories ; elles devraient choisir celles qui sont les plus appropriées au contexte dans lequel elles travaillent.

Accident ou maladie

Tout accident affectant des employés ou des biens de l'organisation et tout autre incident non intentionnel (accidents, maladie soudaine).

Décès accidentel

Tout décès causé involontairement et qui ne peut être attribué à des causes naturelles. Les causes de décès accidentel peuvent inclure des accidents de véhicule ou des complications résultant de blessures.

Maladie

Toute maladie grave d'un employé.

Mort naturelle

Tout décès qui peut être attribué à une cause naturelle (crise cardiaque, maladie, accident vasculaire cérébral).

Incendie de cause naturelle

Tout incendie, de cause naturelle ou involontaire, qui endommage la propriété ou met en danger les employés. Il peut s'agir de feux de forêts ou d'incendies accidentels (feux électriques, fuites de gaz).

Suicide

Le décès volontaire et intentionnel d'un employé qui s'est donné la mort.

Autre accident

Un évènement fortuit dans lequel des employés sont blessés ou des biens de l'organisation sont endommagés.

Activités d'aide

Tout incident qui a eu lieu sur un site de projet ou pendant la distribution de l'aide, y compris le pillage des biens destinés aux distributions, l'intimidation, le harcèlement ou le comportement menaçant envers les membres du personnel. Ces incidents comprennent les évènements qui se produisent dans le contexte d'un conflit, d'une guerre ou d'un crime.

Activité armée

Activités impliquant des armes menées par un État, un non-État ou des entités armées organisées.

Visant les bénéficiaires

Des menaces ou des actes de violence ont été utilisés à l'encontre d'un bénéficiaire.

Harcèlement direct

Incidents dans lesquels un employé est directement harcelé par une personne ou un groupe de personnes (exemple : harcèlement concernant les activités ou les programmes de l'organisation).

Intimidation directe

Incidents dans lesquels un employé est directement intimidé par une personne ou un groupe de personnes (exemple : employé qui se sent intimidé par des acteurs armés patrouillant près d'une distribution alimentaire).

Menaces directes

Incidents dans lesquels un employé est directement menacé par une personne ou un groupe de personnes. Ce type d'incident se caractérise par une forme de conséquence associée au non-respect des règles (exemple : menace de représailles pour ne pas avoir inclus une certaine personne dans une activité de l'organisation).

Pillage

Vol pendant des troubles, des violences, des émeutes ou d'autres soulèvements.

Crime

Incidents à motivation criminelle qui touchent les employés, leurs biens ou les biens de l'organisation.

Vol à main armée

Vol sous la menace d'une arme ou dont les auteurs armés ont fait des victimes parmi les employés ou endommagé des biens.

Incendie criminel

Tout incendie qui, causé volontairement, a endommagé des biens ou mis en danger des employés. L'incendie criminel comprend, sans s'y limiter, le recours à des dispositifs incendiaires, le sabotage intentionnel de systèmes électriques ou de conduites/réservoirs de gaz, ainsi que l'utilisation d'un agent accélérateur en vue de réduire les biens à néant.

Chantage

Menaces, extorsion ou manipulation d'un individu pour le contraindre à un certain acte ; il peut s'agir de l'obtention d'une chose, en particulier de l'argent, par la force ou les menaces.

Effraction

L'introduction illégale dans les locaux ou les véhicules d'une organisation humanitaire dans l'intention de commettre un vol.

Cambriolage

L'introduction illégale dans une résidence du personnel, généralement dans l'intention de commettre un vol.

Classification du cambriolage par rapport au vol qualifié :

- **cambriolage** = lorsque les occupants ne sont pas présents ou ne sont pas au courant de l'incident (pendant leur sommeil) ;
- **vol qualifié/vol à main armée** = lorsque les occupants sont présents ou directement menacés pendant l'incident.

