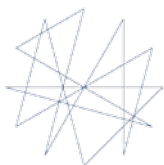


دليل إدارة معلومات الحوادث الأمنية



Funded by
European Union
Humanitarian Aid

eisf



redruk
people and skills for disaster relief

Aid in Danger



Insecurity
Insight

Data on People in Danger

”تتضمن إدارة معلومات الحوادث الأمنية جمع المعلومات وتسجيلها وتحليلها واستخدامها للحفاظ على أمن الموظفين والوصول إلى المستفيدين. وتجد إدارة المعلومات الأمنية الجيدة التوازن الصحيح بين هذه المنافع والتكاليف الإدارية للنظام“

شكر وتقدير

تم إعداد وإتاحة هذا الدليل بالتعاون بين كل من RedR UK، و Insecurity Insight، ومنتدى الأمن الأوروبي المشترك بين الوكالات (EISF)، وذلك كجزء من مشروع إدارة معلومات الحوادث الأمنية الممول من قبل المفوضية الأوروبية للمساعدات الإنسانية والحماية المدنية (Humanitarian EU Aid). للمزيد من المعلومات يرجى الاطلاع على الصفحة التي خصصتها منظمة RedR للمشروع.

عملت مارين مونييه (RedR UK) على تنسيق هذا المشروع. وقد حظي هذا الدليل بمدخلات كثيرة من كريستينا ويل (Insecurity Insight) وليزا ريلي (EISF). أما محررة الدليل فهي أديليسيا فيربانكس (EISF). كما يود فريق المشروع التقدم بجزيل الشكر إلى أعضاء الفريق الاستشاري وغيرهم من المساهمين الذين لا يمكن ذكر أسماء كل واحد منهم على حدة هنا على مشاركة خبراتهم وأدواتهم وملاحظاتهم القيمة. ويقر مشروع ”إدارة معلومات الحوادث الأمنية“ بتوسيع نطاق المساهمات المقدمة واستعداد المنظمات والأفراد للمشاركة.

إخلاء مسؤولية

يعتبر هذا الدليل عنصراً واحداً من عناصر مشروع أوسع نطاقاً يرمي إلى بناء قدرات القطاعين الإنساني والإنمائي؛ لذلك فإن أنشطة بناء القدرات الأخرى تُكمل هذه الأداة. وتعكس هذه الوثيقة الممارسات الحالية في هذا القطاع، وتقدم توصيات وملاحظات، بما في ذلك آراء أو توصيات الأطراف الثلاثة. وهذه الممارسات ليست إلزامية، وهي عمل قيد التقدم والتطور.

في حين يسعى مشروع ”إدارة معلومات الحوادث الأمنية“ إلى ضمان دقة وجودة المعلومات الواردة في ”دليل إدارة معلومات الحوادث الأمنية“، فإن RedR UK، و Insecurity Insight، و EISF لن تكون مسؤولة قانونياً عن أية خسارة أو ضرر أو إزعاج ناتج عن أي استخدام أو عدم القدرة على استخدام أو تفسير أية من المعلومات الواردة في هذا الدليل. لن تتحمل RedR UK، و Insecurity Insight، و EISF المسؤولية ولن تكون مسؤولة تجاهك أو اتجاه أي شخص آخر عن الأضرار التي قد تتكبدها أيا كانت القرارات أو الإجراءات المتخذة استناداً إلى المعلومات المقدمة في ”دليل إدارة معلومات الحوادث الأمنية“.

تم توفير المعلومات الواردة في هذه الوثيقة ”كما هي“، دون أية شروط أو ضمانات أو أية شروط أخرى من أي نوع، ويكون الاعتماد على أية معلومات جوهرية أو معلومات أخرى تحتوي على هذه الوثيقة على مسؤوليتك الخاصة.

المختصرات

Aid in Danger	AiD
قاعدة البيانات الأمنية للعاملين في مجال تقديم المعونة	AWSD
منتدى الأمن الأوروبي المشترك بين الوكالات	EISF
الأسئلة الشائعة	FAZ
المقر الرئيسي	HQ
اللجنة الدائمة المشتركة بين الوكالات	IASC
اللجنة الدولية للصليب الأحمر	ICRCC
منظمة حكومية دولية	IGO
القانون الدولي الإنساني	IHL
منظمة دولية غير حكومية	INGO
الأيزو - المنظمة الدولية لتوحيد المقاييس	ISO
منظمة غير حكومية محلية	LNGO
منظمة غير حكومية	NGO
الإسعافات الأولية النفسية	PFA
الاستغلال والاعتداء الجنسيين	SEA
منسق شؤون الأمن	SFP
إدارة معلومات الحوادث الأمنية	SIIM
معاً من أجل إنقاذ الأرواح	SLT
إجراءات التشغيل الموحدة	SOPs
إدارة الأمم المتحدة لشؤون السلامة والأمن	UNDSS
منظمة الصحة العالمية	WHO

المحتويات

الهدف الثاني: الدروس المستفادة

- 41 والمطبقة
- 42 2.1 تحليل ما بعد الحوادث
- 44 2.2 تنفيذ الدروس المستفادة
- 45 2.3 التحليل وإجراءات متابعة الحالات الحساسة

الهدف الثالث: فهم السياق

- 47 التشغيل
- 48 3.1 التطبيقات العملية لمشاركة المعلومات الأمنية
- 51 3.2 المشاركة الخارجية لمعلومات الحوادث
- 52 3.3 المنتديات ومشاركة المعلومات الأمنية
- 53 3.4 مصادر تحليل أنماط السياق الخارجية

الهدف الرابع: اتخاذ القرارات

- 57 الاستراتيجية
- 59 4.1 التسجيل المنهجي للحوادث: ما هو النظام الذي ينبغي استخدامه؟
- 61 4.2 تحليل الاتجاهات للاسترشاد بها في اتخاذ القرارات الاستراتيجية
- 62 4.3 الهياكل التنظيمية لمناقشة قضايا الأمن الاستراتيجي
- 63 4.4 كيفية استخدام معلومات حوادث العنف الجنسي على المستوى الاستراتيجي
- 64 4.5 استخدام معلومات الحوادث الأمنية للدعوة الاستراتيجية

مقدمة

- 1 حول هذا الدليل
- 2 لمن تم إعداد هذا الدليل؟
- 2 طريقة استخدام هذا الكتيب
- 5 التعاريف الرئيسية

الفصل 1: التعرف على إدارة

- 8 معلومات الحوادث الامنية
- 9 ما هي إدارة معلومات الحوادث الأمنية؟
- 10 التحديات الرئيسية لإدارة معلومات الحوادث الأمنية
- 12 إدارة المخاطر الأمنية وإدارة معلومات الحوادث الأمنية
- 13 كفاءات الموظفين الأمنيين وإدارة معلومات الحوادث الأمنية
- 14 أمن المعلومات
- 15 إدارة الحوادث وإدارة معلومات الحوادث الأمنية: فوائد التأهب التنظيمي
- 17 واجب الرعاية

الفصل الثاني: الأهداف الأربعة

20 لإدارة معلومات الحوادث الأمنية

21 الهدف الأول: الاستجابة الفورية

- 1.1 توجيهات حول الإبلاغ عن الحادث: ماذا؟ متى؟ كيف؟ من؟
- 23 1.2 التعامل مع الإجهاد
- 30 1.3 عملية متابعة الحوادث الأمنية
- 33 1.4 الاتصالات
- 1.5 التعامل مع الحالات الحساسة: العنف الجنسي ضد الموظفين
- 36

102	الأداة 10: تخزين الحادث
	الأداة 11: التقنية المستخدمة في الإبلاغ عن
105	الحوادث وتسجيلها
109	الأداة 12: تحليل ومقارنة اتجاهات البيانات
	الأداة 13: الأسئلة الاستراتيجية المتعلقة
112	باتخاذ قرارات إدارة معلومات الحوادث

116 قائمة المراجع

121	معلومات إضافية
121	المنظمات
121	جهات الاتصال

68 الفصل الثالث: الأدوات

	الأداة 1: شبكة التقييم الذاتي لإدارة
69	معلومات الحوادث الأمنية
74	الأداة 2: تصنيف الحوادث
83	الأداة 3: الحوادث التنظيمية أو الخارجية
85	الأداة 4: نموذج الإبلاغ عن الحوادث
88	الأداة 5: تحليلات الحوادث
92	الأداة 6: كيفية إجراء الاستجواب الواقعي
	الأداة 7: الممارسات الجيدة للإبلاغ عن
	الحوادث ذات الصلة بالاعتبارات الجنسانية
	وآليات الشكاوى للإبلاغ عن الاستغلال
95	والانتهاك الجنسيين (SEA)
98	الأداة 8: خطة العمل لمتابعة الحادث
	الأداة 9: أنظمة إدارة معلومات الحوادث
99	الأمنية

مقدمة

حول هذا الدليل

إدارة معلومات الحوادث الأمنية هي جمع المعلومات (بما في ذلك البيانات) المرتبطة بالحوادث الأمنية والإبلاغ عنها وتسجيلها وتحليلها ومشاركتها وتبادلها واستخدامها. تعتبر إدارة معلومات الحوادث الأمنية جزءاً أساسياً من الإدارة الأوسع للمخاطر الأمنية في المنظمة، والتي تهدف إلى دعم الأمن التنظيمي من أجل تحسين الوصول إلى السكان المحتاجين في نهاية المطاف.

يسعى دليل إدارة معلومات الحوادث الأمنية إلى تقديم مساهمة هامة في النهوض بالممارسات المتصلة بإدارة معلومات الحوادث الأمنية داخل المنظمات غير الحكومية.

يهدف الدليل إلى دعم المستخدمين في إنشاء وتطوير إدارة معلومات فعّالة لنظم الإبلاغ عن الحوادث الأمنية ورصدها، على الصعيدين الداخلي والخارجي في جميع أنحاء المنظمة والقطاع.

تشكل هذه الوثيقة جزءاً من مشروع أوسع نطاقاً لإدارة معلومات الحوادث الأمنية يهدف إلى تعزيز الاستجابات الإنسانية للأزمات من خلال بناء قدرات المنظمات غير الحكومية لتحسين إدارة المعلومات المتعلقة بالحوادث الأمنية وتعزيز قدرتها على تبادل المعلومات المتعلقة بالحوادث بطريقة آمنة ومناسبة لدعم اتخاذ القرارات الجيدة عبر مختلف مستويات المنظمة.

يقدم "دليل إدارة معلومات الحوادث الأمنية" مجموعة واسعة من الأدوات والتوجيهات، بدءاً من النصائح حول كيفية تصميم تقرير فعال عن الحوادث الأمنية وصولاً إلى مشاركة المعلومات المتعلقة بحوادث الأمن بكفاءة مع مجموعة واسعة من أصحاب المصلحة المعنيين. يتبع نهج إدارة المخاطر الأمنية والمفردات الواردة في هذه المبادئ التوجيهية المعيار العالمي الصادر عن المنظمة الدولية للتوحيد القياسي (أيزو)، "إدارة المخاطر - المبادئ والمبادئ التوجيهية" (من الآن فصاعداً ISO 31000:2009).

يتناول هذا الدليل إدارة معلومات الحوادث الأمنية، وليس إدارة الحوادث الأمنية بحد ذاتها.

ينطبق معظم هذا الدليل على جميع أنواع الحوادث، بما في ذلك الحوادث الخطيرة، أي الأحداث التي تعطل العمليات العادية والروتينية وتتطلب استجابة المنظمة لإدارة الأزمات. وسيتم في هذا الدليل استخدام مصطلح "حادث" للإشارة إلى جميع أنواع الحوادث. وعند الإشارة إلى حادثة حرجية، سيتم تحديد ذلك. ويمكن الإشارة أحياناً إلى "الحوادث غير الحرجية" التي ستشير إلى جميع الحوادث التي لا تعتبر حرجية وبالتالي لا تتطلب استجابة لإدارة الأزمات. غير أنه من المهم التشديد على أنه في حين أن منظمة ما قد تعتبر بعض الحوادث حرجية إلا أن منظمة أخرى قد لا تعتبرها كذلك إذ لديها القدرة على التعامل مع الحادث من خلال إجراءات الإدارة الروتينية.

على الرغم من أن جمع وإدارة المعلومات المتعلقة بالحوادث التي لا تعتبر أمراً حرجياً، بما في ذلك "الحوادث التي أوشكت على الوقوع"، غالباً ما لا تقل أهمية، فإن جمع المعلومات ذات الصلة بالأمن واتخاذ القرارات المتعلقة بالأمن على أنها معلومات من الأحداث الحرجية أمر مهم. ولذلك،

يوفر هذا الدليل أدوات للمساعدة في وضع معايير للإبلاغ وإدارة المعلومات لجميع الحوادث، بما في ذلك تلك التي تحدث بشكل أكثر شيوعاً، ولا تعتبر عموماً حاسمة.

يعكس هذا الدليل الممارسات الحالية في القطاع، ويوفر توصيات وملاحظات للمنظمات غير الحكومية. ويستقي الدليل محتواه من موارد من مجموعة واسعة من الخبراء بما في ذلك منتدى الأمن الأوروبي المشترك بين الوكالات (Insecurity Insight، RedR UK، EISF) والعديد من المنظمات الأعضاء في هذه المجموعات والشبكات الواسعة. وفي الوقت الذي تستخدم فيه الأدوات والتوجيهات الحالية، فإنها تهدف إلى تجنب الازدواجية من خلال تسليط الضوء على عناصر إدارة معلومات الحوادث الأمنية واستخلاصها. هذا الدليل ليس إلزامياً، إلا أنه يقدم قائمة واسعة من الخيارات للمنظمات لتعزيز إدارة معلومات الحوادث الأمنية لديهم.

بالرغم من أن هذا الدليل قد كُتب مع التركيز على المنظمات والعمليات الإنسانية، إلا أن المعلومات الواردة فيه قابلة للتطبيق على المنظمات غير الحكومية الأخرى، وبالأخص المنظمات التي تُعنى بالتنمية.

يتضمن هذا الإصدار من الدليل (الذي نُشر في 2017) الملاحظات والمدخلات التي تم تلقيها من أصحاب المصلحة في القطاع الإنساني والتنموي.

هذه الوثيقة مفتوحة المصدر، وستكون متاحة عبر شبكة الإنترنت باللغات العربية والإنجليزية والفرنسية.

لمن تم إعداد هذا الدليل؟

إن "دليل إدارة معلومات الحوادث الأمنية" موجه لجميع الأفراد الذين يتحملون أي مستوى من المسؤولية في إدارة معلومات الحوادث الأمنية داخل منظمة غير حكومية، بصرف النظر عن موقعهم أو منصبهم. وهو مصمم كأداة لمستشاري الأمن والمديرين منسقي شؤون الاتصال والمحللين، فضلاً عن الإدارة العليا والمديرين العاملين للمشاريع / البرامج الذين يتحملون مسؤولية أمنية داخل المنظمات غير الحكومية، وهو مُعد في المقام الأول للممارسين.

طريقة استخدام هذا الكتيب

"دليل إدارة معلومات الحوادث الأمنية" مقسم إلى فصول، يقدم للقارئ نظرة عامة عن إدارة معلومات الحوادث الأمنية:

- يقدم الدليل في بادئ الأمر مفهوم "إدارة معلومات الحوادث الأمنية" وتماشيه مع النطاق الأوسع لإدارة المخاطر الأمنية في المنظمة.
- ثم يتناول الدليل الأهداف الأربعة لإدارة معلومات الحوادث الأمنية، مع تسليط الضوء على الخطوات الرئيسية في الإدارة الفعالة لمعلومات الحوادث الأمنية التي ستمكّن من تحقيق كل هدف.
- تتم الإشارة والرجوع إلى الأدوات في كامل النص، ويمكن إيجادها في نهاية هذا الدليل.

يوضح الشكل البياني التالي مختلف مكونات إدارة معلومات الحوادث الأمنية. ويتبع هيكل الدليل هذا الرسم البياني، وسيشير كل قسم منه إلى الجزء الذي تجري مناقشته من الدورة.

دورة إدارة معلومات الحوادث الأمنية: الأمن التنظيمي لتمكين الوصول دون معوقات إلى تقديم الإعانة

جاء هذا الرسم البياني على شكل دوري لإظهار أن إدارة معلومات الحوادث الأمنية هي عملية مستمرة تغذي فيها كل العناصر بعضها البعض لتحقيق أربعة أهداف أساسية. وفي قلب المعلومات المتعلقة بالحوادث الأمنية نجد الأمن التنظيمي مع هدف تمكين الوصول دون معوقات إلى تقديم الإعانات.



يوفر هذا الدليل نقاطاً للنقاش ونصائح ومشورة ونماذج مقترحة عبر الأهداف الأربعة الأساسية لإدارة معلومات الحوادث الأمنية ذات الصلة بأربعة أطر زمنية محددة وأربعة مستويات مختلفة للتركيز التنظيمي:

الهدف الأول: الإبلاغ عن ردة الفعل والاستجابة الفورية لحادث أمني. الهدف هنا هو ضمان البحث عن المعلومات واستخدامها لتوجيه الاستجابة الفورية للحادث. وعادة ما يتم هذا في الميدان و/أو على المستوى القطري بمجرد وقوع الحادث.



الهدف الثاني: تنفيذ الدروس المستفادة بعد وقوع الحادث الأمني لأغراض المتابعة والوقاية. الغرض هنا هو فهم ما حصل مع النظر إلى التخطيط وتنفيذ أي تغييرات وإجراءات من شأنها المساعدة في معالجة مخاطر الأحداث المماثلة في المستقبل، والتركيز بشكل خاص على الوقاية. وعادة ما يتم هذا الأمر على المستوى القطري/المقر الرئيسي بعد فترة قصيرة من وقوع الحادث.



الهدف الثالث: فهم السياق الأمني للمنظمة غير الحكومية. ويهدف هذا إلى تحسين المعرفة السياقية باستخدام بيانات الحوادث الداخلية والخارجية. سيساعد هذا الأمر على اتخاذ القرارات الاستراتيجية والتواصل الشامل والتفكير الذاتي بين وكالات الإعانة. وعادة ما يحدث هذا الأمر على المستوى القطري وعلى مستوى الإدارة العليا في المقر الرئيسي، ويفضل مراجعته على أساس منتظم.



الهدف الرابع: توجيه اتخاذ القرارات الاستراتيجية في المنظمة. والغرض من ذلك هو تقييم الطبيعة المتغيرة للحوادث، وفهم بيئات العمل الأكثر تحدياً، وكشف المنظمة للمخاطر، وتحديد أفضل الاستجابات الاستراتيجية. ويحدث ذلك على المستوى القطري والإقليمي والمقر الرئيسي خلال فترة معقولة من الزمن بعد وقوع حادث أمني وأثناء مراحل التخطيط والبرمجة.



من المهم النظر إلى هذه الأهداف الأربعة على أنها جزء من هدف أشمل، تتمثل في التقليل من المخاطر الأمنية للمنظمة، وبالتالي تحسين وصولها إلى السكان المحتاجين.

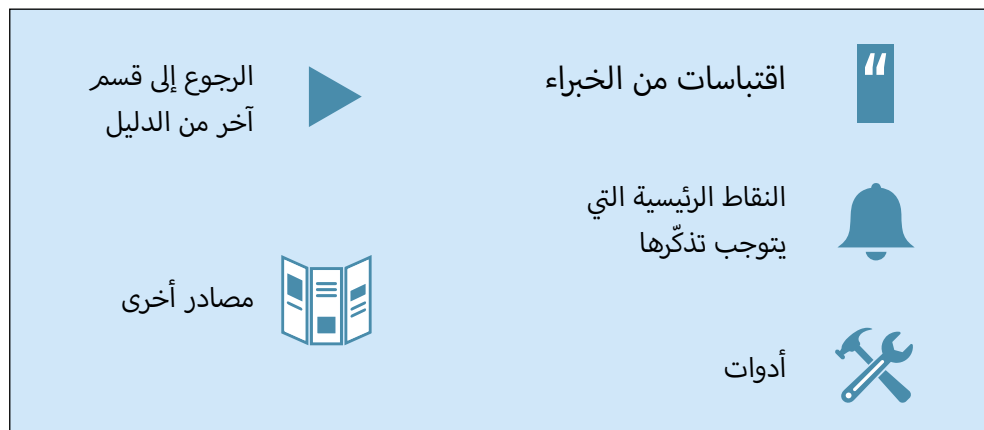
يقدم كل قسم توجيهات بشأن الخطوات الرئيسية وكيفية وضع معايير وتصنيفات محددة جيداً تمكن المنظمات من تحليل البيانات بسهولة أكبر. ومتى يتم تبادل البيانات بين الوكالات، والتعاريف الموحدة والإجراءات الأخلاقية ضرورية.

إن المنظمات وموظفيها مدعوون إلى:

- استخدام الدليل للحصول على فهم أقوى لإدارة معلومات الحوادث الأمنية وما هي الخطوات الرئيسية التي يمكن اتباعها لتحسين إدارة المخاطر الأمنية الشاملة لمنظمتكم.
- استخدام الأدوات المتوفرة في نهاية هذا الدليل لتحسين نظام إدارة معلومات الحوادث الأمنية في منظمتهم. ويمكن إيجاد قائمة هذه الأدوات هنا.
- استخدام الأداة 1: شبكة التحليل الذاتي لإدارة معلومات الحوادث الأمنية لتقييم احتياجات إدارة معلومات الحوادث الأمنية في منظمتهم. ويمكن القيام بهذه المراجعة على فترات منتظمة. وبعد مرور فترة زمنية محددة، ينبغي للمنظمات أن تنظر في التقدم الذي أحرزته منذ التقييم الذاتي الأولي.

يمكن الاطلاع على الدليل الكامل أو يمكن إعطاء الموظفين المعنيين أجزاءً أو أدوات محددة منه. إن الأهداف الرئيسية الأربعة المبينة في هذا الدليل مختلفة عن بعضها البعض ولكنها مترابطة في الوقت نفسه؛ حيث أن تحسين الممارسات لتحقيق هدف واحد من شأنه أن يساعد المنظمة على تحقيق الأهداف الأخرى، وتسهم هذه الأهداف ككل في التأهب والاستعداد التشغيلي والأمن التنظيمي.

ولمزيد من السهولة، سيتم استخدام هذه الرموز لتوجيه المستخدم ومساعدته على تحديد نوع الموارد المقدمة:



من أجل سهولة التصفح، يتم ربط الأدوات ومراجع الموارد الخارجية، فضلاً عن الحالات المرجعية لأقسام أخرى داخل الدليل باستخدام الارتباطات التشعبية (hyperlink).

يتم ربط المربعات على الجانب الأيمن من كل صفحة مع بداية الفصل المحدد.

يتم ربط المراجع الواردة في الهوامش باستخدام الارتباطات التشعبية مع "قائمة المراجع" في نهاية الدليل.

