outil 46 Gestion des informations

Fiche d'information

Afin de protéger la sécurité et la vie privée des victimes et de limiter les risques pour l'organisation, les informations sur les cas de violations graves doivent être gérées dans le strict respect des règles de confidentialité. Cela implique des précautions spéciales en matière de recueil, de conservation et de partage de ces informations.

Sécurité et confidentialité lors du recueil des informations.
Analysez votre vulnérabilité dans des situations pouvant compromettre votre sécurité ainsi que celle de votre source et/ou la confidentialité des informations et prenez des mesures appropriées atténuant les risques selon leurs niveaux.

Risque	Niveau (élevé/ moyen/faible)	Suggestions
Des informations peuvent être entendues par hasard ou relayées à des personnes qui n'ont *pas besoin* de les connaitre		☐ Choisissez un endroit adéquat pour mener des entretiens. ☐ Ne discutez pas des informations sur des cas avec ou devant des personnes qui n'ont *pas besoin* de les connaitre (par ex. chauffeurs de taxi ou du bureau, personnel chargé du ménage ou d'autres services, collègues d'autres projets ou organisations, amis personnels, voisins, proches, etc.). ☐ Evitez de communiquer des informations sensibles par téléphone s'il existe un risque que votre téléphone soit sur écoute et soyez extrêmement prudent si vous devez le faire (par ex. utilisez des mots codés). ☐ Ne laissez pas des informations sur des cas à la vue de tous ou dans des endroits communs. ☐ Ne transmettez pas d'informations sur des cas par l'intermédiaire d'autres personnes, à moins qu'elles soient spécifiquement autorisées à le faire.
Des informations peuvent être perdues		☐ Gardez toujours sur vous les informations sur des cas jusqu'à ce que vous puissiez les conserver. ☐ Conservez des copies des informations sur des cas dans un endroit sûr. ☐ Utilisez des codes pour la victime, le surveillant, le lieu, la violation et l'auteur.
Des informations peuvent être saisies (arrestation, barrage routier, point de contrôle)		☐ Utilisez des codes pour le cas, la victime, le lieu, le point de contact, l'auteur. ☐ S'il existe un risque imminent ou probable que les informations soient saisies, limitez-vous à des échanges oraux et écrivez le rapport plus tard dans un lieu sûr. ☐ Ne notez que quelques informations et complétez le rapport dès que possible dans un lieu sûr. ☐ Assurez-vous de savoir quoi dire et comment vous comporter dans une situation où des informations sensibles risquent d'être saisies (raid, arrestation, barrage routier, point de contrôle).
La source qui a fourni des informations à votre organisation peut être découverte, ce qui l'expose au harcèlement, à des représailles ou à la stigmatisation		☐ Choisissez un endroit adéquat pour mener des entretiens et vérifiez que la source se sent en sécurité à cet endroit. ☐ Assurez-vous que la victime ou le parent/tuteur donne son consentement éclairé avant un entretien. ☐ Gardez un profil bas quand vous menez des entretiens. ☐ Coordonnez-vous étroitement avec l'ONU pour vous assurer que les missions de vérification n'attirent pas trop l'attention sur la source. ☐ Identifiez les organisations ou entités partenaires capables de fournir une protection physique à une victime/témoin en danger (par ex. transfert) et discutez de cette option avec la victime/témoin.
Autre :		

Sécurité et confidentialité lors de la conservation des informations.

Evaluez vos vulnérabilités – à quel niveau se situent les risques suivants pour votre bureau/organisation – et sélectionnez les moyens pertinents pour les limiter en fonction du niveau de risque :