Vol de véhicule/Détournement

Tout incident dans lequel un véhicule appartenant à l'organisation ou utilisé par un employé, que celui-ci en soit le conducteur ou un passager, est saisi de force.

Cyber-attaque

Exploitation délibérée de systèmes informatiques ou d'entreprises et de réseaux dépendant de la technologie, dont les conséquences perturbatrices peuvent compromettre les données et donner lieu à des cyber-crimes.

Extorsion

Pratique consistant à obtenir quelque chose, notamment de l'argent, d'un employé par la force ou les menaces.

Fraude

Tromperie illicite ou criminelle destinée à entrainer un gain financier ou personnel.

Intrusion

Entrée illicite ou non autorisée dans les locaux, les véhicules ou les résidences du personnel d'une organisation par des criminels ou des civils (mais pas par les autorités de l'État).

Piraterie

Attaque et vol de navires en mer ou de bateaux sur les rivières.

Vol qualifié

IIncidents dans lesquels :

- l'auteur n'est pas armé ;
- l'employé ou les employés affectés étaient présents lors de l'incident et étaient pleinement conscients d'être volés et du fait que des biens ont été pris.

Dommage matériel

Tout dommage ou dégât dépassant un montant prédéfini, qui est causé à des biens de l'organisation soit involontairement (catastrophes naturelles, accidents) ou intentionnellement (émeutes qui causent des dommages matériels).

Vol de biens

Toute situation dans laquelle des biens personnels sont volés à un employé ou d'un lieu sans que la victime en soit consciente.

Vol des biens de l'organisation

Toute situation dans laquelle des biens sont volés à une organisation sans qu'un employé n'observe l'acte.

Vandalisme

Destruction/dommages délibérés aux biens de l'organisation ou du personnel.

Conflit et guerre

Incidents qui se produisent dans le contexte de conflits armés ou de situations de volatilité politique grave et qui ont des répercussions directes ou indirectes sur une organisation, son personnel ou ses opérations locales et internationales, à titre privé ou professionnel. Les incidents peuvent ou non affecter directement l'organisation, son personnel ou son infrastructure.

Activité armée

Activités impliquant des armes menées par un État, un non-État ou des entités armées organisées.

Échange de tirs

Toute situation dans laquelle un ou plusieurs employés ou des biens de l'organisation sont pris dans une attaque ou une fusillade entre deux ou plusieurs parties armées. Dans cette situation, les employés et les biens concernés ne sont pas la cible de l'attaque.

Coup d'État

Coup d'État, mutinerie et autres rébellions par une force armée. Un coup d'État est défini comme une tentative (généralement armée) de supprimer et de remplacer un gouvernement. Qu'elle soit réussie ou non, violente ou non, une tentative de coup d'État peut être politiquement déstabilisante.

Fusillade

Tir ciblant des personnes autres que le personnel de l'organisation.

Découverte de munition non explosée

Fait référence à la découverte d'un engin non explosé. Il s'agit de restes explosifs de guerre qui n'ont pas explosé lors de leur déploiement et qui présentent toujours un risque de détonation.

Meurtre/Blessures/Enlèvement

Tout incident entrainant la mort, la blessure ou l'enlèvement d'un employé. Ces incidents sont généralement classés comme des incidents critiques.

Rapt/Détournement/Prise d'otage/Enlèvement

Tout incident au cours duquel des employés sont saisis par la force. Cet incident peut impliquer ou non une demande de rançon. Les employés tués en captivité sont inclus dans la catégorie « kidnappé » et non « tué ».

Coups

Incident au cours duquel un employé est agressé par une personne utilisant ses poings, ses pieds ou d'autres parties du corps, ou des objets (bâtons ou objets tranchants).

Meurtre

Tout décès causé intentionnellement (fusillade, attaque physique, empoisonnement). Les décès intentionnels ne comprennent pas les suicides. Les employés tués en captivité sont inclus dans la catégorie « kidnappé » et non « tué ».