التعاريف الرئيسية

التحليل: عملية تحويل الحقائق والأرقام وغيرها من الأشياء غير المنظمة إلى معلومات ذات معنى يمكن استخدامها لأغراض متعددة، مثل المساعدة في اتخاذ القرارات.

المهارات التحليلية: وهي القدرة على تصوّر أو توضيح أو صياغة أو حل المشكلات المعقدة وغير المعقدة على حد سواء، بما في ذلك القدرة على تطبيق التفكير المنطقي لتفكيك المشكلات المعقدة إلى أجزائها المكونة.

الأزمة: هو الحدث الذي يتطلب استجابة أكبر من تلك الممكنة من خلال الإدارة أو الإجراءات الروتينية. وقد تتطلب الاستجابة مدخلات إضافية من الإدارة المتخصصة و / أو الإدارة العليا (على الأرجح يكون ذلك على مستوى المقر الرئيسي). وستصنف العديد من المنظمات الحادث الذي يتطلب الإدارة كحالة أزمة على أنه "حادث حرج".

البيانات: هي الحقائق والإحصائيات التي يتم جمعها لأغراض التحليل أو المرجعية، وهي معلومات في حالتها الخام أو غير المنظمة والتي تشير إلى أو تمثلها الشروط والأفكار أو الأشياء.

واجب الرعاية: وهو "مسؤولية أو التزام الشخص أو المنظمة قانونياً بتفادي الأعمال أو الامتناع عن الأعمال التي يمكن توقعها بشكل معقول، والتي قد تُعرض الآخرين للأذى¹. كما ينبغي على المنظمات أيضاً أن تأخذ في الاعتبار واجب العناية الأخلاقي²."

الحدث: حدوث أو تغيير مجموعة معينة من الظروف. وفي هذا الدليل، يتم استخدام "حدث" بالتبادل مع "حادث".

تدفق المعلومات الأفقي: تبادل المعلومات أفقياً فيما بين المنظمات وبين المنظمات وأصحاب المصلحة.

الحادث (incident): هي الأحداث التي تتعرض فيها سلامة الموظفين أو أمنهم للخطر؛ أو الأحداث التي تؤدي إلى إصابة أي طرف ثالث تابع أو غيره بأذى في سياق أنشطة المنظمة؛ وتعرض عقارات أو ممتلكات المنظمة إلى السرقة أو الضرر أو الخطر؛ حيث يكون هناك تضارب في إيصال المساعدة و / أو تعرض العمل المستقل لوكالة المعونة للخطر، بما في ذلك الضرر بالسمعة.

ملحوظة: قد تكون الحوادث تنظيمية (تمس بشكل مباشر المنظمة وقدرتها على تقديم المساعدة) بالإضافة إلى الأحداث الخارجية (التي تمس الآخرين خارج المنظمة). إن رفع التقارير حول كلا النوعين سيكون مفيداً في إدارة معلومات الحوادث الأمنية.

يمكن تقسيم الحوادث إلى فئات على النحو التالي:

الحوادث الحرجة (الخطيرة): وهي الحوادث التي تعطل العمليات العادية والروتينية. ويمكن أن تؤدي الحوادث الحرجة أو الخطيرة إلى الوفاة أو الإصابات الحرجة أو المرض الذي يهدد الحياة وهي تفعل استجابة المنظمة لإدارة الأزمات. وتميل هذه الأحداث إلى حدوث الاستجابة العاجلة.

¹ كيمب، إيه وميركالباخ، إم (2011)، هل يمكنك التعرض للمقاضاة؟ المسؤولية القانونية لمنظمات المعونة الإنسانية الدولية تجاه موظفيها. مبادرة إدارة الأمن

² كيمب، إيه وميركالباخ، إم (2016): واجب الرعاية: مراجعة أحكام قضية دينيس ضد مجلس اللاجئين النرويجي وآثارها. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

الحوادث الوشيكة: وهي الحوادث التي كادت أن تؤدي إلى حدوث ضرر أو إصابة أو خسارة للمنظمة أو موظفيها أو برامجها أو التي كادت أن تؤدي إلى حدوث إصابات بالغة، أو الوفاة، ولكنها لم تتسبب في نهاية المطاف إلا في إصابات أو أضرار أو خسائر طفيفة.

ملحوظة ١: يمكن النظر إلى العوائق الإدارية (على سبيل المثال العوائق والحواجز البيروقراطية المبالغ فيها، وصعوبة منح التأشيرات أو تصاريح السفر للمناطق المتضررة من الكوارث، وما إلى ذلك) والإبلاغ عنها على أنها حوادث، لأنها يمكن أن توفر أيضاً معلومات عن السياق.

الحوادث العشوائية (accident): الأحداث العشوائية التي تؤدي إلى وقوع ضرر أو خسارة للمنظمة أو موظفيها أو برامجها. وعلى النقيض من ذلك، فإن "الحوادث" تدفعها إرادة الأفراد للتسبب في ضرر للأشخاص أو الكيانات، أو الاستيلاء على الأصول أو تعطيل تسليم المعونة والمساعدة، إما عن طريق الاستهداف المباشر لتلك الوكالة أو موظفي الوكالة، أو غير ذلك. وينبغي الإبلاغ عن كافة الحوادث أو الأحداث بغض النظر عن طبيعتها سواء كانت أمنية أم لا. ومع ذلك، عندما يشير هذا الدليل إلى "الحوادث" أو "الحوادث الأمنية" فإنه يشير في المقام الأول إلى الأحداث المتعلقة بالأمن. ومع ذلك، يتطلب من القارئ أن يضع في الاعتبار أن النماذج والأدوات والإرشادات الواردة في هذه الوثيقة توفر أيضاً توجيهات مفيدة في إدارة المعلومات المتعلقة بالحوادث، مثل حوادث المرور على الطرق.

المعلومات: ما يتم نقله أو تمثيله بترتيب أو تسلسل معين للبيانات. وهو الإبلاغ عن أو استقبال المعرفة أو الذكاء. يتم تحويل البيانات الخام إلى معلومات عن طريق التحليل.

إدارة المعلومات: وهو المصطلح الشامل المستخدم لوصف السياسات والمبادئ التوجيهية المصممة من أجل:

- تنظيم أنواع المعلومات التي تقوم المنظمة بجمعها وتخزينها والإبلاغ عنها،
- الحد من المخاطر التي يتعرض لها الموظفون والمنظمات المتأصلة في هذه العمليات،
- ضمان قدرة الأشخاص المناسبين على الحصول على هذه المعلومات في الوقت المناسب³

المسؤول عن المعلومات: هو الفرد (أو مجموعة الأفراد) الذين لديهم القدرة على إنشاء وتحرير وتعديل وتبادل وتقييد الوصول إلى البيانات.

أمن المعلومات: "الحفاظ على سرية ونزاهة وتوافر المعلومات ... ويمكن أيضاً إشراك خصائص أخرى، مثل الصحة والمساءلة وعدم التنصل والموثوقية".⁴

الموظفين (العاملين): الموظفون والمتطوعون وأي أفراد آخرون يندرجون تحت مظلة المنظمة بما في ذلك المستشارين والشركاء والزوار وغيرهم.

المخاطر: "أثر عدم اليقين على الأهداف".⁵ ويمكن أن تكون المخاطر أيضاً احتمال وجود تهديد يؤثر على المنظمة والأثر الذي سترتب عنه إذا ما حدث.

3 آير. آر (2010). تحدي إدارة المعلومات: موجز عن أمن المعلومات في مجال المنظمات الإنسانية غير الحكومية. EISF

4 ISO/IEC 27000:2014

5 ISO 31000:2009

تقييم المخاطر: وهي عملية تحديد التهديدات على السلامة والأمن التي قد تؤثر على الموظفين والأصول والبرامج وتحليل احتمالية حدوثها وأثرها، وذلك من أجل تحديد درجة المخاطر المعنية.

السلامة: التحرر من المخاطر أو الضرر الناجم عن الأفعال أو الأحداث أو المخاطر غير المقصودة أو العرضية.

الأمن: التحرر من المخاطر أو الأضرار الناجمة عن أعمال العنف المتعمدة أو العدوان و / أو الأعمال الإجرامية ضد موظفي الوكالة أو أصولها أو ممتلكاتها.

معلومات الحوادث الأمنية: البيانات والمعلومات المتعلقة بحادثة أو سلسلة من الأحداث الأمنية المحددة.

إدارة معلومات الحوادث الأمنية: جمع المعلومات والإبلاغ عنها وتسجيلها وتحليلها ومشاركتها واستخدامها (بما في ذلك البيانات) المرتبطة بحادث أمني، وذلك مع وضع هدف شامل يتمثل في الحصول على إمكانية الوصول إلى المساعدة دون أية معوقات عن طريق تحسين إدارة المخاطر الأمنية التنظيمية.

أمن المعلومات: تركز الإدارة الجيدة للممتلكات والحلول التقنية على التدريب الفعال للموظفين والموارد الكافية، مما يشكل ثقافة قوية لإدارة المعلومات يقوم فيها الموظفون بتنفيذ سياسات الأمن بشكل تلقائي تقريباً.

إطار إدارة المخاطر الأمنية: مجموعة السياسات والبروتوكولات والخطط والوكالات والمسؤوليات التي تدعم الحد من المخاطر الأمنية للموظفين والبرامج والمنظمة.

العنف الجنسي: أي فعل جنسي، أو محاولة الحصول على فعل جنسي، أو تعليقات جنسية غير مرغوب فيها أو أوجه تقدم، أو القيام بممارسة حركة جنسية لشخص ما، باستخدام الإكراه أو التهديد بالإيذاء أو القوة البدنية، من قبل أي شخص بغض النظر عن علاقته بالضحية، في أي مكان، بما في ذلك ولكن لا تقتصر على المنزل والعمل. ويتخذ العنف الجنسي أشكالاً كثيرة، بما في ذلك الاغتصاب والاسترقاق الجنسي و / أو الاتجار، والحمل القسري، والتحرش الجنسي، والاستغلال الجنسي و / أو الإيذاء، والإجهاض القسري.⁶

تصنيف الحوادث: تصنيف الحوادث وفقاً لأنواع عامة.



الأداة 2: تصنيف الحوادث، تقترح هذه الأداة تصنيفاً تستخدمه Insecurity insight في تحليلاتها وهو قائم على تصنيفات وأنماط تستخدمها العديد من المنظمات.

التدفق العمودي للمعلومات: المعلومات التي تنتقل صعوداً وهبوطاً ضمن هيكل المنظمة. وعندما يقوم أحد أصحاب المصلحة في منطقة ما بجمع تقارير الحوادث وإرسالها إلى المقر لإجراء تحليل أكثر تفصيلاً، فهذا يعتبر تدفقاً تصاعدياً للمعلومات. وعند إجراء تحليل المعلومات واستخلاص الاستنتاجات، يمكن نشرها في اتجاه تنازلي للموظفين الميدانيين.

⁶ Inter-Agency Standing Committee (IASC). (2015). Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing risk, promoting resilience and aiding recovery.

التعرف على إدارة معلومات الحوادث الامنية



يزودنا هذا القسم بمقدمة عن إدارة معلومات الحوادث الأمنية ويناقش كيفية تناسبه مع المجالات الأوسع للمخاطر الأمنية، من أجل تعزيز الحماية من الحوادث الأمنية واتخاذ التجهيزات المناسبة لها.

- ▶ ما هي إدارة معلومات الحوادث الأمنية؟
- ▶ التحديات الرئيسية لإدارة معلومات الحوادث الأمنية
- ▶ إدارة المخاطر الأمنية وإدارة معلومات الحوادث الأمنية
- ▶ المهارات الأمنية للموظفين وإدارة معلومات الحوادث الأمنية
- ▶ أمن المعلومات
- ▶ إدارة الحوادث وإدارة معلومات الحوادث الأمنية: فوائد التأهب والجاهزية التنظيمية
- ▶ واجب الرعاية

الأدوات ذات الصلة:

- ▶ الأداة 1: شبكة التقييم الذاتي لإدارة معلومات الحوادث الأمنية

ما هي إدارة معلومات الحوادث الأمنية؟

إدارة معلومات الحوادث الأمنية هي جمع المعلومات وتسجيلها وتحليلها وإعداد التقارير عنها ومشاركتها واستخدام المعلومات (بما في ذلك البيانات) المرتبطة بحدث أمني أو سلسلة من الأحداث الأمنية.

تعمل الإدارة الفعالة لمعلومات الحوادث الأمنية على تعزيز قدرة المنظمات غير الحكومية على مشاركة واستخدام المعلومات المتعلقة بالحوادث داخل المنظمة وخارجها بطريقة آمنة ومناسبة لتسهيل عملية اتخاذ قرارات جيدة ومناسبة على مختلف مستويات المنظمة.

يجب ألا تقتصر عملية إدارة معلومات الحوادث الأمنية على حالات الوفاة أو الإصابة أو الاختطاف وألا تقتصر على البلدان الأكثر تضرراً. ومن المفيد أن يتم الإبلاغ عن جميع الحوادث التي تؤثر على عملية إيصال المساعدات وأن يتم تحليلها من قبل المنظمات. وهذا يساعد المنظمات على (من بين العديد من الأمور):

- تبني إجراءات مناسبة وفعالة على الفور من أجل الحد من الخطر، مما يجعل المدراء على دراية بشكل سريع عن الحادث لكي يتمكنوا من تقديم الدعم اللازم للموظفين المتضررين أو المشاركين في حادث ما؛
- تحسين تحليل السياق عن طريق تحديد المسارات والأنماط الناشئة والتي يتم بناءً عليها اتخاذ القرارات التشغيلية المناسبة من قبل الإدارة العليا؛
- إبلاغ الجهات ذات العلاقة بالتهديدات والمخاطر المحتملة حتى يتمكنوا من وضع تدابير مناسبة لتفادي المخاطر؛
- الاحتفاظ بسجل كامل للحوادث الأمنية في المنظمة.

الخطوات الأساسية في إدارة معلومات الحوادث الأمنية هي:

- إعداد التقارير.
- تسجيل المعلومات.
- تحليل البيانات التي تم جمعها خلال الحادث.
- مشاركة المعلومات (داخل المنظمة وخارجها).
- اتخاذ القرارات في الميدان، والتي تكون عادة كاستجابة فورية لحادث ما.
- اتخاذ القرارات على المستوى القطري أو الإقليمي، باستخدام معلومات عن الحوادث المبلّغ عنها من أجل تحسين إجراءات الأمن عن طريق تطبيق الدروس المستفادة.
- تحليل بيانات الحوادث لتحديد الاتجاهات والأنماط.
- استخدام تحليل الاتجاهات لتعزيز التحليلات السياقية، وتقييم المخاطر واتخاذ قرارات مناسبة لتحديد أفضل التدابير الأمنية لتحسين الأمن في المنظمة.
- اتخاذ القرارات الاستراتيجية في المقر الرئيسي والتي تشمل على استخدام تحليلات الاتجاهات التي تم تحديدها من الحوادث التي تم التبليغ عنها لاتخاذ قرارات مناسبة على نطاق المنظمة عالمياً.

ستتم مناقشة هذه الخطوات الرئيسية بمزيد من التفاصيل في "الفصل الثاني: الأهداف الأربعة لإدارة معلومات الحوادث الأمنية".

التحديات الرئيسية لإدارة معلومات الحوادث الأمنية

يمكن ربط التحديات التي تواجه إدارة معلومات الحوادث الأمنية بالعوامل الفردية والتنظيمية على حد سواء.

قلة التبليغ عن الحوادث

لا يتم الإبلاغ أو تسجيل العديد من الحوادث. وغالباً ما يتم الإبلاغ عن الحوادث غير الحرجة أكثر من الحوادث الوشيكة على الرغم من قلة الإبلاغ عن كليهما. وهذا لا يعني أن هذه الأنواع من الحوادث لا تقع، بل أنها تحظى باهتمام أقل بالمقارنة مع الحوادث الأخرى التي تحتوي على مخاطر أكبر بكثير في البيئات الأكثر عدائية.

يمكن أن تكون الحوادث غير الحرجة في البيئات الخطرة مؤشراً على تدهور الوضع وتزايد التوتر، وينبغي إبلاغ المدير المباشر أو منسق الشؤون الأمنية، وإجراء مراجعة السياق وتحليل المخاطر في المنظمة.

الاختلافات في التعاريف

يمكن أن تختلف التصورات حول ما يشكل حادثة اختلافاً كبيراً بين المنظمات، وكذلك بين الأفراد داخل المنظمة نفسها. وقد ترى إحدى المنظمات غير الحكومية أن إطلاق النار القصير خلال الليل يستحق الإبلاغ، في حين أن منظمة أخرى قد لا ترى ذلك ضرورياً في حال كان إطلاق النار أمراً شائعاً في البيئة التشغيلية التي تعمل فيها. وبالمثل، قد يكون لدى الموظفين الدوليين والوطنيين وجهات نظر مختلفة بشأن ما يمثل حادثاً يحتاج إلى الإبلاغ.



يتعين على المدراء إعطاء توجيهات وإرشادات واضحة حول ما يشكل حادثاً يتطلب الإبلاغ في مواقع معينة، وذلك لضمان استخدام نهج متسق في كامل المنظمة.

يجب أن يكون لدى جميع الموظفين فهم مشترك للمصطلحات المرتبطة بإدارة معلومات الحوادث الأمنية حتى يتمكنوا من التواصل بشكل فعال داخلياً وخارجياً. ويشكل عدم الاتساق في استخدام المصطلحات مشكلة بالنسبة للتحليل. على سبيل المثال، قد تشير الوثائق الأمنية إلى حوادث ذات صلة أو حوادث مشابهة مثل "السطو" و "السرقه" دون التمييز بينها. ومن أجل تجميع ومقارنة البيانات من مختلف الوكالات، وكذلك عبر مختلف البلدان التي تعمل فيها المنظمة، من الضروري أن يكون هناك تعريفات مشتركة.

المخاوف المتعلقة بالسمعة

يشير الحادث الأمني إلى أن شيئاً ما قد حدث بشكل خاطئ. وعلى الرغم من أن منظمات الإغاثة نادراً ما تكون مسؤولة عن وقوع حادث أمني، إلا أنها قادرة في كثير من الأحيان على تحديد العناصر المتعلقة بإجراءاتها أو سلوك الموظفين التي قد تكون ساهمت بأي شكل من الأشكال في جعل الحدث ممكناً أو أثرت على نتائج الحادث. ونظراً للأثر المحتمل للمعلومات المتعلقة بالحوادث التي قد تحدث على سمعة المنظمة، فقد تفضل العديد من المنظمات غير الحكومية عدم مشاركة تفاصيل ما حدث من خطأ، ولا سيما مع الجهات الفاعلة الخارجية.

“

إن التعلم من الحوادث الوشيكة والأخطاء يعتبر من الممارسات القياسية في الصناعات الأخرى. ففي قطاع الطيران، على سبيل المثال، تلتزم جميع الشركات بالإبلاغ عن أي فشل - سواء كان ذلك تقنياً أو بشرياً - وقد تم استخدام هذه المعلومات في وضع التوجيهات والإرشادات التي جعلت من الطيران من أكثر وسائل النقل أماناً اليوم.⁷ ولذلك، فإن مشاركة الدروس المستفادة من الأخطاء التي تحدث داخل منظمة غير حكومية واحدة يمكن أن يساعد المجتمع الإنساني والإنمائي ككل.



تستفيد المنظمات عندما تحدد بشكل واضح على مستوى السياسة متى ينبغي تبادل المعلومات المتعلقة بالإبلاغ عن الحوادث داخلياً وخارجياً، وكيفية ضمان السرية عند الاقتضاء، والخطوات الواجب اتباعها من أجل إدارة المعلومات بحكمة.

العبء الإداري

إن توثيق الحوادث يستغرق وقتاً طويلاً ويحتاج إلى موارد بشرية هامة. ومع ذلك، إذا تمكنت المنظمات من وضع نظام فعال، فإن بإمكانها التخفيف من العبء الإداري، وبالتالي تجنب الموظفين قضاء الوقت في البحث عن التعليمات المتعلقة بكيفية تسجيل الحوادث والإبلاغ عنها. إن توفير الأدوات والنماذج يساعد في جعل التسجيل والإبلاغ أكثر اتساقاً في جميع أنحاء الوكالة كما يجعله أقل مشقة أيضاً وبالتالي أكثر احتمالاً للحدوث...



ينبغي شرح إجراءات وسياسة إدارة معلومات الحوادث للموظفين وإبقائها بسيطة قدر المستطاع.

الثقافة التنظيمية

يتحمل المديرون، على أي مستوى، مسؤولية تبادل المعلومات رأسياً داخل المؤسسة، مثل تبادل المعلومات مع المدير المباشر أو مع المقر، ولكن غالباً ما لا يتم تبادل المعلومات المناسبة لمجموعة متنوعة من الأسباب. حيث لا يشارك المديرون (المحليين والدوليين) المعلومات رأسياً خوفاً من رد فعل سلبي من جانب الإدارة، أو من الاعتراف بمخالفة السياسة، أو "لحفظ ماء وجههم". وبالرغم من أن الموظفين المحليين هم من يتكبد العبء الأكبر من حيث الوفيات والإصابات في المنظمات غير الحكومية، إلا أنهم يشعرون أن سمعتهم ستأثر سلباً في حال أبلغوا عن حادث ما. ويخشى الكثيرون من أن يعاقبوا من خلال تقليل فرصهم في الترقية أو، في أسوأ الحالات، فقدان عملهم.

يمكن الكشف عن أي سلوك سيء أو خرق للإجراءات الأمنية (أو مدونة قواعد السلوك) من خلال تحليل الحوادث. ويمكن للمنظمة أن تقرر ما إذا كانت هناك حاجة إلى اتخاذ تدابير تأديبية. وكثيراً ما يخضع هذا السؤال للمناقشات داخل المنظمات التي تعتبر مسألة العقوبات عاملاً إضافياً لعدم الإبلاغ. وستستفيد المنظمات من اتخاذ موقف واضح بشأن ذلك وتحقيق التوازن بين هذه الشواغل والمخاوف.

ويجب أن تكون الاستجابة للانتهاكات في الإجراءات الأمنية متنسقة. حيث أن السياسات الأمنية ستكون غير فعالة إذا ما اخترقتها الإدارة العليا أو موظفي الأمن دون أية عواقب.