Risque	Niveau (élevé/ moyen/faible)	Suggestions
Dommage aux locaux (et documents) en raison d'un événement ou d'une catastrophe naturelle		☐ Conservez des copies des fichiers électroniques et papier dans un autre lieu. ☐ Réduisez le volume d'informations que vous conservez dans ce lieu, par exemple en archivant les anciens dossiers ailleurs (dans un autre bureau ou à l'étranger). ☐ Envisagez de conserver toutes les informations ailleurs. ☐ Notez bien toutes les mesures nécessaires dans un plan d'intervention en cas d'urgence.
Fouilles/raids		☐ Réduisez le volume d'informations que vous conservez dans ce lieu, par exemple en archivant les anciens dossiers ailleurs (dans un autre bureau ou à l'étranger) tous les deux ans. ☐ Conservez des copies des fichiers électroniques et papier dans un autre lieu ☐ Envisagez de conserver toutes les informations ailleurs. ☐ Conservez les tirages papier dans un endroit discret mais sûr si vous estimez qu'un meuble fermé à clé attirerait trop l'attention lors d'une fouille ou d'un raid. ☐ Notez bien toutes les mesures nécessaires dans un plan d'intervention en cas d'urgence.
Vol		☐ Conservez les tirages papier dans un meuble fermé à clé ou dans un endroit discret si un meuble fermé à clé attirerait trop l'attention lors d'un vol. ☐ Ne conservez pas de fichiers dans des équipements de valeur (ordinateurs portables) ou veillez à ne pas les laisser dans les locaux à l'heure de la fermeture. ☐ Conservez les fichiers électroniques dans un équipement portable que vous pouvez emporter hors des locaux. ☐ Détruisez tous les fichiers en dernier ressort (effacez, déchiquetez, incinérez). ☐ Evaluez la sécurité du bureau et renforcez-la, si nécessaire. ☐ Conservez des copies des fichiers électroniques et papier dans un autre lieu.
Fermeture soudaine des locaux en raison d'une attaque imminente		☐ Envisagez de conserver toutes les informations ailleurs. ☐ Conservez les fichiers électroniques dans un équipement portable que vous pouvez facilement emporter hors des locaux. ☐ Retirez les dossiers des locaux avant de fermer les locaux. ☐ Détruisez tous les fichiers en dernier ressort avant de fermer les locaux (effacez, déchiquetez, incinérez). ☐ Conservez des copies des fichiers électroniques et papier dans un autre lieu. ☐ Notez bien toutes les mesures nécessaires dans un plan d'intervention en cas d'urgence.
Surveillance électronique		☐ Protégez les fichiers électroniques avec des mots de passe ou par cryptage. ☐ Modifiez les mots de passe à intervalles irréguliers. ☐ Limitez le nombre de personnes autorisées à avoir un accès direct aux informations. ☐ Assurez-vous que votre ordinateur dispose d'un pare-feu en état de fonctionnement.
Autre :		

Sécurité et confidentialité lors du partage des informations avec les points de contact MRM.

☐ Clarifiez le format et le mode de communication : évitez d'envoyer des informations sensibles par voie électronique ou faites-le avec précaution si vous devez le faire (les pare-feux ne protègent pas les documents envoyés par voie électronique) : protégez tous les documents par des mots de passe et/ou utilisez une plate-forme de partage de fichiers sécurisée.

OUTIL 46

(suite)

- ☐ Clarifiez le type d'informations que vous pouvez partager avec le point de contact MRM et si des codes ou des mots codés seront utilisés.
- ☐ Clarifiez qui, dans votre organisation, est autorisé à fournir des informations au point de contact MRM.
- ☐ Clarifier qui, à l'ONU, est le point de contact MRM qui recevra vos informations.
- ☐ Etablissez une relation basée sur la confiance avec votre point de contact MRM.
- ☐ Clarifiez comment l'ONU gèrera les informations fournies par votre organisation (où seront-elles conservées, comment seront-elles communiquées au sein du MRM).
- ☐ Envisagez l'adoption d'un protocole officiel de partage des informations avec l'ONU, détaillant tous les points mentionnés ci-dessus.

Documents institutionnels susceptibles d'être élaborés ou adaptés selon la manière dont vous participez au MRM.

Documents	Points clés
Code de conduite du personnel	• Comportement lors du recueil d'informations sensibles. • Comportement lors de la discussion d'informations sensibles. • Respect des protocoles et plans internes.
Protocole interne de protection des données [Voir documents utiles ci-dessous relatifs au Système de gestion des informations pour la protection de l'enfance]	• Qui recueille les informations ? • Comment ces informations sont-elles transférées du terrain au bureau principal ? • Qui d'autre, dans l'organisation, peut avoir accès aux informations ? • Qui analyse les informations ? • Qui communique les informations aux acteurs externes ? • Quels codes et mots codés sont utilisés ? • Où les informations sont-elles sauvegardées et conservées (format papier, électronique) ? • Qui a accès aux mots de passe et clés ? • Plan d'intervention en cas d'urgence : quelles sont les mesures à prendre, qui est responsable ?
Inclure la gestion des informations dans le plan de sécurité de l'organisation	• Inclure des mesures préventives pour conserver les informations sensibles en toute sécurité. • Inclure un plan d'intervention pour supprimer ou détruire les informations sensibles en cas d'urgence.
Informations sur la personne / formulaire de consentement	• Présenter une diversité d'options quant à la manière dont l'information sera utilisée et qui pourra y avoir accès afin de faciliter le consentement éclairé.

autres outils pertinents

- outil 45 – Exemplaire de base de données pour la surveillance et la communication de l'information sur les violations graves
- outil 44 – Q&R 'utiliser une base de données de cas'
- outil 29 – Checklist 'confidentialité'
- outil 30 – Checklist 'consentement éclairé'
- outil 47 – Exercice en groupe 'confidentialité & gestion des informations'

autres documents

- Child Protection Information Management System, Training Manual (Template data protection protocol and data protection checklist) available at **www.childprotectionims.org**
- *Standards Minimums pour la protection de l'enfance dans l'intervention humanitaire,* Groupe de Travail sur la Protection de l'Enfance (GTPE), 2012 – Standard 5 'Gestion de l'information'
- Trousse de Sécurité: outils et tactiques de sécurité numérique, Tactical Technology Collective & Frontline Defenders
- Manuel de sécurité: mesures pratiques pour les défenseurs des droits humains en danger, Frontline Defenders, 2011