Disparition

Un incident au cours duquel un employé a disparu ou a été porté disparu.

La distinction entre disparition et enlèvement est la suivante :

- **le perpétuateur —** les acteurs non étatiques ont tendance à kidnapper tandis que les acteurs étatiques ont tendance à faire « disparaître » des gens, lesquels seront alors appelés « disparus » ;
- **la façon dont l'auteur du crime communique au sujet de l'employé qui a été saisi —** les kidnappeurs ont tendance à exiger une rançon, tandis que pour les personnes disparues ou portées disparues, on n'entend plus jamais parler d'elles ;
- **le motif —** généralement, une personne est enlevée pour une demande précise, tandis que les disparitions visent à faire taire un membre du personnel, souvent pour des raisons politiques.

Torture

Mutilation/blessure physique intentionnelle qui est explicitement caractérisée par la torture du personnel.

Blessures

Un incident au cours duquel un employé a été blessé avec une arme plutôt que d'être battu.

Privation de liberté

Détails et résultat de toute action qui prive les individus de leur liberté (enlèvement, prise d'otage, rapt, arrestation ou détention).

Évasion

La victime s'est échappée ou a tenté de s'échapper, ce qui a pu entrainer sa mort ou sa libération.

Libération

L'incident a été résolu par la libération de la victime.

Mort

La victime a été tuée en captivité, lors d'une mission de sauvetage ou au cours d'une tentative d'évasion.

En captivité

La victime est toujours en captivité.

Disparition

La victime est portée disparue.

Mission de sauvetage

Une mission de sauvetage tentée ou exécutée qui peut avoir entrainé la mort ou la libération.

Aucune information

Il n'y a pas d'autres informations sur ce qui est arrivé à la victime.

Espace opérationnel

Des actions directes ou indirectes, ou des menaces, prises par un État ou un acteur non étatique qui affectent l'accès humanitaire.

Abus de pouvoir

L'utilisation, par des fonctionnaires, de pouvoirs conférés par la loi, par un organe exécutif pour réaliser des gains privés illégitimes. Un acte illégal commis par un titulaire de fonction ne constitue un abus de pouvoir que si cet acte est directement lié à ses fonctions officielles.

Refus de l'accès

Des actes qui :

- empêchent une organisation d'atteindre des bénéficiaires, ou des bénéficiaires potentiels, pour l'évaluation des besoins ou la prestation directe de services ;
- empêchent les bénéficiaires d'accéder aux services d'une organisation.

Accusations

Une accusation d'actes répréhensibles par les autorités du pays d'accueil.

Application des lois

Application de lois, décrets, arrêtés ou règlements existants ou nouveaux qui, lorsqu'ils sont appliqués, ont un effet réel sur la mise en œuvre de l'aide. Cela peut inclure la confiscation d'équipements ou de l'inscription de personnes ou d'organisations sur des listes de surveillance.

Arrestation

Arrestations d'employés. Pour distinguer cet incident d'une prise d'otages, il faut que la partie qui procède à l'arrestation soit investie d'une fonction publique (comme la police). Les arrestations suivent généralement des accusations formelles.

Attaque contre une autre organisation

Attaque signalée contre une autre organisation, mais n'affectant pas directement l'organisation

Poursuites judiciaires

Une procédure judiciaire en bonne et due forme engagée par une autorité publique affirmant qu'un employé ou l'organisation a commis un crime.

Poste de contrôle

Un poste de contrôle non frontalier ou frontalier, érigé dans des zones qui sont sous contrôle militaire, paramilitaire ou d'un groupe armé pour surveiller ou contrôler le mouvement des personnes et des matériaux, et ayant un impact sur l'action humanitaire.

Refus de visa

Retard ou refus d'un timbre officiel, d'un visa ou d'un autre permis autorisant l'entrée requise dans un pays, ou dans un territoire à l'intérieur d'un pays, pour l'acheminement de l'aide.