التواصل بين الوكالات

قد يكون من الصعب تبادل المعلومات الأمنية، بما في ذلك الإبلاغ عن الحوادث والأوضاع بين المنظمات. ويتم مناقشة التغلب على التحديات الرئيسية التي تواجه التعاون، مثل السرية والثقة وإدارة المعلومات، بمزيد من التفصيل في "الهدف الثالث: فهم السياق التشغيلي"

إدارة المخاطر الأمنية وإدارة معلومات الحوادث الأمنية

تشمل إدارة المخاطر الأمنية أن تضع المنظمة السياسات والبروتوكولات والخطط والاليات وأن تحدد مسؤوليات الموظفين لدعم الوصول الأفضل من خلال تحسين الأمن التنظيمي. ويعرض الرسم البياني أدناه، الذي يوضح إطاراً لإدارة المخاطر الأمنية على نطاق المنظمة، مختلف الركائز التي تمكن الإدارة الفعالة للمخاطر الأمنية.⁸



في حين يتم تسليط الضوء على مراقبة الحوادث بوصفها ركيزة أساسية من أركان إطار إدارة المخاطر الأمنية، يمكن لمعلومات الحوادث الأمنية المدارة جيداً أن تغذي وتعزز جميع العناصر الرئيسية لإدارة المخاطر الأمنية.

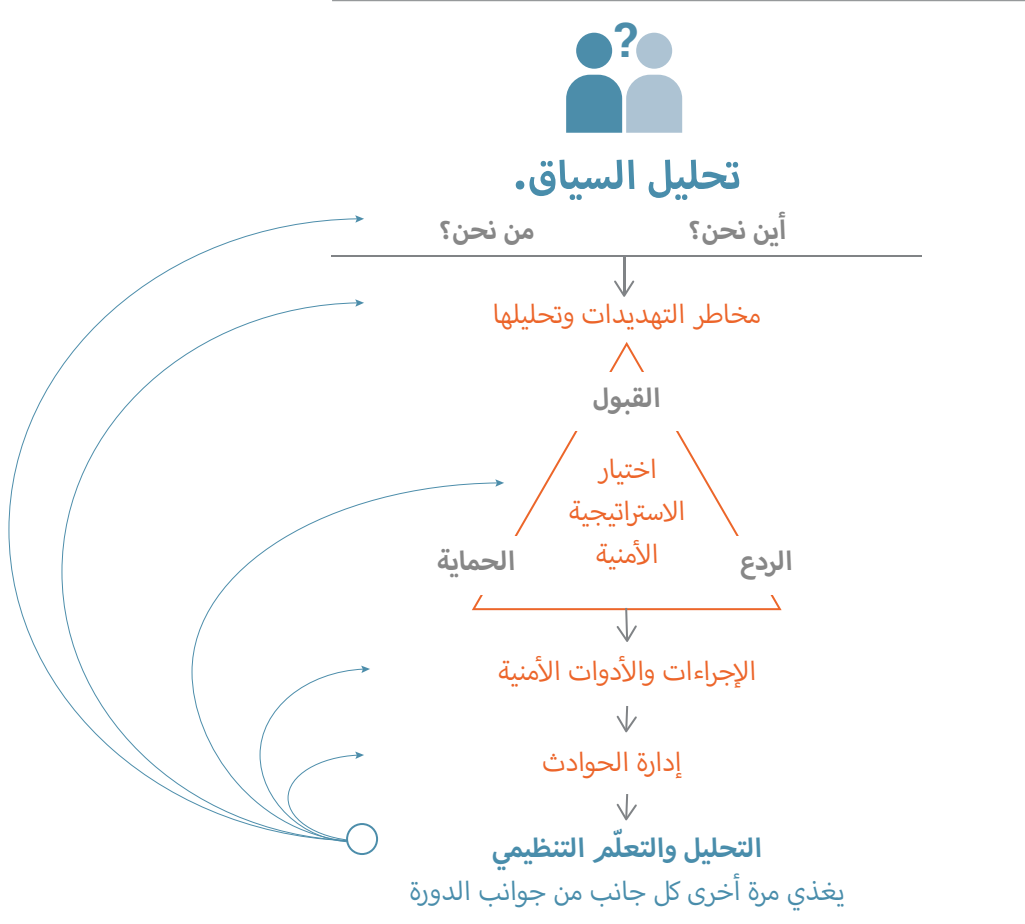
ابتداءً من ضمان إنشاء هيكل إدارة الأزمات في الوقت المناسب بعد وقوع حادث حرج وصولاً إلى استخدام معلومات الحوادث غير الحرجة لاطلاع الموظفين عن مخاطر السفر، فإن إدارة معلومات الحوادث الأمنية تعتبر عنصراً بالغ الأهمية في الإدارة الجيدة للمخاطر الأمنية.



“

“تعتبر الحوادث مناسبات مثالية وفرصة للتعلّم والتحسين. وينبغي لتحليل الحوادث أن يغذي إطار إدارة الأمن برمته”

يمكن لمنسقي شؤون الأمن والمحللين الأمنيين استخدام معلومات الحوادث الداخلية وغيرها من المصادر لفهم السياق في مواقع مختلفة. وينبغي الاستفادة من المعلومات التي يتم استخراجها وتحليلها بعد وقوع الحادثة في تحليل المخاطر في المنظمة من خلال إبراز التهديدات ومواطن الضعف في السياق المعين. كما يمكن استخدامها في مراجعة إجراءات التشغيل الموحدة وخطط الطوارئ، ويمكن أن تستخدم أيضاً كأدلة داعمة جيدة لإحداث تغييرات في السياسات.



كفاءات الموظفين الأمنيين وإدارة معلومات الحوادث الأمنية

تُدرج الهيئة المعنية بالخبراء الأمنيين للمنظمات غير الحكومية واسمها الرابطة الدولية للسلامة والأمن في المنظمات غير الحكومية (INSSA)، إدارة المعلومات باعتبارها أحد مجالات اختصاصها الرئيسية للموظفين المسؤولين عن الأمن على الصعيد القطري والإقليمي والعالمي والاستراتيجي.

سيدعم الموظفون في كل مستوى أنظمة وإجراءات إدارة المخاطر الأمنية الشاملة للمنظمة، ومن الأهمية بما كان أن يتم:

- تحديد وتمييز المسؤوليات الأمنية للموظفين في كل مستوى،
- ضمان حصول الموظفين على الدعم والتدريب الكافيين لتأدية المسؤوليات المنوطة بهم بما يتماشى مع المستوى الذي يعملون فيه



انظر وحدة إدارة الأشخاص في دليل EISF "الأمن في العمل" "Security to Go" للمزيد من المعلومات حول الترابط بين إدارة الأشخاص والأمن التنظيمي

أمن المعلومات

في سياق إدارة معلومات الحوادث الأمنية، من المهم أن تضمن المنظمة أن وسائل الاتصال المستخدمة في إعداد التقارير، وجمعها، وتحليلها، وتبادلها، وتخزينها آمنة.



كثيراً ما يتعين على المنظمات أن توازن بين الحاجة إلى إدارة المعلومات المتعلقة بالحوادث الأمنية والقيود المتعلقة بالميزانية. ومع ذلك فإنه من المهم معالجة أمن البيانات، أيًا كانت الموارد المالية المتاحة. لتحليل أجهزة الراديو والهواتف المحمولة والأقمار الصناعية ورسائل البريد الإلكتروني والجوانب الفنية الأخرى لإدارة المعلومات، يرجى الرجوع إلى دليل GPR8 الخاص بمنظمة ODI للاطلاع على الفصل الخاص بالاتصالات السلكية واللاسلكية ودليل "Security to Go" EISE.

إن الواجب القانوني والأخلاقي للمنظمات غير الحكومية لضمان سرية المعلومات أمرٌ بالغ الأهمية، لا سيما إذا كانت "البيانات شخصية" - أي المعلومات تتعلق بشخص محدد أو يمكن التعرف عليه. حيث أن الفشل في وضع أو تنفيذ سياسات إدارة المعلومات يمكن أن يكون له تداعيات سلبية على الموظفين والمنظمات، ويمكن أن تؤدي إلى اتخاذ إجراءات قانونية والتعويض.

“

يتمثل جزءٌ من إدارة معلومات الحوادث الأمنية الجيدة في تحقيق التوازن الصحيح في السياق المحدد بين فوائد جمع وتسجيل ونقل مجموعات معينة من المعلومات وبين المخاطر التي تنطوي عليها هذه الإجراءات.”

ينبغي للمنظمات غير الحكومية تعزيز ثقافة إدارة المعلومات من خلال التأكد أن أمن المعلومات جزءٌ لا يتجزأ من سياسات وإجراءات إدارة المخاطر على نطاق أوسع، وضمان إدماجها بسلاسة في التفكير التنظيمي والبرمجي. ويمكن التخفيف من معظم المخاطر من خلال التوعية بها، والحس العام والانضباط الجيد: المشار إليها هنا باسم "الإدارة الجيدة". وتغطي الإدارة الجيدة الأعمال المكتبية والنسخ المطبوعة وكذلك أمن تقنية المعلومات - حيث أن أفضل تقنيات أمن تقنية المعلومات في العالم لن تحول دون ترك الموظفين للوثائق على مكتبهم ليلاً أو وضعهم ووثائق حساسة في صناديق القمامة دون تقطيعها.



أمن المعلومات ليس تحدياً يمكن لإدارات وأقسام تقنية المعلومات معالجته لوحدها. تركز الإدارة الجيدة للممتلكات والحلول التقنية على التدريب الفعال للموظفين والموارد الكافية، مما يشكل ثقافة قوية لإدارة المعلومات يقوم فيها الموظفون بتنفيذ سياسات الأمن بشكل تلقائي تقريباً.

لضمان أمن المعلومات الجيد في إدارة معلومات الحوادث الأمنية، يتعين على المنظمات معالجة المسائل الرئيسية التالية على كافة المستويات وفي كل مراحل جمع المعلومات والإبلاغ عنها وتسجيلها وتحليلها واستخدامها ومشاركتها:

- **الأمن المادي:** حماية أجهزة الحاسوب، والمرافق المكتبية وأصول المنظمة من الظروف والأحداث المادية التي قد تتسبب في أضرار أو خسائر جسيمة بما في ذلك السرقة والحرائق والكوارث الطبيعية.
- **الأمن الرقمي:** حماية الملفات الإلكترونية المخزنة على أجهزة الكمبيوتر - من الهواتف المحمولة وأجهزة المساعد الرقمي الشخصي إلى أجهزة USB وأجهزة الحاسوب - من الوصول غير المصرح به والفساد والخسارة وسوء الاستخدام أو التدمير. وينبغي دائماً مراعاة التدابير الأمنية الرقمية الأساسية، مثل حماية حسابات المستخدمين، وشبكات الإنترنت اللاسلكية، والوثائق الحساسة.

- **إمكانية الوصول:** تصنيف المعلومات والموظفين بحيث لا يمكن الوصول إلى المعلومات إلا من قبل الموظفين الذين يشغلون مناصب أو أدوار ذات صلة أو الذين لديهم ما يكفي من الأقدمية في المنظمة. (انظر "فئات المعلومات" في الهدف الثالث)
- **النسخ الاحتياطية:** المبادئ التوجيهية المتعلقة بكيفية ووتيرة تكرار النسخ الاحتياطية للملفات، مع ضمان إبقاء وقف انقطاع البرنامج إلى أدنى حد ممكن، نظراً لأن خطر تلف أو خسارة الأجهزة لا يمكن التخلص منه نهائياً.
- **التخلص من المعلومات وتدميرها:** مبادئ توجيهية واضحة حول كيفية ووقت تدمير المعلومات (بشكلها المادي والرقمي)، مع العلم بأنه ينبغي القيام بذلك بسرعة في بعض الأحيان. في البيئات ذات التهديدات العالية، ولا سيما تلك التي يشتهر في وجود رقابة متطورة عليها، ربما لا يمكن جمع أنواع معينة من المعلومات وتسجيلها على الإطلاق. بالإضافة إلى ذلك، ينبغي فصل إدارة المعلومات الحساسة بشكل واضح عن إدارة المعلومات الروتينية. وهكذا، إذا كان السياق المتدهور يفرض تدميراً سريعاً للمعلومات الحساسة، فسيكون من الممكن تحديد الاحتياجات التي تدمر بسرعة.
- **أمن الاتصالات:** ينبغي أن تحدد سياسة إدارة المعلومات كيفية التواصل في بيئات معينة. قد تكون المعلومات أكثر عرضة للإصابة عندما يتم إرسالها: إذ أن الراديو غير آمن، ويمكن أن يتم توصيل المكالمات الهاتفية، ورسائل البريد الإلكتروني التي يتم اعتراضها، وما إلى ذلك ...

انظر دليل GPR8 الخاص بمنظمة ODI للاطلاع على الفصل الخاص بأمن الاتصالات

عدّة الأمان (Security-in-a-box)

تعتبر أدوات وتكتيكات الأمن الرقمي القوية من المكونات الرئيسية لأمن المعلومات. أنجز مشروع عدّة الأمان "Security-in-a-box" بشكل مشترك بين كل من Front Line Defenders و Tactical Technology Collective، بالتعاون مع شبكة ممتدة من النشطاء المدربين والخبراء بمواضيع الأمن الرقمي حول العالم، مما أدى إلى تطوير أدلة مجتمعية تقدم مشورة مصممة خصيصاً بشأن الأدوات والتكتيكات ذات الصلة باحتياجات فئات معينة من الأفراد. وهي تغطي المبادئ الأساسية لمنصات الشبكات الاجتماعية والهواتف المحمولة، بما في ذلك تقديم المشورة بشأن كيفية استخدام هذه الشبكات بشكل أكثر أماناً. توفر "عدّة الأمان" (Security-in-a-box) والأدوات التكتيكية إرشادات خطوة بخطوة حول كيفية تثبيت واستخدام البرامج والخدمات الأمنية الرقمية الأكثر أهمية (هذه الموارد متوفرة للتنزيل من موقعها على الويب).

إدارة الحوادث وإدارة معلومات الحوادث الأمنية: فوائد التأهب التنظيمي

وعلى الرغم من أن إدارة الحوادث ليست محور هذا الدليل، إلا أننا نرى أن إدارة معلومات الحوادث الأمنية عنصر أساسي في إدارة الحوادث والتأهب التنظيمي.

إن التأهب التنظيمي يعني وجود إجراءات واضحة وتدريباً جيداً على إدارة الحوادث وإدارة معلومات الحوادث، مما يضمن أفضل الردود والاستجابات الممكنة للأحداث.

عادة ما تكون للحوادث، وخاصة الحرجة منها، الخصائص التالية:

- عنصر المفاجأة؛
- معلومات غير كافية؛
- تصعيد الأحداث التي قد تتجاوز الاستجابة؛

- المشكلات الهامة التي تؤدي إلى تدقيق خارجي؛
- فقدان السيطرة (الحقيقي أو المتصور)؛
- تعطيل عمليات صنع القرار العادية؛
- يميل الأشخاص المتأثرين مباشرة بهذه الحوادث إلى اعتماد التركيز قصير الأجل.

ما لم تكن الحوادث بالغة الأهمية، فإنها عادة ما تُعالج في إطار الإجراءات المحددة سلفاً. ولكن حتى الحوادث غير الحرجة يمكن أن تخلق الارتباك والذعر لمن ليسوا على استعداد للاستجابة لها.



الغرض من التأهب للحوادث الأمنية وإدارتها هو الحد من أثر الحوادث وتعزيز قدرة المنظمة على مواكبة الحاضر والتعلم للمستقبل.

في أعقاب الحادث، ستسعى المنظمة إلى:

- منع المزيد من الضرر وضمان صحة و / أو سلامة الضحية (الضحايا) والموظفين؛
- طمأنة الموظفين والعائلات بأن الاستجابة الفعالة والمسؤولة في طريقها إليهم؛
- ضمان الإدارة التنظيمية المستمرة، بالأخص في الحوادث الجارية، مثل الاختطاف؛
- ضمان استمرارية البرنامج؛
- الحد من خسارة الأصول (مثل الهواتف وأجهزة الكمبيوتر والمركبات، إلخ)؛
- استبدال الأصول المفقودة من خلال السرقة، إلخ.
- الوفاء بالمسؤوليات التنظيمية والحد من مخاطر الدعاوى والنزاعات القضائية؛
- تقديم الشكاوى (على سبيل المثال، إخطار السلطات المحلية المختصة بأي تهديدات موجهة ضد الموظفين)؛
- حماية صورة المنظمة وسمعتها؛
- تبادل المعلومات الهامة مع المنظمات غير الحكومية والشركاء الآخرين الذين قد يكونون أيضاً في خطر أثناء أو بعد وقوع حادث ما؛
- إعداد البيانات الصحفية و / أو إبلاغ وسائل الإعلام ومنافذ الأخبار الإنسانية / الإنمائية بمعلومات محددة تفيد الجمهور وتحمي المعنيين في الوقت نفسه.



إن الوعي الأمني وتحليل المخاطر والتهديدات ونقاط الضعف، والإجراءات الفعّالة، والحفاظ على تدريبات الأمن والسلامة، وبناء العلاقات القوية والتواصل مع الشركاء والوكالات الخارجية والتخطيط الجيد للطوارئ، كلها طرق استباقية للتعامل مع الحوادث وبالتالي الأزمات المحتملة.

يعد التأهب التنظيمي أمراً أساسياً للإدارة الفعالة للحوادث وإدارة معلومات الحوادث الأمنية.

على الرغم من أن السياسات لا يمكن أن تغطي كل الاحتمالات، إلا أن وجود خطط الطوارئ وخطط إدارة الحوادث، وتحديثها بانتظام للعمل من خلال سيناريوهات "ماذا لو؟"، فضلاً عن وجود إجراءات فعّالة لإدارة الأزمات، من شأنه أن يساعد بشكل كبير على إبقاء الوضع تحت السيطرة والحفاظ على عمليات آمنة.

“

في حال الأحداث الحساسة، مثل العنف الجنسي ضد أحد الموظفين، فإن الإجابة على السؤال "ماذا لو كان مرتكب العنف الجنسي موظفاً؟" في وقت مبكر سيساعد المنظمة وموظفيها على الاستعداد بشكل مناسب لمثل هذا الاحتمال".

- من الأهمية بما كان عند معالجة الحوادث الأكثر شيوعاً أن نفكر في أسئلة من قبيل:
- هل استجبتنا بالشكل المناسب وبأفضل ما لدينا للحدث (الأحداث) الأخيرة؟
 - ما الذي تعلمناه من الحوادث الوشيكة وهل قمنا بإجراء تغييرات على طريقة عملنا استناداً لما تعلمناه؟

عادة ما تُصح المنظمات قبل وقوع الحوادث وفي سياق الممارسات الجيدة بتضمين الإدارة الجيدة والقوية لمعلومات الحوادث في سياسات وإجراءات إدارة الحوادث الشاملة للمنظمة. ويمكن للمنظمة القيام بذلك من خلال:

- تطوير وتنفيذ ومراجعة السياسات والإجراءات التنظيمية بانتظام. مثل تلك المتعلقة بإدارة الحوادث والإبلاغ عنها، بما في ذلك الحوادث الوشيكة، أو معالجة حالات العنف الجنسي أو غيرها من الأحداث الحساسة بشكل خاص، أو أمن البيانات والموارد البشرية، إلخ
- اختيار نظام التسجيل والإبلاغ الذي يتيح الإدارة الآمنة لمعلومات الحوادث الأمنية داخل المنظمة وخارجها (انظر "الهدف الرابع - التسجيل المنهجي للحوادث" لمزيد من المعلومات حول أنظمة التسجيل).
- تحديد الهيكل وتحديد الأدوار والمسؤوليات في إدارة الحوادث وإدارة معلومات الحوادث لجميع الموظفين والمديرين ومنسقي شؤون الأمن المعينين، على كل مستوى من مستويات المنظمة ابتداءً من الميدان ووصولاً إلى المقر.
- تقييم وتحديد الموارد (الداخلية والخارجية) التي من شأنها تمكين المنظمة من الاستجابة بكفاءة وفعالية لأي حادث.
- توجيه وتدريب الموظفين الرئيسيين على إدارة الحوادث وإدارة معلومات الحوادث.

تستفيد المنظمات من تضمين الإجراءات الواضحة والتدريب على إدارة معلومات الحوادث ضمن الاستجابة الأوسع لإدارة الحوادث. وسيضمن ذلك جمع البيانات وتحليلها والإبلاغ عنها على نحو مناسب، ودعم الاستجابة الفورية للحدث، وأيضاً توفير فوائد طويلة الأجل للمنظمة.

انظر الأداة 1: شبكة التقييم الذاتي لإدارة معلومات الحوادث الأمنية هي عبارة عن نموذج للتقييم الذاتي يساعد المنظمات على تقييم نقاط القوة التي تتمتع بها ومواطن الضعف التي تعاني منها فيما يتعلق بإدارة معلومات الحوادث الأمنية.

واجب الرعاية

لماذا ينبغي على المنظمات الاهتمام بإدارة معلومات الحوادث الأمنية؟

لدى إدارة معلومات الحوادث الأمنية أربعة أهداف أساسية، والتي سيتم تناولها بتفصيل أكبر في الفصل الثاني: "الأهداف الأربعة لإدارة معلومات الحوادث الأمنية". ولكن الأساس المنطقي الشامل للإدارة الفعالة لمعلومات الحوادث الأمنية هو الحفاظ على سلامة الموظفين والبرامج والمنظمة. وتدعم الإدارة القوية للمخاطر الأمنية التنظيمية وصولاً أكبر إلى السكان المحتاجين، ولكنها تسمح أيضاً للمنظمات بصفتها صاحب العمل بالوفاء بواجب الرعاية تجاه الموظفين.

إن المنظمات غير الحكومية مُلزَمة بواجب رعاية قانوني (ويمكن القول بأنه واجب أخلاقي): "واجب الرعاية هو التزام قانوني يُفرض على فرد أو منظمة ويشترط منهم الالتزام بالرعاية المعقولة أثناء أداء الأعمال التي يمكن أن تشكل خطر الإضرار بالآخرين."¹⁰



يتطلب واجب الرعاية هذا تجاه الموظفين وغير الموظفين الذين تظهر لهم المنظمة درجة من الرقابة¹¹ أن تقوم المنظمات غير الحكومية بوضع نظم وعمليات قوية لإدارة المخاطر الأمنية.¹² ويشمل هذا الالتزام تنفيذ إدارة قوية لمعلومات الحوادث الأمنية.

سيدعم نظام إدارة معلومات الحوادث الأمنية الجيدة والفعل:

- فهماً أفضل لبيئة التهديدات ووضع تدابير وثيقة الصلة بالوقاية و/أو الاستباقية في معالجة الخاطر
- توثيق المعرفة التوظيفية، و
- معرفة وفهم أفضل للاتجاهات في القطاع والممارسات المجتمعية وبالأخص فيما يتعلق بالأمن.

في حالة حدوث تدهور كبير في مستوى الأمن، لاسيما في بيئات النزاع وما بعد النزاع، لا بد من أن تكون لدى المنظمات إجراءات تسمح لها بإظهار واجب الرعاية اتجاه كامل موظفيها والأشخاص الذين تتحمل مسؤوليتهم.