Détention

Garder un employé en détention avant qu'il ne soit accusé ou inculpé officiellement ; cela inclut la détention temporaire pendant des heures ou des jours.

Expulsion

Consiste à forcer un employé ou une organisation à quitter un pays ou un territoire.

Harcèlement direct

Incidents dans lesquels un employé est directement harcelé par une personne ou un groupe de personnes (exemple : harcèlement concernant les activités ou les programmes de l'organisation).

Intimidation directe

Incidents dans lesquels un employé est directement intimidé par une personne ou un groupe de personnes (membre du personnel qui se sent intimidé par des acteurs armés patrouillant près d'une distribution alimentaire).

Menaces directes

Incidents dans lesquels un employé est directement menacé par une personne ou un groupe de personnes ; ce type d'incident se caractérise par une forme de conséquence associée au non-respect des règles (menace de représailles pour ne pas avoir inclus une certaine personne dans une activité de l'organisation).

Amende

Argent qui doit être payé par l'organisation en guise de punition pour ne pas avoir obéi à une règle ou à une loi.

Fermeture forcée

Ordre du gouvernement ou d'autres autorités d'interrompre les opérations dans un pays ou un territoire ; il peut s'agir de la fermeture d'un seul ou de plusieurs programmes.

Intervention des pouvoirs publics

Action prise par le gouvernement hôte ou le gouvernement donateur, et ayant un impact direct ou indirect sur la capacité financière d'un organisme à fournir de l'aide ; il peut s'agir, entre autres, de gel des fonds, de l'introduction de taxes ou de la fin des subventions.

Emprisonnement

Détention d'un employé dans un lieu connu, officiel ou inconnu, comme une prison, souvent à la suite d'accusations formelles.

Introduction de lois

Rédaction ou vote de lois, décrets, arrêtés ou règlements qui, lorsqu'ils sont appliqués, auront un effet réel ou potentiel sur l'action de l'organisation. Cela peut inclure, sans s'y limiter, des procédures d'enregistrement ou des règlements d'importation restrictifs, ou la publication régulière des aides financières reçues.

Enquêtes policières

Le processus ou l'acte d'examiner les faits liés aux allégations contre les employés ou l'organisation.

Catastrophe naturelle

Catastrophe naturelle, réelle ou prévue, qui se produit ou devrait se produire dans une ville ou un pays où l'organisation a un bureau. Les catastrophes naturelles peuvent inclure des tremblements de terre, des volcans, des ouragans, des tornades, des tempêtes produisant des dommages (grêle, inondations soudaines), des inondations ou des tsunamis.

Perquisition

Perquisition d'un local par des autorités extérieures.

Menace à distance contre l'organisme

Incident au cours duquel l'organisation ou un employé de celle-ci reçoit une menace, non pas en face à face, mais par un mécanisme à distance (e-mails, SMS, téléphone ou menaces générales émises sur un site Web ou un réseau social). Il peut s'agir, entre autres, de menaces directes criées par des civils lors de manifestations.

Risque d'atteinte à la réputation

Incidents impliquant un risque perçu, réel, effectif ou potentiel pour le logo/l'emblème, l'image ou la réputation de l'organisation.

Prise de contrôle/occupation des bureaux de l'organisation

La saisie et l'occupation de tout bâtiment, entrepôt ou enceinte de l'organisation par des agents du gouvernements ou des membres du public.

Menace de fermeture

Incidents impliquant la menace d'une fermeture forcée d'une activité, d'un programme ou d'une organisation.

Employé témoin

Situation dans laquelle un membre du personnel est témoin d'une attaque ou d'un crime contre un autre membre du personnel, des membres de sa propre famille ou des bénéficiaires.