“

إذا اعتبرنا إدارة الحوادث أداة تعليمية هامة فيما يتعلق بإدارة المخاطر الأمنية، فإن إدارة معلومات الحوادث تصبح أفضل وسيلة لإظهار نضج المنظمة في تحليل الأحداث واتخاذ القرارات. ويمكن أن يكون جمع بيانات الحوادث التي تواجه المنظمة وتحليلها والإبلاغ عنها وتسجيلها على نحو شامل، وكيفية معالجتها، جزءاً حيوياً من دفاع المنظمة، في حالة وقوع حادث أدى إلى رفع قضية ضد المنظمة“

دراسة حالة: قضية دينيس ضد المجلس النرويجي للاجئين (NRC) (2015)

تعتبر قضية دينيس ضد المجلس النرويجي للاجئين (NRC) سابقة قانونية لواجب الرعاية في قطاع المساعدات الإنسانية. تسلط هذه القضية الضوء على بعض من الدروس الهامة التي يمكن الاستفادة منها في إدارة معلومات الحوادث الأمنية.

ملخص الحقائق:

في 29 من يونيو 2012، تعرض "ستيفن دينيس" وهو موظف لدى المجلس النرويجي للاجئين (NRC) وثلاثة من زملائه إلى الإصابة والاختطاف، بعد هجوم حدث خلال زيارة لكبار الشخصيات إلى أحد مخيمات اللاجئين في منطقة "داداب" بكينيا. بعد مرور أربعة أيام من الاختطاف، تم تحرير الرهائن إثر عملية مسلحة قامت بها السلطات الكينية والميليشيا المحلية. وبعد مرور ثلاثة أعوام عن هذه الحادثة، رفع دينيس دعوى في محكمة مقاطعة أوصلو ضد صاحب العمل السابق "المجلس النرويجي للاجئين"، طالباً فيها التعويض عن الخسائر الاقتصادية وغير الاقتصادية التي تعرض لها بعد الاختطاف. وبعد مراجعة دقيقة للحقائق المحيطة بهذه القضية، قضت المحكمة بأن المجلس النرويجي للاجئين (NRC) كان مهملاً للغاية وحكمت على المنظمة بتعويض دينيس.¹³

¹¹ الإنسانية الدولية تجاه موظفيها. مبادرة إدارة الأمن

¹² بما في ذلك المستشارين، والزوار، والمتطوعين، إلخ

كيمب، إيه وميركالباخ، إم (2016): واجب الرعاية: مراجعة أحكام قضية دينيس ضد مجلس اللاجئين النرويجي

¹³ وآثارها. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

كيمب، إيه وميركالباخ، إم (2016): واجب الرعاية: مراجعة أحكام قضية دينيس ضد مجلس اللاجئين النرويجي

وآثارها. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

الدروس المستفادة:

أشارت الخطة الأمنية للمجلس النرويجي للاجئين (NRC)، والتي اعتمدت على معلومات من مصادر وحوادث داخلية وخارجية، إلى أن خطر الاختطاف كان مرتفعاً. وأشار تحليلها أيضاً إلى أن الموظفين الدوليين معرضون لخطر الاختطاف أكثر من الموظفين المحليين. وقد استخدمت هذه المعلومات لوضع تدابير فعّالة لمعالجة المخاطر، بما في ذلك استخدام مرافقين مسلحين والحد من زيارات كبار الشخصيات إلى المنطقة. غير أن المنظمة قامت بتغيير الإجراءات الأمنية قبل زيارة كبار الشخصيات بناءً على نتائج إعادة تقييم المخاطر. واستناداً إلى الأدلة المقدمة، خلصت المحكمة إلى أن إعادة التقييم هذه كانت غير واضحة وغير مبررة. وبشكل أساسي، تم اعتبار المعلومات التي استند إليها القرار الأمني ضعيفة ومتناقضة مع المعلومات الأمنية القوية المسجلة سابقاً.

وقد دافعت المنظمة قائلة إن خطر الاختطاف قد تراجع بسبب عدم وقوع حوادث اختطاف في المنطقة خلال الشهور التسعة السابقة. غير أن المحكمة رأت أن عدم وجود حوادث لا يعني بالضرورة أن الخطر قد انتهى، بل يمكن أن يُعزى ذلك إلى تدابير قوية لمعالجة المخاطر، ومن بينها عدم وجود زيارات لكبار الشخصيات واستخدام مرافقين مسلحين من قبل جميع المنظمات غير الحكومية العاملة في داداب في ذلك الوقت. وقد كان من الممكن لتحليل أفضل لأسباب "عدم وقوع الحوادث" أن يساعد المجلس النرويجي للاجئين (NRC) على تحديد المستوى الفعلي - وليس المتصور - للمخاطر.

وبمجرد وقوع الحادث، قيّد المجلس النرويجي للاجئين (NRC) كمية المعلومات المتعلقة بالحادث التي شاركها مع الموظفين المتضررين والمشاركين. وقيل إن هذا النقص في الشفافية من جهة المنظمة قد لعب دوراً كبيراً في قرار دينيس برفع القضية ضدها.

لو أن إدارة المعلومات الأمنية كانت قوية بما يكفي في هذه الحالة فربما ساعدت في اتخاذ المنظمة قرارات أمنية مختلفة فيما يتعلق بزيارة كبار الشخصيات، مما كان سيحول دون وقوع الحادث.

لكن في حال وقوع الحادث، فإن توثيق المعلومات الأمنية القوية المستخدمة في اتخاذ القرارات الأمنية كان سيساعد المنظمة في الدفاع عن تلك القرارات.

وقد يكون من شأن اتباع نهج مختلف لتبادل المعلومات بعد الحادث أن يؤدي أيضاً إلى نقاش أقل شدة وأكثر انفتاحاً بشأن الفشل والدروس المستفادة بين المنظمة والموظفين المتضررين.



لقد وضعت منظمة Irish Aid مبادئ توجيهية لمساعدة المنظمات على إظهار التزامها بشكل أفضل فيما يخص الوفاء بالالتزامات القانونية لواجب الرعاية. وتهدف هذه المبادئ التوجيهية إلى تزويد المنظمات بتوجيهات حول كيفية الوصول إلى مستوى عالٍ من الاحتراف عند تحقيق أهداف مهمتها. ويرافق كل موضوع إجراءات رئيسية ومؤشرات وملاحظات التوجيهية. وينبغي أن يساعد الالتزام بهذه المبادئ التوجيهية في ضمان امتثال المنظمة بمسؤوليات واجب الرعاية، كما أنها توضح أن إجراءات الإبلاغ عن الحوادث الأمنية تشمل المستوى المناسب من الأشخاص الذين يعملون بالطريقة الصحيحة، وفي الوقت المناسب.¹⁴ كما أصدرت مؤخراً وزارة الخارجية السويسرية، ووحدة تحقيق الاستقرار، ومركز عمليات السلام الدولية (ZIF)، مبادئ توجيهية بشأن واجب الرعاية. والتي يمكن الاطلاع عليها هنا

الفصل الثاني: الأهداف الأربعة لإدارة معلومات الحوادث الأمنية



يوفر هذا الفصل لمحة عامّة عن الأهداف الأربعة الأساسية لإدارة معلومات الحوادث الأمنية والخطوات الرئيسية الواجب اتباعها لتحقيق هذه الأهداف. ويغطي هذا الفصل:

- ▶ الهدف الأول: الاستجابة الفورية
- ▶ الهدف الثاني: الدروس المستفادة والمطبقة
- ▶ الهدف الثالث: فهم السياق التشغيلي
- ▶ الهدف الرابع: اتخاذ القرارات الاستراتيجية
- ▶ جميع الأدوات ذات صلة بهذا الفصل



الهدف الأول: الاستجابة الفورية



يناقش هذا القسم إدارة معلومات الحوادث الأمنية بهدف الإرشاد والتوجيه للرد الفوري على الحادث الأمني والاستجابة له. يغطي هذا القسم:

- 1.1 التوجيه حول كيفية الإبلاغ عن الحادث: ماذا؟ متى؟ كيف؟ من؟
- 1.2 التعامل مع الإجهاد
- 1.3 عملية متابعة الحوادث الأمنية
- 1.4 التواصل
- 1.5 التعامل مع الحالات الحساسة: العنف الجنسي ضد الموظفين

الأدوات ذات الصلة:

- الأداة 2: تصنيف الحوادث
- الأداة 3: الحادث التنظيمي أو الخارجي
- الأداة 4: نموذج الإبلاغ عن الحوادث
- الأداة 5: شبكات تحليل الحوادث
- الأداة 6: كيفية إجراء الاستجواب الواقعي
- الأداة 7: الممارسة الجيدة في الإبلاغ عن الحوادث ذات الصلة
بالاعتبارات الجنسانية وآليات الشكاوى للإبلاغ عن الاستغلال والانتهاك الجنسيين

“

عادة ما يقوم الموظفون المشاركون في الحادث بإجراء أول مكالمة أو اتصال مع منسق شؤون الأمن. واستناداً إلى المعلومات التي يتم تبادلها شفويًا، يقوم منسق شؤون الأمن بتقديم المشورة ويسعى إلى الحصول على المعلومات الأساسية، مثل من فعل ماذا لمن، وأين ومتى. وبعد ذلك، عندما يكون الموظفون في مأمن، يتم ملء تقرير الحادث بشكل أكثر شمولية من قبل منسق شؤون الأمن، وذلك باستخدام المعلومات التي يتم جمعها من استجواب واستخلاص المعلومات بشكل صحيح مع الموظفين المشاركين في الحادث”

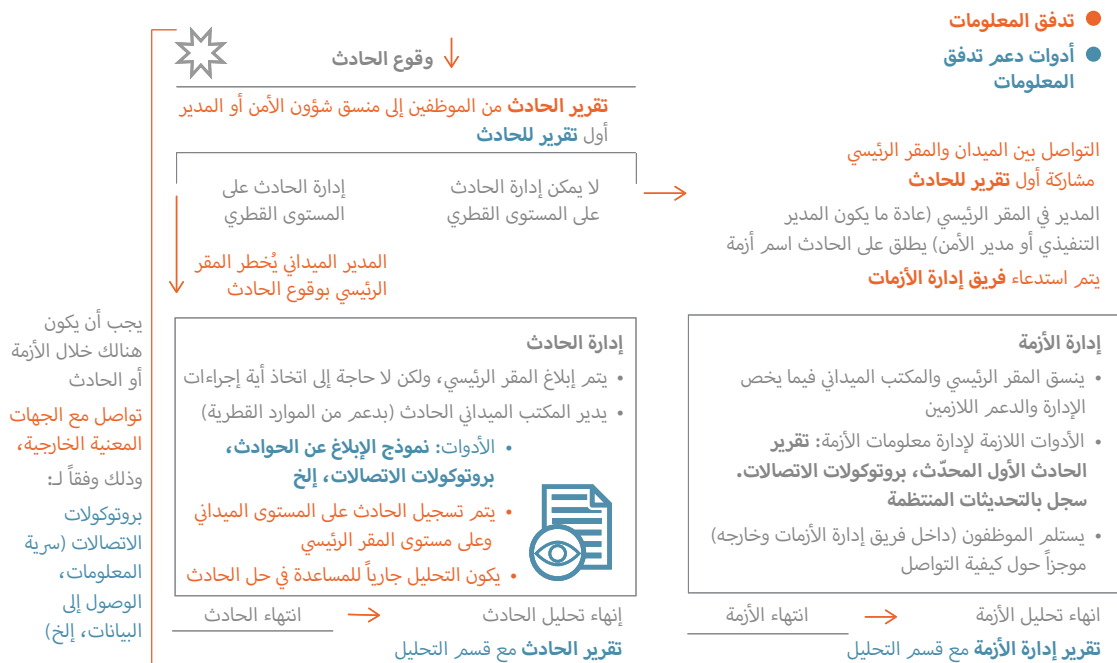
يتمثل أحد الأهداف الرئيسية لإدارة معلومات الحوادث الأمنية في توجيه وإرشاد رد الفعل الفوري والاستجابة لحادث ما. والغرض من ذلك هو التأكد من أن صانعي القرار والموظفين المتضررين أو المعنيين يحصلون على المعلومات ويستخدمونها في توجيه الاستجابة الفورية للحادث. ويحدث ذلك عادة على المستوى الميداني و / أو القطري، وأثناء الحدث أو بعده مباشرة.

ينبغي أن تساعد المعلومات المسجلة والمبلغ عنها في تحديد الدعم المطلوب للموظفين المتضررين وما إذا كانت المنظمة بحاجة إلى تنفيذ أي تغييرات فورية في عملياتها، مثل الحد من الحركة أو تعليق العمليات مؤقتاً. وهناك صلة مباشرة بين المعلومات المطلوبة وخيارات الاستجابة التي ينبغي النظر فيها.



عند وقوع الحوادث، على الموظفين إعطاء الأولوية للإبلاغ والاستجابة والتسجيل.

تحتاج المنظمات إلى تدفق فعال للمعلومات من شأنه أن يضمن حصول جميع الموظفين ذوي الصلة في المقر الرئيسي والمكاتب الإقليمية والمكاتب القطرية والمستوى الميداني على المعلومات اللازمة، وأن تلك المعلومات تُفعل آليات الاستجابة المناسبة. يظهر الرسم البياني¹⁵ التالي التدفق المحتمل للمعلومات عبر المنظمة بعد وقوع حادث أمني.



تتم مشاركة معلومات محددة داخل وخارج المنظمة للأغراض التالية:

- حفظ وتسجيل التقرير الكامل في المستويات ذات الصلة
- تنفيذ الإجراءات الفورية - أداة التخطيط للإجراءات
- استخدام المعلومات في الدروس المستفادة، وتعزيز اتخاذ القرارات، وتحليل الاتجاهات - التقارير، الإحصائيات، إلخ

يمكن مشاركة المعلومات المناسبة والضرورية المتعلقة بالحدث مع المنظمات الأخرى التي تعمل في نفس المنطقة أو البلد لمساعدتها على اتخاذ تدابير احترازية لمنع تكرار وقوع الحوادث.

أما بالنسبة لإدارة المعلومات المتعلقة بالحوادث الأمنية، فإن الإبلاغ الجيد وتسجيل الحادث في أعقاب حدوثه مباشرة أمر أساسي.



لا تنسى أن الهدف من التقارير المباشرة للحوادث هو تزويد الموظفين بالدعم الفوري.

1.1 توجيهات حول الإبلاغ عن الحادث: ماذا؟ متى؟ كيف؟ من؟

ينبغي على المنظمات إرشاد الموظفين بشأن إدارة معلومات الحوادث الأمنية، وينبغي أن يبدأ ذلك بتقديم توجيهات واضحة بشأن الإبلاغ عن الحوادث.

“

عادة ما يتم تناول إجراءات الإبلاغ عن الحوادث في قسم إجراءات التشغيل الموحدة في الخطة الأمنية. وقد قرّرت بعض المنظمات إعداد وثيقة قائمة بذاتها لتغطية سياسة الإبلاغ عن الحوادث وتقديم التوجيهات اللازمة للموظفين في جميع المستويات داخل المنظمة (من المقر الرئيسي إلى الميدان)، وربطها مع وثائق السياسة الأخرى (الموارد البشرية، مدونة قواعد السلوك، السياسة الأمنية، وما إلى ذلك)“

إن إنشاء بروتوكول فعال للإبلاغ عن الحوادث من شأنه أن يسمح للإدارة بـ:

- دعم الأفراد المتضررين
- التعرف على أنماط الحوادث واتجاهاتها
- إجراء تحسينات على التدريبات والإجراءات والهيكل المادية
- تخصيص الموارد بشكل مناسب

من المهم أن يعرف الموظفون إلى من عليهم رفع تقارير الحوادث، ومن المهم أيضاً أن تُحدد إجراءات الإبلاغ عن الحوادث هيكل وخطوات الإبلاغ بالإضافة إلى ما يجب أن يحصل لاحقاً.

ويحدد الجدول التالي الخطوات الرئيسية التي تنطوي عليها عملية الإبلاغ عن الحوادث الأمنية وتحليلها والأطر الزمنية التقريبية المستخدمة للإرشاد والتوجيه.

متى	الخطوة	الإجراءات
مباشرة بعد وقوع الحدث	ملخص ووصف زمني للوقائع. التحليل الأولي للمخاطر.	اكتمال تقرير الحادث، واتخاذ إجراءات الاستجابة الفورية.
بعد الاستجابة الفورية للحادث	استخلاص معلومات الوقائع بعد الحادث: ما هي الوقائع / التحليلات التي ستم مراجعتها / إضافتها إلى تقرير الحادث الأمني المكتمل بعد إدخال عناصر / معلومات جديدة؟ تحليل جديد للمخاطر، مثل الأصول البشرية والمالية والمادية، والمخاطر التشغيلية والقانونية، والمخاطر المتعلقة بالسمعة/الصورة، وما إلى ذلك. والإجراءات التي تم اتخاذها أو التي يتعين اتخاذها للحد من هذه المخاطر.	استخلاص معلومات الوقائع بعد الحادث: التعديلات التي يتعين إدخالها على تقرير (تقارير) الحوادث الأمنية التي تم تقديمها بالفعل والتي تتضمن معلومات جديدة. تم تصميم خطة العمل. تمت إعادة تقييم إجراءات التشغيل الموحدة. تقديم الملاحظات والتعقيبات للشخص الذي يُبلغ عن الحادث وغيره من الموظفين المتضررين حول الإجراءات الواجب اتخاذها.
في الأسابيع التي تلي وقوع الحدث	يتأكد منسق شؤون الأمن أو المدير المسؤول من اتخاذ الإجراءات اللازمة ويقرر ما إذا كان التحليل السابق دقيقاً أم لا. يتم اتخاذ قرار بشأن ما إذا كان الحادث "مغلقاً" لأغراض إدارة الحوادث. وإذا لم يكن الأمر كذلك، ينبغي وضع خطة عمل أخرى.	يتم تحديث تقارير الحوادث عند الضرورة. تم مراجعة خطة العمل، واعتبارها منجزة أو يتم تصميم خطة أخرى. يتم إبقاء أي إجراءات تشغيل موحدة أو يتم الرجوع إلى الشروط السابقة. يتم تقديم التعقيبات والملاحظات إلى الموظفين المتضررين.

ما الذي ينبغي الإبلاغ عنه

تستخدم معظم المنظمات تعريفاً واسعاً للحوادث الأمنية لأغراض إعداد التقارير. من المهم أن يكون هذا التعريف موحداً في جميع مستويات المنظمة لمراعاة الاتساق، ومن المهم أيضاً أن يشمل هذا التعريف جميع الحوادث: الحرجة، وغير الحرجة، والحوادث الوشيكة. انظر 'المقدمة - التعاريف الرئيسية' للاطلاع على التعاريف المتعلقة بإدارة معلومات الحوادث الأمنية.

يمكن أن تتأثر المنظمة بأنواع مختلفة من الحوادث التي لا ترتبط مباشرة بالمسائل الأمنية (مثل الصحة والسلامة)، ويتعين على المنظمة أن تقرر ما إذا كان ينبغي الإبلاغ عن هذه الحالات وتسجيلها من خلال الآليات نفسها. وإذا لم يكن الأمر كذلك، ينبغي توضيح الإجراءات البديلة التي على الموظفين اتباعها للإبلاغ عن الحوادث المتعلقة بالصحة والسلامة. وفي حال تم دمجها ضمن نظام التسجيل نفسه، ينبغي إدراج مؤشر واضح في البيانات لبيّن الفئة التي يندرج ضمنها كل حادث، وذلك من أجل السماح للتحليل بالتركيز على جميع فئات الأمن أو الصحة والسلامة أو أجزاء منها فقط.

“

”في حالة الشك، ينبغي رفع تقرير عن الحادث إلى مدير الأمن أو منسق شؤون الأمن أو المكتب الرئيسي. وسوف يقرر هؤلاء الموظفون كيفية متابعة الحادث.“

لا يمكن تحديد المجموعة الكاملة للحالات التي قد تشكّل حادثة أمنية. وبالتالي، فإن المصطلح معرّف على نطاق واسع جداً ويشمل، على سبيل المثال لا الحصر، ما يلي:

- جميع الجرائم التي تصيب موظفي المنظمة وممتلكاتها (مثل السرقة والسطو والنهب وسرقة السيارات والاختطاف وما إلى ذلك)
- جميع الحالات التي يتعرّض فيها موظفو المنظمة إلى التهديد بالسلح أو إلى أعمال العنف، جميع أنواع المضايقات أو التهديدات من أي نوع،
- أعمال الحرب والنزاعات المسلحة مثل القصف أو الألغام أو إطلاق النار أو العدوان العسكري، النهب، والهجوم على الممتلكات والتخريب،
- جميع الحالات التي قد يكون فيها موظفو المنظمة متورطين في أنشطة غير مشروعة،
- جميع الانتهاكات والمخالفات للوائح التنظيمية الخاصة بأمن المنظمة،
- جميع حالات محاولة الرشوة ضد المنظمات للوصول إلى المواقع أو الطرق أو السكان المتضررين، سواء كانت ناجحة أم لا،
- التهديدات الداخلية وحالات الاحتيال داخل المنظمة.

ينبغي أيضاً الإشارة إلى ضرورة الإبلاغ عن الحوادث التي تقع خارج ساعات العمل بالنسبة للموظفين المحليين أو في الوقت الخاص بالنسبة للموظفين الدوليين. وتشمل الممارسة الجيدة الإبلاغ عن جميع الحوادث حتى تلك التي تقع خارج ساعات العمل المعتادة، لأن ذلك يعزّز ويحسن من تحليل السياق، وقد تختلف في هذه الظروف الإجراءات المتّبعة للإبلاغ عن الحوادث.

“

”يمكنك إعطاء أمثلة على الحوادث الأمنية التي ينبغي الإبلاغ عنها، والتي من شأنها أن تساعد الموظفين على تحديد ما الذي يشكّل حادثاً. إن التصنيف ليس ضرورياً في بداية الإجراءات ولكنه سيساعد الموظفين على فهم ما إذا كان ينبغي عليهم الإبلاغ أم لا. يحتاج الناس إلى أمثلة ذات صلة بمجال عملهم والعمليات التي يقومون بها. ويمكنك أيضاً أن تقرر مناقشة فئات الحوادث غير المعروفة لدى أعضاء الفريق. حيث أن هنالك العديد من دراسات الحالة التي يمكن الاستشهاد بها في هذا السياق“



للاطلاع على القائمة الكاملة لأنواع الحوادث، انظر الأداة 2: تصنيف الحوادث

ويتعين على المنظمات أن توضّح للموظفين ما إذا كان عليهم الإبلاغ عن الحوادث التي تقع خارج المنظمة غير الحكومية، أي تلك التي تؤثر على المنظمات الأخرى. حيث ستركّز المنظمات في كثير من الأحيان على الإبلاغ عن الحوادث التنظيمية وتسجيلها (أي الحوادث التي لها تأثير مباشر على المنظمة وموظفيها وممتلكاتها وسمعتها)، دون الإبلاغ عن الحوادث الخارجية أو تسجيلها في نظامها. وعادة ما يتم رصد الأحداث الخارجية على المستوى الميداني حتى لا يتم تفويت المعلومات السياقية الهامة، ولكن المنظمة بحاجة إلى تحديد الحوادث الخارجية التي قد تؤثر عليها، والإجراءات الواجب اتّباعها عند الإبلاغ رسمياً عن الحوادث الخارجية. ونظراً لأن مثل هذه الإجراءات قد يستغرق وقتاً طويلاً، يمكن للمنظمات أن تعتمد على الأجهزة الخارجية التي تعمل لدى مجتمع المنظمات غير الحكومية لتسجيل الحوادث الخارجية والإبلاغ عنها.