Autres

Autre incident

Tout incident que ne peut décrire adéquatement l'une des catégories d'incidents prédéfinies dans cette liste. Dans le cas où cette catégorie est retenue, la personne effectuant le signalement devrait fournir une description détaillée de l'incident dans le champ « description de l'incident ».

Quasi-accident

Incidents qui auraient pu causer des dommages ou affecter le travail de l'organisation. Inclut toute situation dans laquelle un incident de sécurité a failli se produire, mais ne s'est pas produit, s'est produit près d'un travailleur humanitaire, d'une organisation ou d'un programme, ou dans laquelle les personnes concernées ont pu éviter tout préjudice grave. En cas de préjudice, l'incident doit être classé dans une autre catégorie.

Incident criminel évité

Incident évité de justesse survenu dans un contexte criminel.

Meurtre/Blessures/Enlèvement évités

Lors de l'incident, un employé a évité de justesse d'être tué, blessé ou enlevé.

Accident de la route

Tout accident de la route impliquant des véhicules de l'organisation. Le terme « véhicule » désigne toute forme de transport, y compris, mais sans s'y limiter, les voitures, les camions, les autobus, les motocyclettes ou autres (bicyclettes, bateaux), que ce soit pendant ou en dehors du service.

Accidents mortels à moto

Accident de moto avec décès d'employés.

Blessures causées par un accident de moto

Accident de moto avec blessures des employés.

Accident de moto sans blessuress

Accident de moto sans blessures pour les employés.

Décès associés aux véhicules automobiles

Accident de véhicule avec décès d'employés.

Blessures associées à des véhicules automobiles

Accident de véhicule avec blessures d'employés.

Accident de véhicule sans blessures

Accident de véhicule sans blessures pour les employés.

Autre accident de la circulation

Autre accident de la route non répertorié ici. Dans le cas où cette catégorie est retenue, la personne effectuant le signalement devrait fournir les détails dans le champ « description de l'incident ».

Mesures de sécurité

Mesures prises par des organismes à la suite d'une insécurité généralisée ou d'un incident lié à la sécurité.

Évacuation médicale

Évacuation d'un employé pour des raisons médicales, impliquant généralement des blessures ou des maladies qui ne peuvent être traitées de manière adéquate à l'hôpital local, au cabinet médical ou au centre de soins.

Évacuation non médicale

Évacuation d'un employé pour des raisons de sécurité. L'évacuation fait référence au déplacement des employés hors du pays d'opération. Le déplacement des employés vers un autre site au sein du même pays pour des raisons de sécurité est appelé une relocalisation.

Hibernation

Processus de confinement jusqu'à ce que le danger soit passé ou qu'une aide supplémentaire soit apportée.

Imposition de couvre-feu

Imposition d'un couvre-feu dans une ville ou un pays dans lequel l'organisation a un bureau.

Fermeture du bureau

Décision de fermer un bureau en raison du contexte général d'insécurité ou à la suite d'un incident spécifique.

Suivi continu

Processus de surveillance active d'une situation de sécurité en vue de modifier éventuellement les mesures de sécurité.

Suspension du programme

Processus consistant à modifier de manière significative les activités prévues, généralement en interrompant une activité ou un programme spécifique.

Relocalisation

Déplacement du personnel vers un site plus sécurisé dans le même pays.

Interdiction de voyager — sans couvre-feu

Toute imposition d'une interdiction de voyager qui affecte le personnel. Ce type d'incident est comparable à un avis aux voyageurs et peut être le résultat de troubles politiques ou sociaux, d'épidémies ou de catastrophes naturelles.

Exploitation et abus sexuels

Tout acte sexuel ou tentative d'acte sexuel, parfois réalisé avec violence ou coercition. La violence sexuelle peut aller des commentaires sexuels non désirés et du harcèlement sexuel au viol.

Commentaires sexuels non désirés

Avances verbales, comme le fait de siffler, de crier et/ou de dire des phrases ou faire des propositions sexuellement explicites ou implicites, qui ne sont pas désirées.