“

عادة ما تضطلع البعثة الميدانية بمسؤولية متابعة وتسجيل مثل هذه الحوادث، كجزء من مؤشرات تقييم المخاطر، ولكن لا يتم تسجيلها في الإحصائيات العامة للمنظمة.”



انظر الأداة 3: الحوادث التنظيمية أو الخارجية

تساعد النماذج والقوالب الجاهزة على ضمان الاتساق عند الإبلاغ عن الحوادث. ويمكن إيجاد هذه النماذج على شكل وثيقة وورد (Word)، أو جدول بيانات، أو منصة إلكترونية وغيرها، وينبغي أن يغطي هذا النموذج ما يلي:

- مؤلف (مؤلفو) التقرير (بما في ذلك تفاصيل الاتصال بهم، مناصبهم والتاريخ)،
- ما الذي حدث (وصف الحادث ونوعه)،
- الضحية (الضحايا) (محلين، دوليين، الجنس، السن، إلخ)،
- نوع العمل الذي يتم القيام به،
- متى وقع الحادث،
- أين وقع الحادث،
- ما إذا كان الحادث عرضياً أو متعمداً، وخصائصه إذا كان متعمداً،
- القرارات التي تم اتخاذها، وإجراءات المتابعة (التي تم تنفيذها أو الموصى بها) والتحليلات أيضاً.

إذا كان الحادث يتطلب استجابة عاجلة، يمكن إعطاء التوجيه للموظفين لضمان إعطاء الأولوية للأسئلة الست التالية:

- من هو المعني؟
- ما الذي حدث؟
- متى وقع الحادث؟
- أين وقع الحادث؟
- ما الذي قمت به حيال هذا الأمر؟
- ما هي المساعدة المطلوبة؟

انظر الأداة 4: نموذج الإبلاغ عن الحوادث، والتي تنطوي على المعلومات المباشرة المطلوبة في إدارة معلومات الحوادث الأمنية والتحليل الأولي.



انظر الأداة 5: شبكات تحليل الحوادث للمزيد من الأسئلة والبنود التي يمكن إضافتها في المراحل اللاحقة من أجل المساعدة على التحليل المتعمق للحوادث.

يمكن تعزيز الاتساق في كتابة تقارير الحوادث الأمنية من خلال تدريب الموظفين. ويمكن تقديم التوجيهات والإرشادات التالية حول كيفية وصف الحوادث بالإضافة إلى نموذج الإبلاغ عنها.

اللغة	استخدم عبارات محددة وقم بوصف السلوك الذي حدث بوضوح. كن دقيقاً حول التفاصيل ولا تقترض أن الآخرين سوف يفهمون العموميات. على سبيل المثال، تجنب استخدام كلمات مثل 'عدواني' أو 'منزعج' أو 'مضطرب'. وبدلاً من ذلك، أذكر السلوك الذي لاحظته والذي جعلك تعتقد أن الشخص كان عدوانياً أو منزعجاً أو مضطرباً. تذكر أن وصف الحادث هو ما سيعتمد عليه الآخرون للحصول على معلومات تتعلق بالفرد (الأفراد) المعنيين والحادث. ومن المهم التأكد من أن التقرير لا ينقل صوراً سلبية عن المعنيين. حيث أن للتقرير القدرة على التأثير على الآخرين، لذا يجب الحرص على إعدادة بشكل صحيح وتقديم تقرير واقعي عن الحادث. راجع تقريرك قبل تقديمه للتأكد من أنك لم تستخدم مصطلحات فيها إصدار أحكام على الآخرين وللتأكد من الإجابة على جميع الأسئلة.
موثوقية المراقبة	هل سيُتفق الأشخاص الآخرون الذين سمعوا أو شاهدوا الحادثة مع ما كتبت في التقرير؟ وإذا كان شخص آخر متورطاً في الحادث أو شاهداً عليه، فمن المستحسن التشاور مع ذلك الشخص لضمان توافق التقرير مع ملاحظاته. تختلف تصورات الأشخاص حول الحادث الواحد، وقد يكون من السليبي تجاهل آراء الآخرين. ومن المهم أيضاً معرفة أن ذكريات الأفراد ستتغير مع مرور الوقت.
الموضوعية	عند كتابة تقرير حادث أمني متعلق بحادث حالي، ينبغي بذل كل جهد ممكن ليكون موضوعياً قدر الإمكان وتجنب التأثير بالحالات السابقة. وبصفتك مؤلف تقرير الحادث، فإنك تكتبه كمسجل للوقائع وليس كقاض. وبناءً على ذلك، تأكد من أن التقرير خال من التصريحات أو السخرية أو التعليقات المتعاطفة.
سبب الحادث	إذا شعرت بأنك لا تمتلك المعلومات الواقعية الكافية، يمكنك إعطاء رأيك شريطة أن تميز بوضوح تام بين الرأي والحقيقة. وحتى إذا كان السبب الفعلي للحادث لا يزال غير معروف بعد محاولتك تحديده، يجب عليك تقديم أكبر قدر من المعلومات عما حدث قبل أو أثناء الحادث، حيث أن ذلك قد يوفر دليلاً للقارئ. وإذا لم تشاهد الحادث على أرض الواقع، وكنت بحاجة إلى كتابة تقرير عنه، تأكد من الإشارة إلى أن المعلومات مبنية على ما تم إبلاغك به والشخص الذي قام بالإبلاغ.

متى ينبغي الإبلاغ عن الحادث

يعتمد توقيت ومستوى تفاصيل التقرير عن الفئة التي ينتمي إليها الحادث:

- ينبغي الإبلاغ فوراً عن **الحوادث التي تستدعي اتخاذ إجراءات فورية** بغرض طلب الدعم والحصول على التعليمات الإضافية. وتعتبر الحوادث الخطيرة التي تشكل تهديداً كبيراً و/أو مستمراً على موظفي المنظمة أو ممتلكاتها أو برامجها على أنها طارئة ودرجة بشكل عام لأغراض الاستجابة والإبلاغ الفوريين.
- **الحوادث التي لا تستدعي اتخاذ إجراءات فورية:** الحوادث الوشيكة التي تعكس انعدام الأمن أو التغيير في بيئة التهديد، ولكنها لا تشكل خطراً مباشراً على موظفي المنظمة أو ممتلكاتها أو برامجها، والتي لا تكون ملحة أو درجة لأغراض إعداد التقارير، وبالتالي يمكن أن تشكل جزءاً من التقارير اليومية المقررة أو التقرير الأسبوعي الذي يُرفع إلى المدير المباشر أو منسق شؤون الأمن.

ويمكن استكمال تقارير الحوادث في عدد من المراحل كلما توافرت المزيد من المعلومات.

على الفور: يتم الإبلاغ عن الحوادث الفورية عندما يصبح الوقت آمناً للقيام بذلك، ويتم ذلك في كثير من الأحيان عن طريق الراديو أو الهاتف. قد يكون الوضع مربكاً في البداية، لذا يجب أخذ الوقت اللازم لتقييم ما حدث للتو، والتأكد إذا ما كان الموظفون وغيرهم من الأشخاص المعنيين في أمان وأنهم حصلوا على المساعدة اللازمة. عند الإبلاغ عن حادث عبر الهاتف أو الراديو، يجب على الموظفين التحدث بوضوح ودقة وإيجاز. إذا لم يكن من الممكن تقديم تفاصيل كاملة (بسبب نقص الوقت، أو لأن القيام بذلك غير آمن خلال حادث مستمر)، قم بتقديم كل ما هو ممكن من المعلومات، من أجل تفعيل الاستجابة المناسبة. حيث أن مشاركة أقل المعلومات وأكثرها إيجازاً قد يساعد في إنقاذ الأرواح.

ينبغي تدريب الموظفين الذين يحتمل أن يتلقوا تقارير فورية عن الحوادث (مثل مشغلي الراديو والمديرين المباشرين ومنسقي شؤون الأمن) على كيفية الاستجابة. إن معرفة الأسئلة التي يجب طرحها والتعاطف مع المراسل يمكن أن يكون له تأثير كبير على فعالية الاستجابة وتعافي الأفراد المتأثرين.

في الساعات والأيام التالية: قد تتطلب بعض الحوادث واحداً أو أكثر من تقارير متابعة الحوادث. ويمكن إعداد تلك التقارير كلما كان ذلك ضرورياً، مع تحديد وتيرة ومستوى التفاصيل منذ البداية وتنقيحها بانتظام. في الحالات الأمنية المستمرة، يجب على منسق شؤون الأمن أو السلطة المعنية الاحتفاظ بسجل يومي للأنشطة. ولن يساعد الحفاظ على سجل للقرارات والأنشطة في تحسين إدارة الوضع فحسب، بل سيوفر أيضاً المعلومات اللازمة للتحديثات وفي نهاية المطاف سيدعم التعلم التنظيمي. وينبغي تبادل المعلومات خطياً حيثما أمكن للحد من خطر سوء الفهم وسوء التواصل. وهذا يساعد أيضاً الأفراد الذين يعانون من الإجهاد على ترتيب ووضع إطار لأفكارهم. انظر القسم أدناه حول 'التعامل مع الإجهاد'.

بمجرد استقرار الحادث أو "إغلاقه": قد تتطلب بعض الحوادث تقريراً كاملاً/نهائياً للحادث الأمني، وينبغي عادة أن يكون خطياً. وبمجرد أن يصبح من المناسب القيام بذلك، سيطلب من المعنيين تقديم بيان مكتوب عن الحادث والإجراءات التي تم اتخاذها. وحيثما يحتاج المكتب الميداني إلى اتخاذ خطوات محددة لمعالجة المخاطر، بما في ذلك إجراء تصحيحات على الإجراءات القائمة، وتقديم التدريبات، وتخصيص الموارد، وما إلى ذلك، ينبغي الإشارة بوضوح إلى تدابير المتابعة هذه، وتحديد الأفراد المسؤولين عن التنفيذ بالإضافة إلى الإطار الزمني المحدد. وينبغي أن تسجل تقارير المتابعة اللاحقة التقدم المحرز في الإجراءات الموصى بها حتى إتمامها. وينبغي



أن يشكل التقرير الكامل للحدث الأساس لإعادة تقييم أو تحديث إجراءات التشغيل الموحدة ذات الصلة بالمنظمة. وسيتم تناول هذا الأمر بمزيد من التفصيل في 'الهدف الثاني'.



يجب أن يكون الموظفون على معرفة بما يمكن توقعه وما الذي ينبغي طلبه عند الإبلاغ عن الحادث. وينبغي تحديد المسببات بوضوح وشرح الاستجابات مسبقاً. وللد من قلة الإبلاغ، ينبغي أن يكون الإجراء واضحاً ومرناً في الوقت نفسه: يمكن أن يكون التقرير بسيطاً، أو يمكن أن يصبح أكثر شمولاً عند الاقتضاء.

ويفضّل كلما كان ذلك ممكناً أن يتم إعداد تقرير الحادث مباشرة بعد وقوعه لأن الحقائق ستكون واضحة عندئذ في ذهن المتضررين. ومع ذلك، واعتماداً على شدة الحادث، قد يكون الموظفون مضطربين وعاطفيين بعض الشيء في ذلك الوقت ولذلك قد يكون من المفيد أن يقوم شخص آخر بمراجعة التقرير قبل تقديمه.

كيف ينبغي الإبلاغ عن الحادث

ينبغي أن تحدد إجراءات الإبلاغ عن الحوادث أكثر وسائل التواصل أمناً، مع مراعاة أوقات الإبلاغ الثلاثة المذكورة آنفاً.

ينبغي أن يوضح إجراء الإبلاغ عن الحوادث ما إذا كان ينبغي استخدام أجهزة الراديو أو هواتف الأقمار الصناعية أو رسائل البريد الإلكتروني، وضمان تدريب الموظفين على استخدام الأجهزة بشكل سليم وآمن (باستخدام التشفير إذا لزم الأمر). كما ينبغي إطلاع الموظفين على ضرورة ضمان السرية بشأن الإبلاغ عن الحوادث.



ينبغي أن يوضح إجراء تقديم التقارير الفروق بين قنوات الإبلاغ عن أنواع الحوادث المختلفة. على سبيل المثال، سيتطلب حادث سطو وحادث عنف جنسي آليات إبلاغ مختلفة. وقد تتطلب الحوادث التي تستدعي استجابة إدارية، مثل مطالبات التأمين، واستبدال الأصول إجراءات محددة أخرى. انظر 'التعامل مع الحالات الحساسة: العنف الجنسي ضد الموظفين' في هذا القسم أدناه للحصول على مزيد من المعلومات حول الإبلاغ عن الحالات الحساسة.

من الممكن تطوير إجراءات مختلفة للإبلاغ عن الحوادث تبعاً لطبيعة الحادث، أي مستوى السرية والحساسية المطلوبة. ومع ذلك، من المهم التأكيد على أنه لا ينبغي أن تكون القناة المستخدمة في الإبلاغ هي أكبر الاهتمامات (ما لم يكن هناك اعتراض خطير أو مخاوف تتعلق بالخصوصية). ولا سيما بالنسبة للحوادث التي تتطلب استجابة عاجلة، والتي يكون فيها أهم شيء هو إيصال المعلومات للمستفيدين المعنيين في أسرع وقت ممكن حتى يحصل المتضررون على الدعم الذي يحتاجونه.



من المهم أيضاً أن يحترم الموظفون سرية المعلومات داخلياً، لضمان عدم اعتراض إدارة الحادث. ويمكن لمنسقي شؤون الأمن في هذا السياق استخدام جدول 'فئات المعلومات' في الهدف الثالث.

من الذي يتم إبلاغه عن الحوادث

ينبغي أن يكون جميع الموظفين قادرين على الإبلاغ عن الحادث، ويجب أن تشير إجراءات الإبلاغ عن الحوادث في المنظمة إلى الموظفين الذين ينبغي رفع التقارير إليهم. على سبيل المثال، قد ينص الإجراء على رفع تقرير الحادث عبر البريد الإلكتروني إلى شخص محدد أو من خلال نظام رفع تقارير إلكتروني آلي، يرسل بشكل تلقائي التقارير إلى الموظفين المعنيين في المنظمة.

يقدم الجدول التالي أمثلة عن الأفراد والمهام والمسؤوليات المناطة بهم في حال وقوع حادث.

من	المهام و/أو المسؤوليات
جميع الموظفين	عليهم إبلاغ مديريهم أو منسق شؤون الأمن المعين عن الحادث.
منسق شؤون الأمن (في الميدان أو على مستوى المكتب القطري) المدير (في الميدان أو على مستوى المكتب القطري)	بمجرد استلام التقرير الأولي للحادث، على منسق شؤون الأمن التأكد من توفير الدعم اللازم للموظفين المتضررين، وإخطار المكتب الإقليمي/القطري في حال الحاجة إلى دعم من جهتهم، كما عليه متابعة الحادث والترتيب لتقديم معلومات حول الحادث وتحليله. وعليه اقتراح التدابير التشغيلية الفورية للمدير الإقليمي. كما عليه ضمان الاتصالات مع الموظفين الميدانيين عند الحاجة.
منسق شؤون الأمن القطري أو الإقليمي المدير (القطري أو الإقليمي)	عند تلقي المعلومات من الميدان أو المكتب القطري، ينبغي أن يضمن تقديم الدعم إلى الأفراد المتضررين، وإرسال المعلومات إلى المقر الرئيسي في حال الحاجة إلى الدعم، وضمان المتابعة وإمكانية استخلاص المعلومات في حالة إبعاد الموظفين عن الموقع الميداني. يقوم بالمناقشة والاتفاق على تدابير تشغيلية فورية محتملة مع المدير القطري أو الميداني.
مدير أو مستشار الأمن (على مستوى المقر الرئيسي)	بعد استلام المعلومات من المكتب الإقليمي أو القطري، عليه ضمان الحصول على الدعم من المقر الرئيسي عند الحاجة. وسيقوم بالتنسيق مع أصحاب القرار في المقر الرئيسي من أجل التحقق من المستوى المناسب للإدارة.
المدير أو المدير التنفيذي / الرئيس التنفيذي (على مستوى المقر الرئيسي)	سوف يتلقى معلومات الحادث من مدير / مستشار الأمن على مستوى المقر الرئيسي و / أو المديرين على المستوى الإقليمي أو القطري. ينبغي أن يضمن متابعة إجراءات محددة على مستوى المقر الرئيسي، إذا كانت مطلوبة. وعليه ضمان التواصل بشأن الحادث مع موظفي المقر الرئيسي إذا كان ذلك ضرورياً.

يلزم أن تقوم كل منظمة بتكييف تدفق المعلومات المتعلقة بالحادث بما يتماشى مع مناصب الموظفين والتسلسل الهرمي والوجود التشغيلي.

ينبغي تحديد مسؤوليات الموظفين فيما يتعلق بالإبلاغ عن معلومات الحوادث الأمنية وإدارتها بوضوح في وثائق السياسات (مثل سياسة إدارة المخاطر الأمنية، وسياسة الإبلاغ عن الحوادث، ومدونة قواعد السلوك، وما إلى ذلك) والوثائق الإجرائية. وينبغي تسليط الضوء بشكلٍ منتظم على الأدوار خلال عملية الاستقراء طوال دورة العمل.

1.2 التعامل مع الإجهاد

من المرجح أن يكون الموظفون الذين يبلغون عن حادث ما أثناء وقوعه أو بعده مباشرة تحت ضغطٍ كبير. ويستحسن أن يسعى الموظفون الذين يتلقون التقرير الشفهي الأول إلى:

- البقاء هادئين
- تحديد الشخص الذي يقوم بإعداد التقرير
- ضمان أمن وسلامة الأشخاص المتورطين في الحادث
- ترتيب أولويات المعلومات المطلوبة مثل الوضع، وما الذي تم القيام به، وما الذي يتوجب القيام به فوراً
- جمع المعلومات وفقاً لنموذج الإبلاغ عن الحوادث
- طمأنة الشخص الذي يبلغ عن الحادث والاتفاق على المزيد من التواصل

الغرض من هذا التقرير الأول هو الحصول على الحقائق اللازمة لإبلاغ استجابة فورية. وهذا ليس استخلاصاً للمعلومات العاطفية (غالباً ما يسمى التخفيف من حدة الصدمة أو باللغة الإنجليزية defusing). وعند الضرورة، ينبغي أن يقوم خبراء مختصون بتقديم الدعم النفسي واستخلاص المعلومات العاطفية من الأفراد في أعقاب وقوع الصدمات. هذا الاستخلاص العاطفي في معظمه ذو صلة بالحوادث الخطيرة، ولكن بعض الحوادث غير الحرجة سيكون لها أيضاً آثار مؤلمة على الشخص المعني. وينبغي للمنظمة أن تكفل تقديم الدعم للموظفين في كلتا الحالتين.

1.3 عملية متابعة الحوادث الأمنية

ينبغي متابعة جميع الحوادث الأمنية لضمان تغطية جميع المعلومات المتعلقة بالحدث واستخدامها لاستخلاص الدروس المستفادة وتحديث السياق وصنع القرار.

توفّر عملية المتابعة تحديثات لتقارير الحوادث، وذلك اعتماداً على الحقائق الجديدة أو الناشئة. وهي أيضاً عملية مفيدة ينبغي اتباعها عندما تكون هناك تغييرات في الموظفين الذين يشغلون المناصب الرئيسية ذات الصلة، مثل منسق شؤون الأمن. وفي بعض الحالات، قد يتطلب ذلك إعداد نسخة جديدة من تقرير الحادث.

وينبغي أن تتضمن هذه العملية كل حدث جديد أو إجراءات جديدة تتحقق أثناء إدارة الحادث، إلى أن يتم اختتام الحادث وإغلاقه.

يمكن أن تستمر الحوادث الخطيرة لفترة طويلة مثل اختطاف الموظفين، مع توافر معلومات جديدة بشكل متقطع. ومن المهم أن تغطي المنظمة هذه المعلومات الجديدة بطريقة مجدية بحيث يمكن تحليلها وأخذها في الاعتبار في عملية صنع القرار. وينبغي أن يشكل ذلك جزءاً من خطة إدارة الأزمات.



ينبغي تحديد عمليات المتابعة لجميع الحوادث، وذلك لضمان عدم فقدان المعلومات والدروس المستفادة أو إلغائها أولوياتها في البيانات المتغيرة.

استخلاص المعلومات (الاستجابات) الواقعي

ينبغي أن يأتي استخلاص المعلومات الواقعي بعد تلقي الموظفين المعنيين الدعم المناسب عقب وقوع حادث. ويفضل أن يحدث هذا خلال 48 ساعة من وقوع الحادث الأمني. وسيختلف مدى استخلاص المعلومات تبعاً لطبيعة الحادث ومدى تعقيده.

من المهم عند الترتيب لإجراء الاستجابات الواقعي لأغراض جمع المعلومات الحفاظ على المبادئ الأساسية للإسعافات الأولية النفسية¹⁶ وأخذها في عين الاعتبار:

- إجراء الاستجابات الواقعي فقط بعد ضمان حصول الفرد على الأمن البدني والنفسي الأساسي؛
- ينبغي أن يتم استخلاص المعلومات في مكان آمن؛
- التركيز على تمكين الفرد المتضرر؛
- توخي الوضوح بشأن العملية والتوقعات وإجراءات المتابعة.

من المهم أن نتذكر أن تأثير ووقوع الحوادث الشبكية والحوادث الصغيرة على بعض الموظفين قد يكون أشد بكثير من أثرها على المنظمة. على سبيل المثال، قد يؤثر التحرش من قبل أفراد المجتمع أو محاولات السطو الفاشلة على الفرد بشكل عميق.





انظر الأداة 6: كيفية إجراء الاستجواب الواقعي لمزيد من التوجيه حول كيفية تنظيم الاستجواب الواقعي لأغراض جمع المعلومات وتحليلها. يُرجى العلم أن هذه ليست محاولة لتدريب القراء على تقديم الإسعافات الأولية النفسية أو جعلهم محققين محترفين. بل هي عبارة عن قائمة من النصائح لإجراء المقابلات الآمنة والمفيدة لتقضي الحقائق لأغراض الإبلاغ عن الحوادث.

مصدر المعلومات

ينبغي التحقق من المعلومات التي تم جمعها للتأكد من دقتها من خلال التحدث إلى أصحاب المصلحة الداخليين والخارجيين لجمع وجهات نظر مختلفة.



تعتبر مصداقية المعلومات وصحة المصدر من العناصر الحاسمة عند تحليل المعلومات الأمنية.

إن مصفوفة¹⁷ الموثوقية والصحة التالية أداة بسيطة يمكنها مساعدتك في عملية التحقق هذه.

مصداقية المصدر

التصنيف	الوصف
أ	موثوق تماماً لا شك في مصداقية المصدر أو جدارته بالثقة أو كفاءته. لديه تاريخ كامل من الموثوقية.
ب	موثوق عادة شكوك قليلة. معظم المعلومات السابقة المقدمة صحيحة.
ج	موثوق به إلى حد ما شكوك. قدّم المصدر معلومات صحيحة في الماضي.
د	غير موثوق عادة شكوك كبيرة. قدّم المصدر بعض المعلومات الصحيحة في الماضي.
هـ	غير موثوق يفتقر إلى المصداقية والثقة والكفاءة. تاريخ من المعلومات غير الصحيحة.
و	لا يمكن الحكم على الموثوقية معلومات غير كافية لتقييم الموثوقية. يمكن أو لا يمكن أن يكون موثقاً.

صحة المعلومات

التصنيف	الوصف
1	مؤكدة معلومات منطقية، تتماشى مع المعلومات الأخرى ذات الصلة، وقد أكدتها مصادر مستقلة.
2	على الأرجح أنها صحيحة معلومات منطقية، تتماشى مع غيرها من المعلومات ذات الصلة. لم يتم تأكيدها.
3	ربما صحيحة منطقية بشكل معقول، تتفق مع بعض المعلومات الأخرى ذات الصلة، غير مؤكدة.
4	صحيحة بشكل مريب غير منطقية ولكن ممكنة، لا توجد معلومات أخرى حول الموضوع، غير مؤكدة.
5	غير محتملة غير منطقية، تتعارض مع المعلومات الأخرى ذات الصلة.
6	لا يمكن الحكم على الحقيقة لا يمكن تحديد صحة المعلومات.

¹⁷ للحصول على مزيد من المعلومات عن الإسعافات الأولية النفسية، انظر التوجيهات الصادرة عن منظمة الصحة العالمية هنا

على سبيل المثال: سيكون التصنيف (أ.3) من مصدر موثوق به جداً ولكن المعلومات ربما تكون صحيحة فقط. وفي التصنيف (د.1) لا يمكن في العادة الاعتماد على المصدر، غير أن معلومات مؤكدة (تم التحقق منها من مصادر أخرى).

سيكون من السهل استخدام هذه المصفوفة إذا كان لدى المنظمة خريطة محدّثة لأصحاب المصلحة. إن مصداقية المصدر شيء يجب مراعاته على مدى فترة طويلة من الزمن؛ وينبغي أن يقوم منسق شؤون الأمن بفحص أي معلومات تشغيلية يتم تقديمها بانتظام، لتقييم موثوقية المصادر وصحة المعلومات الواردة.

قد تتلقى المنظمات معلومات أمنية من منظمات غير حكومية أو أفراد آخرين بطريقة غير مباشرة، من خلال طرف ثالث أو عن طريق تجاوز أصحاب المصلحة المعتادين. ويُشار إلى هذا أحياناً باسم تدفق المعلومات القطري. على سبيل المثال، ليس لدى الشهود على اختطاف مركبة تابعة لمنظمة غير الحكومية أي وسيلة للاتصال بالمنظمة مباشرة، لذلك قاموا بالاتصال بالتحالف بدلاً من ذلك. وقد نقل التحالف الرسالة إلى مدير الأمن بالمنظمة غير الحكومية، الذي نقل بدوره الرسالة إلى المكتب القطري في الميدان.

1.4 الاتصالات

ينبغي وضع سياسة على المستوى التنظيمي لتحديد المعلومات الأمنية التي ينبغي مشاركتها ومع من، على الصعيدين الخارجي والداخلي؛ وعلى وجه الخصوص مباشرة بعد وقوع حادث، وتحديد الشخص المسؤول عن تبادل المعلومات عبر مختلف مستويات المنظمة (من الميدان إلى المقر) وخارجياً. وينبغي أن تغطي السياسة مسائل السرية من أجل حماية هويّات الأفراد المتضررين وغيرهم من أصحاب المصلحة المعنيين حسب الاقتضاء.

ويفضّل تحديد جهة اتصال واحدة من كل مستوى داخل المنظمة (من الميدان إلى المقر) باعتبارها مسؤولة عن الاتصالات الخارجية، لضمان القيام بذلك بشكل جيد وفي الوقت المناسب.

“

ينبغي معالجة أخلاقيات استخدام المعلومات المتميزة في مناطق النزاع أثناء إدارة الحوادث الأمنية. وينبغي أن يكون منسق شؤون الأمن قادراً على تصفية معلومات محددة لأغراض الالتزام الأخلاقي، مع نشر المعلومات ذات الصلة على نحو فعال لضمان سلامة وأمن الموظفين ومهام المنظمة.”

يمكن للمنظمات أن تستخدم آليات التنسيق لجمع المعلومات وإدخالها في تحليل سياقها وإدارة الحوادث، وذلك من خلال الإجراءات الرسمية وتحسين العلاقات المهنية غير الرسمية مع الجهات الفاعلة الرئيسية.



يجب على قائد الفريق أو منسق شؤون الأمن تحديد مستوى المعلومات التي سيتم مشاركتها داخل وخارج المنظمة، وفقاً للسياسة.

التواصل مع السلطات

قد يكون من الضروري بالنسبة للعديد من الحوادث مشاركة ما هو معروف مع الشرطة أو غيرها من وكالات إنفاذ القانون، وخاصة أثناء وقوع حوادث خطيرة مثل القصف، أو الهجوم، أو الاختطاف، أو الاعتداء وذلك من أجل المساعدة في حل الحادث، والحد من تأثيره، و / أو الحد من احتمال وقوع حوادث مماثلة تؤثر على الآخرين.

وغالباً ما يكون الاتفاق والتعاون مع الحكومة المضيفة عنصراً رئيسياً في عمليات المنظمات غير الحكومية الفعّالة. ولذلك تنصح المنظمات وبشدة في بعض السياقات بإبلاغ السلطات المحلية والشرطة عن الحوادث. ومع ذلك، ينبغي أن يتم هذا الإبلاغ على أساس سياق، مع مراعاة مجموعة متنوعة من العوامل، وينبغي النظر فيه قبل وقوع الحادث وإدراجه في إجراءات التشغيل الموحدة للمنظمة أو خطط الطوارئ.

التواصل مع وسائل الإعلام

يمكن للحوادث الأمنية عالية المستوى أو الحرجة أن تجتذب اهتماماً واسعاً من مصادر خارجية، ولا سيما وسائل الإعلام. كما يمكن للحوادث الأخرى أن تثير اهتمام وسائل الإعلام، تبعاً لجدول أعمالها (مثل اتجاهات المنشورات، وما إلى ذلك).

ينبغي دائماً أن يكون أمن الأفراد المتضررين مباشرة من الحادث وسلامة زملائهم وأسرهم هو الشاغل الرئيسي. وقد تعرّض مشاركة بعض المعلومات حياة الناس للخطر. ومع ذلك، فإن سرعة نقل المعلومات الصحيحة من شأنها أن تنقذ الأرواح. كما أن الطريقة التي تستجيب بها المنظمة، ليس للحادث فحسب، بل للمعلومات ووجهات النظر المتعلقة به مهمة لسلامة الموظفين والمنظمة.



تذكّر: بمجرد خروج المعلومات إلى النطاق العام، فإنه لا يمكن التراجع عنها، في حين يمكن دائماً إصدار تفاصيل إضافية لاحقاً.

ينبغي تكييف المهام التنظيمية الرئيسية وفقاً لحجم الحادث الذي يجري التعامل معه، وينبغي إسناد مسؤوليات هذه المهام خلال مرحلة التخطيط. انظر الجدول التالي لتوجيه الموظفين المسؤولين عن إعداد استراتيجية أمن الاتصالات الخارجية للمنظمة، وخاصة فيما يتعلق بالتعامل مع وسائل الإعلام:

تأكد من أنك تسيطر على المعلومات الخاصة بك.	
استمر في مراقبة المعلومات المتاحة عن الحادث من جميع المصادر.	
أعط الأولوية لمراقبة وسائل التواصل الاجتماعي لتبقى على اطلاع على المعلومات المتوفرة عن الحادث في النطاق العام. راقب مصادر اللغة المحلية وكذلك لغة المقر الرئيسي وغيرها حسب الاقتضاء.	
قم بالتعرّف على المتحدث الرسمي أو قم بتحديد مسبقاً.	
عليك السعي لمنع النشر. وإذا كان هذا غير ممكن، قم بتصحيح و / أو إزالة إشكالية القصص والرسائل والصور والأفلام من أي مصدر. وضح أن اهتمام وسائل الإعلام قد يعرض الموظفين للخطر.	
تأكد من تسجيل المكالمات الهاتفية الواردة مع التاريخ والوقت، والإشارة إلى المتحدث الرئيسي.	
قم بإعداد الرسائل الرئيسية وأجوبة الأسئلة الشائعة للمتحدث الرئيسي و / أو المتحدثين الإضافيين.	
قم بإحاطة وتدريب المتحدث الرئيسي / المتحدثين الإضافيين.	
قم بإعداد بيان مكتوب يقرأه المتحدث إذا لزم الأمر؛ وهذا يساعد على ضمان تركيز الأشخاص على الرسالة.	
عليك التمسك بالوقائع وعدم تقديم معلومات "غير رسمية".	
تأكد من مواءمة الاتصالات الداخلية والخارجية.	
قم بتسجيل القرارات التي تم اتخاذها والعوامل التي أثرت على صنع القرار.	

تأكد من أن يُنظر للمنظمة غير الحكومية على أنها مصدر معلومات صادق وموثوق وجدير بالثقة.	
قل الحقيقة، وتجنب استخدام عبارة «لا تعليق». لا تتكهن. إذا كان تقديم الرد مطلوباً ولكن المعلومات محدودة، قم بإصدار بيان تعليق (holding statement).	
احترم الصحفيين ومواعيدهم النهائية ورد على مكالماتهم الإعلامية. ادعو المتصلين من وسائل الإعلام للاطلاع على موقع المنظمة غير الحكومية أو حساباتها على وسائل التواصل الاجتماعي للحصول على التحديثات، مثل تويتر.	
اقترح تضمين المتصلين من وسائل الإعلام في قائمة البريد الإلكتروني للوكالة، والتأكد من حصولهم على الأخبار والبيانات الصحفية التي يتم تحميلها على شبكة الإنترنت.	
استخدام أدوات مثل تويتر لإطلاق المعلومات بإيجاز، مع روابط إلى الموقع حيث يمكن قراءة البيانات والنشرات الصحفية الكاملة.	
تأكد من أن جميع الموظفين الذين تستدعي مناصبهم العمل في الخارج (مثل الحراس والسائقين) يعرفون الإجابة المناسبة لأية أسئلة وإلى من عليهم توجيه الاستفسارات.	
دع دائماً في الاعتبار أن الهدف الرئيسي هو سلامة وحماية الموظفين المتضررين مباشرة.	
لا تفصح عن أي بيانات شخصية خاصة بالأفراد المتضررين من الحادث أو المتورطين فيه.	



انظر دليل منتدى الأمن الأوروبي المشترك بين الوكالات (EISF) حول "إدارة الرسائل" للحصول على إرشادات وأدوات إضافية، بما في ذلك نموذج بيان التعليق (holding statement).

التعاون مع الوكالات الأخرى

ينبغي أن تخصص كل منظمة جزءاً كبيراً من اتصالات الأمن للتعاون الوثيق وتبادل المعلومات مع الوكالات والمنظمات غير الحكومية الأخرى العاملة في نفس المنطقة أو المناطق التي تعتبر ذات صلة بالعمليات.



يكون التنسيق في مجال الاتصالات مهماً خاصة عندما ينطوي حادث أمني على مجموعة من الأفراد من مختلف المنظمات. وسيكون التنسيق الاستباقي أساسياً في الاستجابة الفورية، وينبغي مناقشة إدارة الحوادث والإبلاغ عنها بصورة متسقة ومنظمة مع ضمان الموافقة عليها مسبقاً. ويمكن معالجة ذلك في إجراءات التشغيل الموحدة.

عندما لا يتم جمع المعلومات المتعلقة بالحوادث الأمنية وإدارتها ونشرها أفقياً، يصعب إلى حد ما التحقق من صورة التهديد في المنطقة. وتزدهر آليات التعاون الأمني عندما يستمر كل من الاتصال الرأسي والأفقي "في إغلاق الحلقة" (أي تقديم التغذية الراجعة) وعندما يعمل أصحاب المصلحة مع بعضهم البعض بطريقة منسقة.

ينبغي إجراء استجابات لاستخلاص معلومات الحوادث مع المنظمات الأخرى ذات الصلة بسرعة بعد وقوع الحوادث الأمنية، إذا ارتأت المنظمة أن مشاركة المعلومات أمر مناسب وضروري.

يمكن استخدام نموذج الإبلاغ عن الحوادث كوثيقة إرشادية لإعداد استخلاص المعلومات. يجب على منسق شؤون الأمن و / أو المديرين المعنيين أن يحددوا مسبقاً أكثر البيانات / المعلومات ذات الصلة التي يمكن مشاركتها مع المنظمات الأخرى. ومع ذلك، ينبغي أن تأخذ هذه القرارات بعين الاعتبار فئة المعلومات التي تدرج تحتها الأجزاء المختلفة لبيانات الحادث (انظر "الهدف الثالث").



يجب أن تركز العناصر الرئيسية في استخلاص معلومات الحوادث على توضيح النقاط التالية: فعل ماذا وأين ومتى. وحرصاً من المنظمات على حماية الأفراد المتضررين، لا ينبغي لها أن تكشف عن الشخص المتورط في الحادث. ومع ذلك، إذا كانت المعلومات المتعلقة بالعرق أو الجنسية أو العوامل الشخصية الأخرى أساسية وهامة، فعليك التفكير في كيفية مشاركة هذه المعلومات مع الحفاظ على السرية. كما أن بناء علاقات وثيقة قبل وقوع الحوادث أمرٌ ضروري لتبادل المعلومات الدقيقة.

ويمكن أيضاً أن يُنظر إلى استخلاص المعلومات أو الاستجواب على أنه فرصة للحصول على الدعم من المنظمات الأخرى، سواءً كان ذلك دعماً لوجيستي أو مساعدات أو تحسين التنسيق وتبادل المعلومات أو اتخاذ موقف سياسي معاً كمجتمع المنظمات غير الحكومية بشأن قضية معينة (انظر "الهدف الرابع").

وكما هو الحال دائماً، ينبغي أن يأخذ قرار تبادل المعلومات في الاعتبار أي أثر محتمل على أمن موظفي المنظمة والأفراد المتضررين الآخرين.

عندما تتلقى المنظمة معلومات عن الحوادث الأمنية من منظمة أخرى، وتحديدًا حول الحوادث الخطيرة، فإنه من المستحسن:

- تجنّب الاتصال بالمنظمة غير الحكومية التي تقود إدارة الحوادث (إذا كان الحادث مستمراً) ما لم تكن هناك معلومات ذات صلة يتوجب مشاركتها من أجل الرد على الحادث.
- تجنّب أي نوع من التدخل ما لم يُطلب منك ذلك.
- لا تشارك المزيد من المعلومات (تقرر المنظمة غير الحكومية المتأثرة من يجب أن يطلع على المعلومات)
- قيّم الحاجة إلى تنفيذ تدابير معيّنة للحد من إمكانية تعرض المنظمة لحوادث مماثلة، وأبلغ أصحاب المصلحة الداخليين الرئيسيين عنها، وقرّر بتنفيذ تدابير معالجة المخاطر المحددة.
- قمر بتحديد المعلومات المطلوبة لتوضيح التدابير المذكورة أعلاه (عند الضرورة) دون الكشف عن المعلومات السرية.
- حاول الحد من الشائعات المحتملة داخل المنظمة من خلال معالجة الأسئلة وتوصية الموظفين بالحفاظ على السرية.
- قيّم الحاجة إلى مراجعة وتحديث التدابير الأمنية للمنظمة.

ينبغي للمنظمات في مجال مماثل أن تستخدم آليات تعاونية لتبادل المعلومات التي قد تكون مفيدة للمنظمات الأخرى في تقييم السياق الأمني. وتتم مناقشة هذا النوع المنظم من تبادل المعلومات عبر مختلف المنظمات بمزيد من التعمق في "الهدف الثالث".

1.5 التعامل مع الحالات الحساسة: العنف الجنسي ضد الموظفين

يجب التعامل مع بعض الحوادث بحساسية وباهتمام خاص، لا سيّما عندما يتعلق الأمر بإدارة معلومات الحوادث الأمنية. ويمكن أن يكون لهذه الحوادث آثار مضاعفة خاصة على الأشخاص المعنيين، والمنظمة، والمجتمع الإنساني والإنمائي الأوسع نطاقاً.

نشير في هذا القسم، إلى الحوادث الأمنية التي غالباً ما تعتبر صادمة بشكل خاص بالنسبة للشخص (الأشخاص) المعنيين. ولأغراض الوضوح، سنستخدم المثال المحدد للعنف الجنسي ضد موظفي المعونة والمساعدات، بالرغم من إمكانية تطبيق المبادئ ونهج الإدارة المبين في هذا القسم على أنواع أخرى من الحالات، بما في ذلك حالات الاختطاف أو قتل الموظفين. ينبغي

استخدام المبادئ التوجيهية في هذا القسم مع بقية الدليل، وينبغي أن ينظر المستخدمون في النهج الذي يركز على الناجين.

تشير الأدلة التي جمعتها منظمة Report the Abuse¹⁸ إلى أن العنف الجنسي، الذي يتراوح من التحرش الجنسي إلى الاغتصاب، يحدث في أماكن عمل المنظمات غير الحكومية وأن أغلبية الجناة هم زملاء الناجين. وتتعرض النساء في مجال تقديم المعونة للخطر بوجه خاص، رغم أن الرجال قد يتعرضون أيضاً للعنف الجنسي.

لخص تقرير نُشر في عام 2016 بشأن هذه المسألة إلى أن 16% فقط من المنظمات الإنسانية غير الحكومية التي جرى تقييمها ذكرت العنف الجنسي باعتباره خطراً على الموظفين في إطار سياساتها وإجراءاتها، ناهيك عن آليات الاستجابة الشاملة أو الحساسة أو الموجهة نحو الناجين.¹⁹

سيشكل وضع نظام مناسب لإدارة معلومات الحوادث الأمنية يتضمن معلومات حول العنف الجنسي ضد الموظفين خطوة كبيرة نحو وضع استراتيجيات أفضل للوقاية والاستجابة لهذا النوع من الحوادث.

يشكل العنف الجنسي ضد العاملين في مجال تقديم المعونة تهديداً خطيراً لا يقوض سلامة وأمن موظفي البرنامج فحسب، بل يمكن أن يؤدي أيضاً إلى تدهور كبير في فعالية وكفاءة عمليات المنظمات غير الحكومية. ومن المهم اعتبار العنف الجنسي انتهاكاً للحقوق، مما يعني أن بُعد الحماية ينطبق مباشرة على إدارة هذه الحالات.

نقص الإبلاغ - الأسباب والعقبات

- لا يتم الإبلاغ عن العنف الجنسي في كل سياق أو بلد أو ثقافة. وهناك أسباب عديدة وراء عدم الإبلاغ عن حوادث العنف الجنسي في السياق الإنساني، نذكر منها:
- عدم المعرفة أو عدم وجود قنوات أو إجراءات للإبلاغ.
- الافتقار إلى الاستثمار التنظيمي في التدريب والمعرفة اللازمة لتلقي تقارير عن العنف الجنسي.
- قلة الأدلة أو اللجوء القانوني، أو الخوف من أن الإبلاغ عن الحادث لن يؤدي إلى العدالة ولا العقاب.
- مخاوف بشأن وضع العلامات التمييزية أو إلقاء اللوم على الضحايا من قبل المنظمة والزملاء.
- العار أو الذنب أو الإهانة المتأصلة اجتماعياً عند تعرض الشخص للعنف الجنسي.
- الخوف من الانتقام، أو العواقب المهنية أو الشخصية.
- عدم الثقة في النظام.

كل هذه أسباب جدية تؤدي إلى عدم إبلاغ الفرد عن العنف الجنسي. ونجد أن الهيكل التنظيمي والثقافة هي التي تدعم معظمها. يجب على كل منظمة غير حكومية أن تفكر في الثقافة التي تخلقها، وأن تتأكد من أن الوصول إليها سهل، وأنها مفتوحة أمام التعليقات والتغذية الراجعة البناءة، وأنها موثوقة، وحساسة، وتركز على الناجين. ومن شأن إشراك الموظفين من جميع المستويات في المناقشات المثمرة والأمنة حول هذه المسألة أن يغيّر إلى حد كبير بعض الشواغل التي تؤدي إلى نقص الإبلاغ.

¹⁸ الجيش الأمريكي. (2006). الدليل الميداني رقم 2-22.3 لعمليات الذكاء البشري.

¹⁹ للمزيد من المعلومات راجع موقع منظمة Report the Abuse: <http://reporttheabuse.org/about/>

نوبيرت، إم (2016)، الوقاية والسياسة وقائمة تدقيق الإجراءات. الاستجابة للعنف الجنسي في المجال الإنساني والإنمائي. Report the Abuse.

“

“لا توجد في الوقت الراهن ممارسات جيدة يمكن للمنظمات غير الحكومية اتباعها من أجل منع العنف الجنسي في أماكن العمل وضمان امتثالها لواجب الرعاية الذي تدين به لموظفيها. ولا تتوفر أيضاً مبادئ توجيهية مفصلة بشأن كيفية الاستجابة عند وقوع حوادث من هذا النوع. ومع ذلك، فإن منظمة Report the Abuse تعمل على تطوير مثل هذه الممارسات الجيدة، ومن المقرر أن تنشر أول أداة لها في ربيع / صيف 2017”²⁰

اعتبارات هامة بشأن العنف الجنسي وإدارة معلومات الحوادث الأمنية:

- الموافقة المستنيرة: يجب الحصول على الموافقة المستنيرة للناجين من حادث ما في جميع مراحل جمع المعلومات واستخدامها.
- التدريب على الإبلاغ عن حوادث العنف الجنسي وإدارتها: يمكن أن تؤدي معرفة كيفية تلقي المعلومات حول حادث عنف جنسي وكيفية تقديم الاستجابة المناسبة له إلى الحد بشكل كبير من إعادة الصدمة وترسيخ الثقة في هياكل ونظم الإبلاغ في المنظمة.
- تقديم تعريفات واضحة عن العنف الجنسي: إن إعلام الموظفين بمعنى العنف الجنسي مثل التحرش الجنسي أو الاعتداء الجنسي سيساعد على وضع سياسة أكثر وضوحاً.