Attouchements sexuels non désirés

Attouchements importuns de nature sexuelle, quelle que soit leur intensité. Il peut s'agir de massage, de pelotage, de saisie ou d'effleurement d'une partie quelconque du corps d'une autre personne.

Harcèlement sexuel

Avances sexuelles importunes, demandes de faveurs sexuelles et autres comportements verbaux ou physiques de nature sexuelle qui affectent l'emploi de la personne visée. Une telle conduite a pour but ou pour effet d'interférer de manière déraisonnable avec les performances professionnelles d'une personne ou de créer un environnement de travail intimidant, hostile ou offensant.

Exemples :

- le consentement à une telle conduite est présenté, explicitement ou implicitement, comme une condition d'emploi de l'individu ;
- le consentement à une telle conduite ou le rejet par un individu est utilisé comme fondement des décisions d'emploi affectant cet individu.

Comportement sexuel agressif

Comportement potentiellement violent axé sur l'assouvissement de pulsions sexuelles.

Harcèlement criminel

Désigne le fait pour une personne de surveiller une autre ou de commettre des actes à son égard de manière non désirée ou répétée.

Agression sexuelle

Acte impliquant un contact sexuel, commis sur le corps d'une personne sans le consentement de celle-ci.

Viol

Rapport sexuel (pénétration orale, vaginale ou anale) contre la volonté et sans le consentement de la victime.

Tentative d'agression sexuelle

Tentative de contact sexuel commis sur le corps d'une personne sans le consentement de celle-ci.

Autres actes sexuels

Lorsqu'une personne prend ou diffuse des photos ou des vidéos d'une autre personne déshabillée sans l'autorisation de celle-ci.

Troubles

Troubles civils ou politiques et comportements tumultueux ou émeutiers, notamment : pillages, révoltes dans les prisons, foules mettant le feu à des biens, ou bagarres avec la police (généralement par des manifestants).

Manifestation

Toute manifestation (protestations, marches, manifestations assises, piquets de grève) qui est non-violente. Rassemblement de masse à des fins politiques ou sociales.

Pillage

Vol pendant des troubles, des violences, des émeutes ou d'autres bouleversements.

Grève/Absence

Décision délibérée du personnel de ne pas se présenter au travail pour des raisons autres que la maladie.

Autres

Toute autre activité ne figurant pas dans la liste plus haut.

Utilisation d'armes

Le type d'arme(s) utilisée(s) lors d'un incident qui a affecté le personnel, les infrastructures ou l'acheminement de l'aide.

Armes chimiques, biologiques, radiologiques et nucléaires (CBRN)

Toute utilisation d'armes biologiques, chimiques, nucléaires ou radiologiques dans une ville ou un pays où l'organisation a un bureau.

Explosifs

Toute utilisation d'armes explosives qui implique les employés ou les biens de l'organisation.

Arme à feu

Toute utilisation d'armes à feu ou d'armes de poing impliquant des employés ou des biens de l'organisation.

Aucune information

Des armes ont été utilisées lors de l'incident, mais le type d'arme n'est pas clair.

Autres

Toute utilisation d'objet tranchant, de feu, de couteau ou de pierre qui implique les employés ou les biens de l'organisation.

Utilisation d'armes explosives

Le type d'arme(s) explosive(s) utilisée(s) dans l'incident qui a affecté le personnel, l'infrastructure ou la livraison de l'aide.

Bombes aériennes

Armes explosives larguées depuis un avion, y compris des armes incendiaires. N'inclut pas les bombes à fragmentation et les missiles sol-sol.

Bombe à fragmentation

Armes larguées depuis un avion ou lancées à partir du sol qui explosent en libérant des milliers d'éclats.

Grenade à main

Petit engin explosif lancé à la main, conçu pour exploser après l'impact ou après un laps de temps déterminé.

Mines

Toute explosion de mine qui implique le personnel.