انظر الأداة 2: تصنيف الحوادث للاطلاع على التعاريف المتعلقة بالعنف الجنسي.

الاستجابة الفورية

عند الإبلاغ عن وقوع حادث عنف جنسي أو عندما يلفت طرف ثالث انتباه المنظمة إليه، ينبغي أن يكون المسار الأول للعمل دائماً هو ضمان وجود الناجي في مكان يشعر فيه بالأمان وأنه يتم معالجة احتياجاته الجسدية والعاطفية. وبمجرد الانتهاء من ذلك، هناك عدد من الإجراءات الموصى بها التي ينبغي اتخاذها لضمان عدم تحول معلومات الحادث إلى إشاعة، أو تصعيد الوضع، أو وضع الناجين وغيرهم من الموظفين في خطر.

تتم توصية منسقي شؤون الأمن المعيّنين باتخاذ الإجراءات الفورية التالية:

- **توضيح الخطوات التالية:** التحدث مع الناجي حول مسار العمل الذي يرغب أن تتخذه المنظمة. وينبغي فحص هذا الموقف بشكل روتيني لمعرفة ما إذا كان الناجي لا يزال مرتاحاً.
- **السرية:** التأكد من أن الموظفين الآخرين المطلعين عن الحادث لا يتحدثون عنه مع أولئك الذين لا يعرفون. من المستحسن منحهم استجابة موحدة إذا تم طرح أسئلة، على سبيل المثال. “لا أستطيع الإجابة على هذا السؤال، يرجى الاتصال بالممثل المقيم.”
- **الاتصالات:** إنشاء خط اتصال مباشر مع جهة اتصال محددة في المقر الرئيسي. وينبغي أن تتم إدارة الاتصالات بين الميدان والمقر من قبل الأشخاص المعيّنين في الميدان فقط. وينبغي ألا تنطوي هذه الاتصالات على سلسلة من الوسطاء أو العديد من المناوين. ولا ينبغي مناقشة الحالة في مكان يمكن سماع تفاصيلها فيه.
- **إدارة وسائل الإعلام:** اتخاذ إجراءات استباقية تجاه وسائل الإعلام إذا ما كان يبدو أن الحادث سيحصل على تغطية صحفية، وإقناع المحررين والصحفيين باستخدام الأحرف الأولى فقط من اسم الناجي، وليس اسمه الكامل. من المستحسن الاتفاق على رمز أو رقم محدد للإشارة إلى الناجي. ويجب أن تُناقش أية إجراءات يتم اتخاذها بشأن الصحافة مناقشة مستفيضة مع الناجي في حالة إمكانية تحديدها.

- **إدارة التقرير:** يجب تحديد التسلسل الإداري بوضوح قبل وقوع حادثة، ومن ثم اتباعه عند تقديم التقرير. ويجب أن يشمل التسلسل خطوطاً بديلة للإبلاغ على الصعيد الميداني، بما يكفل وجود أفراد متعددين من الجنسين ومن مختلف الخلفيات الثقافية يمكن رفع التقارير لهم. ويجب أن يحصل هؤلاء الأفراد على التدريب اللازم لتلقي تقارير عن العنف الجنسي. وينبغي أن يكون هناك أيضاً تسلسل إداري للإبلاغ يتجاوز المستوى الميداني، في الحالات التي قد تكون فيها الإدارة العليا في الميدان متورطة أو غير موثوق بها للتصدي على نحو مناسب لحادث العنف الجنسي.
- **اتخاذ القرارات الإدارية:** نظراً لحساسية المعلومات، يجب اتخاذ تدابير محددة لضمان عدم فقدان الإحصاءات المتعلقة بحوادث العنف الجنسي، بحيث يتم تضمين تدابير التخفيف والإدارة على جميع مستويات السياسة والممارسات الأمنية للمنظمة.

ينبغي إتاحة المعلومات المتعلقة بكيفية إعداد وتقديم التقارير على نطاق واسع بلغة بسيطة وواضحة وفي أماكن مختلفة على طول عمليات المنظمة. ويمكن أن يشمل ذلك وضع نسخ ورقية من العملية في كل مكتب ميداني، بما يكفل قدرة الأشخاص الذين لا يستطيعون الوصول إلى الحواسيب على الحصول عليها. وإضافة إلى ذلك، ينبغي إتاحة المعلومات المتعلقة بعملية تقديم التقارير بجميع اللغات ذات الصلة في بيئة التشغيل. وإذا كان الإلمام بالقراءة والكتابة مصدر قلق، ينبغي استخدام الوسائل الخلاقة لضمان فهم الجميع لحقوقهم وكيفية التصرف في حالة حدوث العنف الجنسي. ويجب عند وضع نظم الإبلاغ ورفع التقارير أخذ المعايير الثقافية المحلية في عين الاعتبار وقد تكون مختلفة بالنسبة للموظفين المختلفين، على سبيل المثال: الموظفين المحليين والدوليين.

جمع المعلومات

بعد صدور التقرير الأولي، ينبغي جمع معلومات إضافية تتعلق بالحدث. ومن المرجح أن يتطلب جمع المعلومات الأمنية اللازمة في هذه الظروف تدريباً خاصاً ومهارات خاصة من أجل معالجة الحادث بحساسية ومهنية وشمولية، وبطريقة لا تضر بالمتورطين فيه.

تقدم النصائح التالية توجيهات إلى الموظفين الذين يجمعون المعلومات فيما يتعلق بحادث العنف الجنسي:

- عندما تحدث مع الناجي حول الحادث وتطلب منه معلومات عنه، عليك التحلي بالصبر والتحدث ببطء، وإعطائه بعض الوقت للاستراحة وجمع وترتيب أفكاره. ابدأ بأسئلة عامة مفتوحة حتى يتم ذكر التسلسل الكامل للأحداث مرة واحدة. ويمكن طرح الأسئلة المتعلقة بتفاصيل محددة بمجرد تقديم تفسير عام.
- عليك إدراك حقيقة أن طلب هذه المعلومات قد يعيد الصدمة إلى ذهن الناجي. يمكنك جعل هذه العملية أسهل من خلال توفير الوقت والمساحة اللازمة للناجين للحديث عن تجربتهم، ومن خلال توفير مكان وجو آمن لهم، وأيضاً من خلال التحلي بمهارات الاستماع المتعاطف والنشط.
- ينبغي طرح الأسئلة في بيئة يشعر فيها الناجي بالأمان والراحة. وينبغي احترام وتشجيع خياره باصطحاب زميل أو صديق أو جهة اتصال موثوق بها. وجود عناصر مثل الماء والمناديل سوف يساعد على خلق جو يشعر فيه الناجي بالدعم.
- لا تطرح الأسئلة التي تعزز أساطير الاغتصاب أو السلوكيات التي تتسبب في إلقاء اللوم على الضحية. مثل: "هل أنت متأكد من أن هذا ما حدث؟"، "ماذا كنت ترتدي؟"، أو "ماذا فعلت لتسبب هذا الحدث؟".

- حيثما كان ذلك ممكناً، قم بجمع ملابس الناجي أو أي مواد أخرى من شأنها المساعدة في إثبات وقوع عنف جنسي في محكمة قانونية. ويجب تخزين هذه الأشياء بشكل نظيف ودقيق كلما سمحت الظروف بذلك.
- إذا لم يقرر الناجي بالاستحمام أو تنظيف نفسه، شجّعه على طلب الرعاية الطبية، إذا كانت متاحة، (بما في ذلك الرغبة في تناول حبوب منع الحمل أو أدوية الوقاية بعد التعرض). تأكد من أن إجراءات التشغيل الموحدة تشمل الوصول إلى واستخدام حبوب منع الحمل وأدوية الوقاية بعد التعرض.
- عند طرح الأسئلة على الناجي، تأكد من أن يكون في مكان آمن مع حصوله على دعم كاف بعد ذلك. وعلى الرغم من أن دورك قد يتمثل بالدرجة الأولى في طرح الأسئلة، إلا أنه يجب عليك أن تؤكد أن بإمكانه الحصول على الدعم النفسي والاجتماعي الضروري، والإشارة إلى سبل الوصول إلى هياكل الدعم هذه، وإذا لزم الأمر اتخاذ خطوات لضمان ذلك.
- أكد للناجي في كافة مراحل الاستجواب بأنه يتم تصديق ما يقوله، وأنه سيتم إبلاغه بجميع الخطوات التالية، وأنه لا يستحق ما حدث له.
- بعد جمع التفاصيل ذات الصلة بالحدث، تأكد من تخزين هذه المعلومات بشكل آمن في مكان لا يمكن الوصول إليه أو تسريبه. وحيثما كان ذلك ممكناً، استخدم أسماء مشفرة أو كلمات سرية أو رقم الحالة للإشارة إلى الناجي، حتى في الاتصالات الداخلية.

قد نميل إلى افتراض أن الشخص قد يكون أكثر راحة عند التواصل مع فرد من نفس الجنس، ولكن هذا ليس هو الحال دائماً، ولذلك، ينبغي توفير الخيارات. وينبغي أن تشمل هذه الخيارات، حيثما أمكن، تنوع الميول الجنسية، والجنسيات، والخلفيات العرقية، والأديان، وغيرها من الصفات.

وتجدر الإشارة منذ البداية أنه يجب حماية هوية المعنيين بالحدث أثناء جمع المعلومات المتعلقة بالحالات الحساسة، فضلاً عن الإبلاغ عن مثل هذه الحوادث، وذلك دون المساس بتبادل المعلومات وسلامة المجتمع الإنساني والإنمائي الأوسع نطاقاً. وعندما يتعلق الأمر بالإبلاغ، هناك أيضاً خط رفيع بين الحفاظ على السرية حول الحادث، وهوية الناجي، وإرسال رسالة بأنه على الناجين الشعور بالخجل من تجاربهم. ومن الممكن من خلال اتباع نهج حساس يركز على الناجين تقليل فرص تخطي هذا الخط الرفيع.

كما تجدر الإشارة أيضاً إلى أن سماع الحوادث الحساسة قد يكون صعباً على الفرد الذي يجمع المعلومات كما هو الحال بالنسبة لمن نجا من الحادث. بل وقد يتعرض لبعض الصدمات إثر ذلك، ولذلك ينبغي تقديم الدعم النفسي والاجتماعي لهذا الشخص إذا لزم الأمر.



انظر الأداة 7: الممارسة الجيدة في طريقة الإبلاغ عن حوادث مراعاة الفوارق بين الجنسين وآلية تقديم الشكاوى للإبلاغ عن الاستغلال والاعتداء الجنسيين.

عندما تكون سلامة وأمن موظفي المنظمات غير الحكومية الأخرى على المستوى الميداني معرضة للخطر، يجب تبادل المعلومات المتعلقة بالحدث على النحو المناسب مع المنظمات الأخرى، أو من خلال الشبكات مثل إدارة الأمم المتحدة لشؤون السلامة والأمن (UNDSS) أو منتديات أمن المنظمات غير الحكومية. ويجب على الناجي أن يعطي موافقته المستنيرة على تبادل المعلومات هذا، وينبغي إبراز دوره في ضمان عدم وقوع هذا الحادث للأحرار.



الهدف الثاني: الدروس المستفادة والمطبقة



يناقش هذا القسم إدارة معلومات الحوادث الأمنية بهدف جمع البيانات ومعالجتها وتحليلها وتحويلها إلى معلومات مفيدة واستخلاص الدروس من الحوادث وتنفيذ إجراءات المتابعة. ويغطي هذا القسم:

- 2.1 تحليل ما بعد الحادث
- 2.2 تنفيذ الدروس المستفادة
- 2.3 تحليل وإجراءات متابعة الحالات الحساسة

الأدوات ذات الصلة:

- الأداة 2: شبكات تحليل الحوادث
- الأداة 8: خطة العمل

الهدف الأساسي الثاني لإدارة معلومات الحوادث الأمنية هو تنفيذ الدروس المستفادة بعد وقوع حادث أمني من أجل إجراءات المتابعة والوقاية.

والغرض من ذلك هو فهم ما حدث بهدف التخطيط وتنفيذ أي تغييرات وإجراءات ضرورية تساعد على منع أو معالجة المخاطر أو تقليل تأثير الأحداث المماثلة. ويحدث ذلك عادة على مستوى القطر / المقر الرئيسي بعد فترة وجيزة من وقوع الحادث الأمني.

وينبغي إجراء مراجعة للحادث داخل المنظمة بعد اعتبار الحادث «مغلقاً». وعادة ما يُعتبر الحادث «مغلقاً» من قبل المنظمة عندما يتم إعداد وتنفيذ التقارير المطلوبة واستخلاص الدروس المستفادة والبروتوكولات المحدثة، وعندما يتوقف الحادث عن التطور. ومن شأن تحديد حالة الحادث أن يدعم التحليل.

حالة الحادث مقابل حالة إدارة الحادث

تستفيد المنظمات من تحديد قائمة بأوضاع الحوادث التي ستطبق على الأحداث وإدارتها. وهذا يدعم عملية متابعة معلومات الحوادث وخاصة التحليل ما بعد الحادث:

- حالة الحادث:
- مستمر: لا يزال يحدث.
- انتهى: يُعتبر الحدث الرئيسي "قد انتهى" من قبل المنظمة.
- حالة إدارة الحوادث:
- مفتوحة: انتهاء الحادث الرئيسي ولكن إدارة الأثر وتحليله لا يزال مستمراً. الحادث قيد التحقيق.
- مغلقة: عندما يتم تنفيذ جميع الدروس المستفادة والإجراءات المتخذة.

بالنسبة للحوادث الطويلة الأمد، مثل الاختطاف، من المفيد إجراء مراجعة وسيطة "في الوقت الحقيقي" للإجراءات المتخذة بعد الحادث الأولي بحيث لا تُفقد هذه الدروس.

يمكن إجراء تحليل ما بعد الحادث مع الموظفين المتأثرين مباشرة أو المشاركين في الاستجابات والقرارات التنظيمية التي قد تكون قد ساهمت في التأثير على كيفية وقوع الحادث.

ويتطلب ذلك تحليلاً للمعلومات النوعية من أجل إجراء تقييم صريح للعوامل المساهمة التي زادت من قابلية الضعف والتي تؤثر على ردود الفعل المحددة التي حدثت مع تطور الحادث. وينبغي أن تجرى عملية جمع المعلومات في جو من السرية والثقة. ومن المهم تجنب إلقاء اللوم على الموظفين المتأثرين في أعقاب الحادث.

2.1 التحليل بعد الحوادث

ينظر تحليل ما بعد الحادث في كيفية تأثر الموظفين والمنظمة بشكل مباشر بالحادث وما إذا كان قد تم توفير الرعاية الكافية لهم. ويدرس كيف ساهمت السياسات التنظيمية أو السلوكيات الفردية في جعل الحادث ممكناً، وينظر فيما إذا كان من الضروري وضع إرشادات أفضل. كما يدرس كيف ساعدت الاستجابات التنظيمية (أو أعاق) تخفيف أو حل القضايا التي نشأت عن الحادث.

ويسعى التحليل إلى فهم «لماذا» وقعت الحوادث الأمنية، وفهم الأسباب الكامنة وراء هذه الحوادث الأمنية. ومع ذلك، لن يكون لكل هذا قيمة إلا إذا اتخذت المنظمة بأكملها إجراءات مناسبة لضمان عدم تكرار هذه الحوادث مرة أخرى.

من المستحسن توثيق الأثر الحقيقي للحدث بالإضافة إلى التدابير التي يتعين اتخاذها للحد من احتمال وقوع مثل هذا الحوادث مرة أخرى، والتقليل من أثرها إذا وقعت. وبالنسبة للحوادث الخطيرة، ينبغي أن يتضمن التحليل أيضاً تقييماً لعملية الإدارة، أي ما هي القرارات التي تم اتخاذها، ومتى، ولماذا. ولا بد من أن تكون العملية المكتوبة ضرورية إذا ما أرادت المنظمة أن توثق بشكل منهجي الدروس المستفادة من الحادث وأن تعكس هذا التعلم في العمليات والسياسات المستقبلية، فضلاً عن تقديم أدلة على التعلم التنظيمي لدعم مسؤوليات المنظمة فيما يخص واجب الرعاية.

بعض النقاط الهامة التي يجب مراعاتها عند التخطيط لتحليل الحوادث الأمنية، ويمكن تقسيمها إلى ثلاث مجموعات، على النحو التالي:

أسباب إجراء تحليل الحوادث الأمنية:

- السعي إلى فهم الأسباب الجذرية وراء الحوادث الأمنية.
- التحليل الدقيق هو المفتاح لتحديد إجراءات التخفيف الجديدة أو المحسنة التي يمكن اتخاذها لتعزيز إجراءات التشغيل الموحدة والمستوى العام لأمن المنظمة، مما يمكن من تحسين الوصول إلى السكان المحتاجين.
- يساعد التحليل على تحديد الدوافع وراء الحادث، على سبيل المثال، إذا كان الهجوم متعمداً أم لا. وهذا التمييز مهم لفهم السياق التشغيلي. وإذا كانت الأدلة تشير إلى وقوع حادث متعمد، فإنه يساعد أيضاً على تحديد ما إذا تم استهداف المنظمة عمداً ولماذا.
- من خلال تضمين عناصر التحليل في كل تقرير عن الحوادث الأمنية، يمكن للمنظمة أن تبني بنكاً للمعلومات يدعم تحليل الاتجاه.

ينبغي أن يركز تحليل الحادث على المجالات التالية:

- ما الذي أدى إلى وقوع الحادث، هل تم اتباع الإجراءات وهل هناك حاجة للتغييرات؟
- هل كانت المنظمة أو الفرد مستهدفين؟ هل حصل هذا لأن شيئاً ما أثار الهجوم؟ وهل كان يُنظر إلى الموظف المتضرر بأنه غني أو هدف ضعيف؟
- ألم تعد المنظمة مقبولة في المنطقة؟
- ما هو أثر الحادث على أنشطة البرنامج؟
- هل كانت إجراءات التعامل مع الحادث مناسبة؟

تشمل العوامل المشتركة المساهمة في الحوادث الأمنية ما يلي:

- عدم فعالية إدارة المخاطر الأمنية و / أو عدم الإلمام بالإجراءات.
- الافتقار إلى الوعي الأمني الأساسي والتدريب.
- صورة المنظمة في البلد وكيف يُنظر إليها من قبل السكان المحليين (على سبيل المثال السلوك، الحساسية الثقافية، وما إلى ذلك).
- العلاقات الشخصية والمشاكل الشخصية (بما في ذلك قضايا الموارد البشرية الداخلية).
- الجريمة بسبب الثروة الميرثية أو المتصورة.
- الافتقار إلى المعلومات الذي يؤدي إلى سوء اتخاذ القرارات الأمنية.
- اتخاذ مخاطر غير ضرورية.
- الحوادث الأمنية المرتبطة بالإجهاد.
- الموظفون الذين يتعدون الحدود، أو يشعرون بالراحة الزائدة في العمل في بيئة غير آمنة.



ينبغي للمنظمات أن تتظر فيما إذا كانت تستطيع أن تشارك مع الوكالات الأخرى التحليل النهائي (أو جزءاً منه) لاستنتاجاتها بشأن أسباب الحادث وكيفية إدارة حالات معينة على نحو أفضل.



لمزيد من الإرشادات، راجع الجداول المختلفة في الأداة 5: شبكات تحليل الحوادث



من المهم تحليل الحادث في سياقه الأمني العام (انظر "الهدف الثالث") ولكن أيضاً في ضوء حوادث أخرى، سواء في المنطقة، أو حسب أنماط مماثلة. ويتحقق تحليل الاتجاه هذا من خلال التسجيل المنهجي للحوادث داخل المنظمة. ويناقش هذا بمزيد من التفصيل في إطار "الهدف الرابع".

2.2 تنفيذ الدروس المستفادة

إن الفائدة الأكثر وضوحاً لجمع المعلومات من حادث أمني هي استخدامها على الفور لأغراض البرمجة، مثل تعديل خطط السفر والرحلات الميدانية لتحسين الأمن التنظيمي. وسيتم استخدام مضمون التحليل لتحديد إمكانية الوصول، ومؤشرات المشروع، والتنفيذ، والروابط مع الموارد البشرية، ووضع الميزانية، والرقابة والتقييم على المستوى التشغيلي.

ومن بين الأمثلة الأخرى للدروس المستفادة من معلومات الحوادث نذكر ما يلي:

- التغييرات الفورية في العمليات وتحديث إجراءات التشغيل الموحدة وخطط الطوارئ، ويمكن للنظر في الحوادث المنفصلة معاً أن يؤدي إلى اتخاذ قرارات على الصعيد القطري.
- وضع مؤشرات جديدة لمتابعة السياق الأمني وتقييم المخاطر.
- من شأن تبادل الدروس المستفادة بين المكاتب في جميع أنحاء العالم أن يسمح لهذه المعلومات بتغذية المراجعة الدورية للإجراءات والسياسات وخطط الأمن القطرية.



ينبغي أن تشمل وثيقة تحليل الحوادث الأمنية الجيدة قسماً للإجراءات الموصى بها، المرتبطة بالأسباب المحددة. وتقتصر الممارسة الجيدة إرفاق خطة عمل متابعة مع تقرير تحليل الحوادث لضمان تنفيذ الإجراءات الموصى بها بالفعل.

قد يساعد استخدام نظام تقنية المعلومات في المؤسسة على ربط خطة العمل مع أدوات التخطيط وإرسال تذكيرات وإخطارات للموظفين المسؤولين.



انظر الأداة 5: شبكات تحليل الحوادث، للاطلاع على أمثلة على الإجراءات التي يمكن تنفيذها بعد إجراء تحليل فيما يتعلق بأسباب الحوادث.

انظر الأداة 8: خطة العمل، للاطلاع على المعلومات التي يجب أن تتضمنها خطة عمل المتابعة.

2.3 التحاليل وإجراءات متابعة الحالات الحساسة

يجب أن يراعي تحليل الحوادث المبادئ التالية: السرية والحياد والمهنية.

في حال وقوع العنف الجنسي داخل المنظمة، فإن الوظيفة الرئيسية لمرحلة التحليل، لأغراض هذا الدليل، هي تحديد الخطوات التي يتعين اتخاذها إدارياً أو قانونياً. وسيختلف هذا الأمر اختلافاً كبيراً بين المنظمات والسياسات التشغيلية.

وإذا أمكن القيام بذلك دون الكشف عن تفاصيل حساسة حول الحادث أو الناجي، فإنه يتم التشاور مع أولئك الذين يشغلون مناصب مماثلة على المستوى الميداني لجمع المعلومات حول الوضع الأمني الأوسع وغيرها من حوادث العنف الجنسي على المستوى الميداني.