Dispositif explosif improvisé radiocommandé

Dispositif explosif improvisé radiocommandé, tel qu'une bombe qui aurait été laissée sur le bord de la route et qui explose à l'approche de la cible.

Lancement au sol

Missiles, mortiers ou obus lancés à partir d'un système de lancement mobile ou stationnaire, y compris des grenades à tube.

Attentat suicide à l'aide d'un véhicule piégé

Engin explosif improvisé porté par une personne (ceinture d'explosifs, explosifs dans un sac à dos).

Véhicule piégé

Véhicule piégé (voiture piégée, voiture contenant un engin explosif).

Autres

Toute autre arme explosive non répertoriée ou une combinaison des éléments ci-dessus. Dans le cas où cette catégorie est retenue, la personne effectuant le signalement devrait fournir les détails dans le champ « description de l'incident ».

Type d'emplacement

Le type d'emplacement où l'incident a eu lieu.

Administratif

Pendant une procédure administrative ou alors que la victime obéissait à un ordre d'une autorité reconnue/publique.

Piste d'atterrissage

Sur une piste d'atterrissage, y compris un aéroport ou dans les airs.

Poste de contrôle

À un poste de contrôle, une porte d'accès ou un barrage routier.

Communication

Sous la forme d'une communication (appel téléphonique, SMS, lettre, e-mail).

Complexe

Dans le complexe où logeait la ou les personnes concernées.

Zone de forte affluence

Dans une zone bondée, comme un marché, un bazar ou un espace public ouvert où les gens se déplacent.

Bâtiment sanitaire

Dans un bâtiment sanitaire, un hôpital, un dispensaire, un bureau d'hôpital ou un poste de premiers secours.

Camp de déplacés ou de réfugiés

Dans un camp temporaire ou permanent de réfugiés ou de personnes déplacées.

Immeuble de bureaux
Dans un complexe de bureaux.

Poste de police
Dans un poste ou des locaux de police.

Site du projet
Sur le site d'un projet.

Bâtiment public
Dans un bâtiment public (restaurants, églises, mosquées, hôtels).

Domicile
Au domicile de personnel humanitaire ; comprend les incidents qui se sont produits tout juste à l'extérieur de tels domiciles.

Route
Sur une route, y compris :

- des endroits non spécifiés pendant un voyage en voiture ;
- tout mode de transport (à pieds, moto, véhicule) ;
- tout incident qui a lieu entre deux lieux ou en transit.

École
Dans une école ou un lieu d'enseignement.

Navire
Sur un bateau ou un navire.

Entrepôt
Dans un entrepôt, y compris les quais.

Eau

Sur l'eau (rivière, lac, mer, océan) ou à proximité.

Aucune information
Les informations disponibles ne permettent pas de savoir où l'incident a eu lieu.

Autres
Dans un type d'emplacement non répertorié ici. Dans le cas où cette catégorie est retenue, la personne effectuant le signalement devrait fournir les détails dans le champ « description de l'incident ».

Auteur des faits

Classification de l'auteur ou des auteurs présumés de l'incident.

Administration
Administrateur/autorité d'un pays/territoire, niveau de commandement élevé d'une force armée ou individus au sein d'un groupe armé qui a assumé le contrôle de facto d'un territoire et qui détermine les lois et les règlements ou maintient l'ordre.

Bénéficiaire

Bénéficiaire direct de l'aide.

Civil

Civil (réfugié, IDP, villageois, colon) qui n'est pas un bénéficiaire direct.

Criminel

Criminel agissant seul ou dans le cadre d'une organisation criminelle.

Employé ou ancien employé

Employé actuel ou ancien de l'organisation.

Maintien de l'ordre

Individus ou organes de l'appareil d'application de la loi de l'État (police et « forces de sécurité »), mais non des forces militaires ou de sécurité privée qui agissent selon les ordres du système d'application de la loi de l'État.

Multiples

Plusieurs auteurs de différentes catégories ont participé à l'attaque.

Groupes armés non étatiques

Groupe armé nommé qui ne fait pas partie des forces de l'ordre, de l'armée ou de l'appareil de sécurité de l'État. Cela inclus les armées privées, les groupes de vigiles, les rebelles, les guérilléros ou les groupes terroristes, mais n'inclut pas les acteurs de la sécurité privée.

Sécurité privée

L'auteur de l'incident appartient à une société de sécurité privée ou exerce les fonctions de garde du corps ou d'agent de sécurité.

Parent ou associé

Membre de la famille, ami ou autre personne connue d'un ou de plusieurs employés.

Acteur étatique

Soldats d'une armée d'État qui agissent sous les ordres du commandement militaire de cet État.

Sous-traitant

Sous-traitant de l'organisme.

Acteurs armés non militaires non spécifiés

Un groupe de personnes armées non identifiées ou sans nom, ou référence dans le rapport dans un sens générique, aux rebelles, aux extrémistes ou aux groupes qui, sous une forme ou une autre, sont affiliés à l'armée ou utilisent des structures militaires (portant des treillis militaires) sans indication de lien à une armée d'État.

Aucune information

Soit le rapport n'identifie pas l'auteur de l'incident, soit l'auteur est inconnu.

Mobile

Classification du mobile de l'auteur ou des auteurs de l'incident.

Critère présumé

Une action ciblée, utilisée spécifiquement contre un employé, une organisation ou un bénéficiaire, mais dont le mobile reste flou.

Aveugle

Une action ciblée utilisée contre des civils et ne visant pas spécifiquement un employé, une organisation ou un bénéficiaire.

Critère relatif aux actifs

Une action ciblée, utilisée contre un employé, une organisation ou un bénéficiaire, dans l'intention d'un gain matériel ou l'accès à des biens ou des infrastructures plutôt que dans l'intention de nuire à l'employé, l'organisation ou le bénéficiaire.

Critère lié à l'action militaire

Une personne ou une chose a été ciblée de manière sélective (mouvements de troupes, usine d'armement, etc.), entrainant des conséquences pour l'employé, l'organisation ou le bénéficiaire. Ne figurent dans cette catégorie que les évènements qui se produisent pendant un conflit actif.

Critère lié au programme

Une action ciblée utilisée contre un employé ou une organisation du fait qu'ils ont fourni un programme ou un service particulier ou contre un bénéficiaire du fait qu'il a utilisé le programme ou le service.

Critère lié au prestataire

Une action ciblée utilisée contre un employé, une organisation ou un bénéficiaire en raison de l'identité ou des valeurs fondamentales de l'organisation.

Aucune information

Le rapport ne contient pas d'informations qui suffisent à déterminer si l'évènement était ciblé ou non.

Autres critère

Une personne ou une chose a été ciblée de manière sélective, entrainant des conséquences pour l'employé, l'organisation ou le bénéficiaire.

Informations sur la victime ou les victimes

Au moment de consigner les informations relatives aux victimes impliquées dans un incident, il convient d'inclure les catégories indiquées plus bas. Ces informations doivent rester confidentielles. Toute décision prise sur la base de ces informations doit être non-discriminatoire et conforme aux politiques d'équité, de diversité et d'inclusion, ainsi qu'aux lois en vigueur.

Genre

Les victimes sont classées selon le sexe biologique ou l'identité de genre choisie (selon la politique de votre organisation).

Origine ethnique

S'il y a lieu, et si cela aide à recenser des schémas sous-jacents de menaces ou de violence, il convient d'inclure des informations sur l'origine ethnique.

Diversité

S'il y a lieu, et si cela aide à recenser des schémas sous-jacents de menaces ou de violence, il convient d'inclure des informations sur d'autres facteurs de diversité (exemples : orientation sexuelle, handicaps).