يمكنك استخدام هذه الأداة وأي أدوات أخرى لإجراء التحليل الأمني وتحديد ما إذا كان الموظفون الآخرون أو المنظمة أو مجتمع المنظمات غير الحكومية الأوسع عرضة لخطر التعرض للعنف الجنسي أو غيره من أشكال العنف.

وينبغي أن يشمل تحليل هذه الأنواع من الحوادث أيضاً تحليلاً للأثر، بما في ذلك الصدمات الأولية والبدلية، فضلاً عن التدريب وغيره من الإجراءات التفاعلية المطلوبة لمنع وقوع مثل هذه الحوادث في المستقبل.

ينبغي التشاور مع جهات التنسيق الضرورية - على مستوى الميدان والمقر الرئيسي - لتحديد إجراءات المتابعة المطلوبة وضمان تنفيذها. وقد يلزم إجراء مشاورات إضافية مع الموارد البشرية أو الخدمات القانونية أو الأخلاقية أو الخدمات الطبية، وذلك حسب ما تقتضيه المنظمة. وينبغي أن تكون المعلومات التي تتم مشاركتها على أساس الحاجة إلى المعرفة، ويجب اتخاذ الخطوات الضرورية لتيسير الإجراءات القانونية بناء على طلب الناجي، وبموافقته المستنيرة. قد تختلف إمكانية اتخاذ إجراء قانوني اختلافاً كبيراً في سياق معين حسب طبيعة الفرد وبيئة التشغيل القانونية. ويجب أن تحكم احتياجات ورغبات الناجين في متابعة المسألة أي إجراءات قانونية. يجب التشاور مع الموظفين الوطنيين والجهات الفاعلة الأخرى للنظر فيما إذا كانت العدالة القانونية ممكنة في السياق، وأي مخاطر قد تواجه الناجي بسبب اتخاذ هذا الطريق. ففي بعض المواقع، قد لا يكون هذا خياراً واقعياً على الإطلاق، وفي مثل هذه الحالات قد تكون هناك حاجة إلى إدارة التوقعات.

حتى لو كان معروفاً أن شخصاً ما في المنظمة قد تعرض للعنف الجنسي، أو حتى عندما يتخذ الناجي خطوات للإبلاغ عن الحادث، فإن هناك العديد من العناصر التي يجب مراعاتها. أولاً، إن المضي قدماً في تقديم التقارير لا يعني تلقائياً أن الناجي يريد مشاركة التفاصيل ومناقشتها على نطاق واسع. وفي جميع مراحل عملية إعداد التقارير، ينبغي إبلاغ الناجي والحصول على موافقته على من سيطلعون على تجربته هذه. وتقع على عاتق الموظفين المعنيين، والمدير، والمنظمة مسؤولية حماية هوية الناجي وسرية تفاصيل القضية.²¹

²¹ مباشرة

ينبغي أيضاً احترام رغبة الناجي في الإبلاغ عن هويته أو مشاركتها، أو مشاركة التفاصيل المحددة الأخرى. وينص النهج الذي يركز على الناجيين في التصدي لحالات العنف الجنسي على أن قرارات الناجين ورغباتهم هي التي تُملي مسار عملية تقديم التقارير.

ينبغي إبلاغ الناجي عن المعلومات المتعلقة بالسرية بطريقة توضح أن احترام رغبته في الحفاظ على سرّية سماته التعريفية لا يعني بالضرورة أن عليه القيام بذلك، وأنه لا يجب عليه الشعور بالعار لكونه تعرّض إلى عنف جنسي. كما ينبغي التأكيد أيضاً من أن الناجي يعرف أن بوسعه الإفصاح عن هويته في وقت لاحق، إذا كان هذا خياره.

ينبغي أولاً مناقشة المعلومات التي سيتم الإبلاغ عنها مع الناجي والحصول على موافقته المستنيرة. وفي بعض الحالات، لا يوجد خيار سوى تقديم تفاصيل عن الحادث إلى الآخرين. وفي هذه الحالة سيساعد السماح الناجيين بأن يكونوا جزءاً من العملية على ضمان بدئهم في استعادة السيطرة التي فقدوها أثناء حادث العنف الجنسي.



ينبغي إبلاغ الأفراد المعنيين فقط بالتفاصيل ذات الصلة، لتقليل فرص وقوع أي ضرر إضافي.

إذا لزم الأمر، ولضمان سلامة الأعضاء الآخرين في المنظمة، قد يجب مشاركة معلومات الحادث مع الموظفين الآخرين. ولكن ينبغي أن يتم ذلك بطريقة حساسة، مع العمل على حماية الناجي قدر الإمكان. وقد يكون سماع معلومات أو أخبار عن حوادث العنف الجنسي أمراً صعباً، ولذلك ينبغي ضمان عدم انتقال الصدمة إلى الموظفين الآخرين، وضمان حصول الجميع داخل المنظمة على الدعم النفسي والاجتماعي.

وفي الوقت الذي تحافظ فيه المنظمة على النهج الذي يركز على الناجيين، يجب عليها أيضاً أن تجد طريقة لضمان الاعتراف بوجود هذا النوع من الحوادث على مستوى القطر والمقر الرئيسي على حد سواء. ونادراً ما يظهر التحرش والعنف الجنسيان في الخطط الأمنية القطرية أو سجلات مخاطر المنظمة، حتى عندما يتم الاعتراف شفويّاً بأنه من المشكلات التي تواجه المنظمات والموظفين.



الهدف الثالث: فهم السياق



يناقش هذا القسم فوائد فهم السياق التشغيلي وكيفية فعل ذلك. حيث يسلط الضوء بشكل خاص على كيفية التعاون مع المنظمات الأخرى لغايات تبادل معلومات الحوادث بالإضافة إلى مصادر الحصول على معلومات السياق. يغطي هذا القسم:

- 3.1 التطبيقات العملية لمشاركة المعلومات الأمنية
- 3.2 المشاركة الخارجية لمعلومات الحوادث
- 3.3 منتديات مشاركة معلومات الحوادث الأمنية
- 3.4 المصادر الخارجية لتحليل أنماط السياق

الأدوات ذات الصلة:
الأداة 2: تصنيف الحوادث

يتمثل الهدف الرئيسي الثالث لإدارة معلومات الحوادث الأمنية في فهم السياق الأمني التشغيلي للمنظمة. تتيح المعرفة الجيدة للسياق للمنظمات فرصة اتخاذ قرارات أمنية وتشغيلية سليمة على المستوى القطري والإقليمي والمقر الرئيسي. ويُعدّ تحليل أنماط الحوادث المبلغ عنها من قبل منظمات أخرى المصدر الأكثر فعالية عن معلومات السياق الأمني المحدد.

من أجل الحصول على فهم أشمل للسياق وتحقيق أفضل استخدام استراتيجي لمعلومات الحوادث الأمنية يجب أن تشتمل التحليلات الأمنية على معلومات عن الحوادث من أكثر من منظمة ومن عدة مصادر.

“

“بالإمكان الحصول على معلومات السياق الأمني العام من مصادر متعددة، من بينها المنظمات الأخرى ووسائل الإعلام (بما في ذلك وسائل الإعلام الإنسانية والإعلام المرتكز على التنمية) والمعلومات التي يوفرها مقدمو الخدمات المتخصصون الذين يمكنهم تقديم تقارير عامة عن البلدان أو توقعات المخاطر والتي تحتاج إلى اشتراك في معظم الأحيان.”

غالباً ما تجد المنظمات غير الحكومية أنه من المفيد مقارنة الحوادث الخاصة بها مع منظمات مماثلة، سواء كان ذلك من حيث التخصص البرامجي (مثل الإغاثة أو التنمية أو حقوق الإنسان، وما إلى ذلك) أو حجم المنظمة (من حيث الحضور أو عدد الموظفين). أما المنظمات الأصغر حجماً، قد يكون ضرورياً الحصول على معلومات إضافية عن الحوادث في نفس البلد قبل تحديد أي أنماط.

يُعدّ تحليل أنماط الحوادث التي أبلغت عنها منظمات مختلفة من أكثر مصادر المعلومات فعالية في السياق الأمني المعني. ويمكن للمنظمات أن تستخدم مخرجات التحليلات المأخوذة من النظرة العامة على الحوادث الأمنية من أجل قياس الأنماط الخاصة بها وإبلاغ الاستراتيجيات والتواصل داخل المنظمات والقطاع الإنساني والإنمائي ككل.

ومن الممكن أيضاً أن يكون تحليل الأنماط أداة مفيدة للتواصل مع وسائل الإعلام والتأثير على الرأي العام والمانحين الحكوميين.

3.1 التطبيقات العملية لمشاركة المعلومات الأمنية

تصنيف المعلومات - من السري للعام

من الممكن أن تكون مشاركة بعض المعلومات أمراً إلزامياً للمنظمات ومسألة تتعلق بسياساتها الداخلية. وكجزء من التأهب التشغيلي، يجب على المنظمات غير الحكومية أن تقرر ما هي معلومات الحادث التي ترغب في مشاركتها خارجياً، ولأية غايات. يقدم الجدول أدناه مثلاً عن كيفية تأثير حساسية المعلومات على الوصول في جميع مستويات إدارة معلومات الحوادث الأمنية، من موقع الحادث إلى مستوى أكثر استراتيجية داخل المنظمة وبين المنظمات أيضاً.

التصنيف	الوصول
معلومات سرية: للمعلومات السرية قيمة كبيرة بالنسبة للمنظمة، وقد يؤدي الإفصاح عنها أو نشرها بشكل غير مصرح به إلى إلحاق ضرر شديد بالسمعة أو حدوث أثار غير مرغوبة على عمليات المنظمة.	يُمنح حق الوصول إلى المعلومات السرية بشكل حصري للأشخاص المعنيين الذين يجب عليهم معرفتها، ويتم ذلك بأقل درجة ممكنة ("مبادئ الحاجة إلى المعرفة" و"أقل الامتيازات"). عند الاحتفاظ بالمعلومات السرية خارج مكاتب المنظمة مثل أجهزة الكمبيوتر المحمولة أو الأجهزة اللوحية أو الهواتف، يجب حمايتها داخل أجهزة مخصصة وأجهزة تشفير و/أو منصات بريد إلكتروني مشفرة. وينطبق ذلك بوجه خاص على الحالات الحساسة، مثل العنف الجنسي. وفي مثل هذه الحالات، فإن أي تبادل للمعلومات يحتاج إلى موافقة صريحة من الشخص المتضرر.
معلومات مقيّدة: لا يتم الإفصاح عن هذه المعلومات أو نشرها، لأنها قد تؤثر على حياة الناس، ويمكن أن تسبب بعض الدعاية السلبية أو ضرر محدود على سمعة المنظمة أو خسائر مالية محتملة للمنظمة.	تخضع المعلومات المقيّدة لضوابط على الوصول لمجموعة صغيرة من الموظفين. يجب الحفاظ على هذه المعلومات بطريقة تحول دون الوصول غير المصرح به، مثل حفظها على نظام يحتاج إلى اسم مستخدم فعال ومناسب من أجل تسجيل الدخول قبل منح حق الوصول إلى المعلومات.
معلومات الاستخدام الداخلي: يؤدي نشر هذه المعلومات إلى الجهات ذات العلاقة إلى ضمان حسن سير العمل التنظيمي والاستجابات الداخلية المناسبة داخل المنظمة. ولن يؤدي نشرها إلى أي ضرر بالمنظمة أو موظفيها، ولكنه يعتبر غير مرغوب فيه.	ويمكن الكشف عن معلومات الاستخدام الداخلي أو نشرها على الأعضاء المناسبين في المنظمة والشركاء وغيرهم من الأفراد، حسبما يراه مالك المعلومات مناسباً، دون أي قيود على المحتوى أو وقت النشر.
معلومات عامة: لن يُعرض نشر المعلومات في الأخبار ووسائل الإعلام وغيرها من القنوات المنظمة أو موظفيها لأي خطر. ويعتبر إطلاقها مرغوباً أو غير قابل للاعتراض على الأقل.	يمكن الكشف عن المعلومات العامة أو نشرها دون أي قيود على المحتوى. يجب ألا ينتهك الإفصاح عن المعلومات أو نشرها أي قوانين أو تعليمات سارية، مثل قوانين الخصوصية.

يجب أيضاً عند تحديد تصنيف المعلومات أخذ مدى أثر "عدم المعرفة" على الجهات ذات العلاقة بعين الاعتبار.

على سبيل المثال، وقع حادث اختطاف على طريق تستخدمه بكثرة المنظمات غير حكومية المتعددة والتي تعمل في المنطقة. يمكن اعتبار هذا الحادث كمعلومات سرية، حيث أن نشر التفاصيل حول الحادث يمكن أن يكون له تأثير خطير على الجانب النفسي للموظفين، والقدرة على تنفيذ البرامج وسمعة المنظمة. غير أن عدم نشر هذه المعلومات في الوقت المناسب قد يؤدي إلى اختطاف الآخرين من المنظمات الأخرى التي تستخدم هذا الطريق. لذلك، فإن معرفة كيف يمكن تبادل المعلومات بأمان أفقياً بين الجهات ذات العلاقة أمر مهم لتصبح أجزاء من معلومات الحادث مقيدة بدلاً من سرية.



يجب ألا يتم الكشف عن بعض المعلومات أو نشرها علناً أو مشاركتها من خلال آلية تبادل المعلومات، مثل أية بيانات شخصية للأفراد المتضررين بحادث ما، بما في ذلك معلومات الاتصال بعائلاتهم وما إلى ذلك.

مشاركة معلومات الحادث ووسائل التواصل الاجتماعي

أصبحت وسائل التواصل الاجتماعي في السنوات الأخيرة مورداً هاماً وذو صلة عندما يتعلق الأمر بالحصول على المعلومات المتعلقة بالأمن أو مشاركتها. يمكن العثور على كمية هائلة من المعلومات الأمنية والسياقية من خلال محركات البحث في تويتر أو فيسبوك.

ويمكن أيضاً استخدام وسائل التواصل الاجتماعي بما في ذلك تويتر وفيسبوك لتنبيه الآخرين (بما في ذلك الجماعات) عن الحوادث أو الحالات الخطرة بطريقة خاصة. لكن تحتاج مصادر المعلومات هذه إلى فهم وتنسيق لضمان الإدارة الآمنة للمعلومات. يمكن مشاركة التوصيات الواردة أدناه مع جميع الموظفين داخل المنظمة وتطبيقها في كل مستوى من مستويات دورة إدارة معلومات الحوادث الأمنية.

توصيات حول وسائل التواصل الاجتماعي والإبلاغ عن الحوادث:

- **تخصيص إعدادات الخصوصية:** ضبط إعدادات الخصوصية على الموقع وتحديد الخيارات التي تحد من الذين يمكنهم مشاهدة المعلومات.
- **فصل المعلومات الشخصية عن المهنية:** استخدام أسماء مستخدمين وصور مختلفة على المواقع المتعددة، لأنه يمكن استخدامها للبحث عن روابط بين المعلومات المهنية والشخصية.
- **وقفة قبل النشر:** تذكر ما إن يتم نشر شيء على الانترنت، فهو سيظل هناك إلى الأبد. حتى المحتوى الذي يتم حذفه يمكن الوصول إليه في بعض الأحيان من قبل الموقع أو من خلال تصوير شاشة المشاركة الأصلية. وقد يشكّل المحتوى الذي يحتوي على معلومات شخصية أو سلوك أو مكان معين خطراً أمنياً.
- **إيقاف تحديد الموقع الجغرافي:** ستطلب العديد من مواقع وسائل التواصل الاجتماعي أو التطبيقات الوصول إلى موقع الجهاز، ولكن في معظم الحالات هذا ليس ضرورياً. بالإضافة إلى الوصول إلى موقع الجهاز، قد تجعل بعض المواقع هذه المعلومات عامة. فعندما "يسجل الأفراد تواجدهم في مكان ما" على مواقع مثل فيسبوك، فإنهم في الواقع يشاركون موقعهم الدقيق مع الآخرين.



“

نظراً لطبيعة المنصات والسرعة التي يتم تبادل المعلومات بها عبر وسائل التواصل، تكون المعلومات غير مؤكدة وقد تكون غير موثوق بها. ينبغي على المنظمات أن تنظر في مصدر وموثوقية المعلومات المتعلقة بالأمن وسريتها قبل اتخاذ أي قرار أو مشاركة المعلومات.

”ينبغي على إدارة مجموعة الواتساب والتي تم إنشاؤها لغرض إبلاغ كل منسق شؤون أمن في المنطقة الإبلاغ عن الحوادث التي تقع في نطاق مسؤوليتهم بعناية. ويجب أن يكون المشرف فقط هو القادر على إضافة أعضاء إلى المجموعة. وينبغي التحقق من صحة أي عضو جديد والإبلاغ عن الإضافة إلى جميع الأعضاء على الأقل. كما ينبغي الاتفاق على قواعد ورموز التواصل وينبغي على المشاركين التأكد من أن الوصول إلى هذه المحادثات محمي في حالة فقدان هواتفهم أو سريتها“.

3.2 المشاركة الخارجية لمعلومات الحوادث

المشاركة مع المنظمات الأخرى

إن مشاركة المعلومات الأمنية، والإبلاغ عن الحوادث والأوضاع الأمنية، ومسح مواقع الخطر بين المنظمات لا يأتي بشكل طبيعي.²² لكن من المتعارف عليه على نحو متزايد أن مشاركة المعلومات الأمنية في سياق تشغيلي محدد والإبلاغ السريع عن الحوادث للمنظمات غير الحكومية الأخرى في المنطقة هو مسؤولية جماعية.²³

يمكن للمنظمات تبادل المعلومات مباشرة مع بعضها البعض، من خلال المنتديات أو من خلال منصات مشاركة المعلومات الأمنية (انظر “منتديات مشاركة معلومات الحوادث الأمنية” و “مصادر تحليل الأنماط السياقية الخارجية” أدناه).

- للأسف، هنالك العديد من الحواجز التي تعيق مشاركة المعلومات الأمنية بين المنظمات: يحتاج جمع البيانات للحصول على نظرة عامة جيدة لأنماط الحوادث الأمنية الفريدة للمنظمات غير الحكومية أن تكون المنظمات نفسها مستعدة لمشاركة تفاصيل الحوادث الأمنية بناءً على اتفاقيات السرية.
- قد يعيق الهيكل التنظيمي للمنظمة ورسالتها وثقافتها، والمفاهيم العشوائية والإقليمية والدينية والتاريخية والعرقية الخاطئة التعاون ومشاركة المعلومات الأمنية ذات الصلة.
- قد ترى بعض المنظمات (أو الأفراد داخل المنظمة) الأمن عائقاً أمام العمليات، في حين قد يشدد آخرون على استقلاليتهم، وعدم الارتباط أو التعاون مع الجهات الأخرى ذات العلاقة في المنطقة.
- يمكن أن يؤدي تعارض الشخصيات بين الجهات الفاعلة في المسائل الأمنية إلى إعاقة التعاون بشكل ملحوظ. ولكون العلاقات بين الأفراد عاملاً مهماً لترسيخ الثقة، فإن الشبكات الرسمية توفر أساساً لبناء هياكل أكثر رسمية لمشاركة المعلومات والتي لا تعتمد فقط على الشخصية حتى تضمن الاستمرارية في حال تغيير الموظفين.
- غالباً ما يعيق عدم توفر الموارد البشرية والمالية للأمن المنظمات من المساهمة أو المشاركة الكاملة في الجهود التعاونية.

- يمكن أن يختلف نهج الأمن اختلافاً كبيراً بين المنظمات. هذه الاختلافات يمكن أن تجعل التعاون الأمني المشترك أمراً صعباً، لكن التنسيق ومشاركة المعلومات سيساعد جميع الأطراف على فهم السياق على نحو أفضل وتنفيذ تدابير واقعية وأكثر فعالية لإدارة المخاطر الأمنية.
- قد تكون المخاوف المتعلقة بالاستخدام غير المناسب للمعلومات الحساسة والتي تتم مشاركتها من خلال آليات التنسيق عائقاً كبيراً أمام مشاركة المعلومات. هناك بعض الأمثلة على معلومات تمت مشاركتها في مثل هذه المنتديات وانتهى بها المطاف منشورة في الصحافة، على الرغم من أنها هذا كان استثناءً. ومن المهم أن تكون على علم تام بآلية تنسيق ومعالجة المعلومات وتوقعات ومسؤوليات التعامل مع المعلومات وعواقب أي خرق لشروط الاتفاق.
- يعتبر الأمن أولوية واحدة فقط من بين أولويات المنظمات المتعددة عند تنفيذ البرامج. ومع ذلك، فقد تبين مراراً وتكراراً أن الممارسات الأمنية غير المناسبة وانعدام التنسيق من جانب إحدى المنظمات يمكن أن يؤثر على قدرة المجتمع بأسره على اكتساب فرص الوصول إلى العمليات الإنسانية والإنمائية والحفاظ عليها.



عندما يتم تحديد الحواجز التي تحول دون مشاركة المعلومات، ينبغي أن يعتمد المتعاونون على حريتهم وقيمهم لإيجاد أرضية مشتركة والعمل على التوصل إلى حل متفق عليه بصورة متبادلة.

من المهم أن نتذكر أن سلوك إحدى المنظمات قد يكون له أثر على أمن الجميع. فإذا لم تقم منظمة ما بمشاركة معلومات الحوادث الهامة، بما في ذلك الحوادث الوشيكة، فقد يؤدي ذلك إلى تهديد كبير على منظمات أخرى بدلاً من أن تكون قادرة على تجنب أو تقليل تأثير هذا التهديد. ويعد التعاون عنصراً أساسياً في المعرفة السياقية والأمن التنظيمي العام.

مشاركة المعلومات مع المانحين

ترسل بعض المنظمات تقارير تحليل ما بعد الحادث إلى الجهات المانحة مع التقارير ربع السنوية أو المتوسطة الأجل إذا كان هناك انقطاع في تنفيذ البرنامج نتيجة لزيادة انعدام الأمن أو ازدياد أعداد الحوادث. وتساعد هذه التقارير الجهات المانحة على تقديم معلومات عن الحالة على أرض الواقع واتخاذ القرارات المتعلقة بتمديد البرامج. وينبغي للمنظمة أن تقرر استراتيجياً ما إذا كانت ترغب في تبادل تقارير الحوادث مع الجهات المانحة، مع ضمان امتثالها لأي متطلبات تعاقدية.

3.3 المنتديات ومشاركة المعلومات الأمنية

يمكنك أن تجد أدناه معلومات وتفاصيل حول بعض المنتديات والمجموعات المتخصصة للتنسيق الأمني والتعاون المعني بجمع وتحليل ومشاركة معلومات الحوادث الأمنية.

لكل منها غاية مختلفة، وبالتالي آليات متعددة لجمع ومشاركة المعلومات. ومع ذلك، كلها مصادر ممتازة للمعلومات ويمكن أن تساعد في تحسين إدارة المخاطر الأمنية.

- **منصات قواعد بيانات الحوادث العالمية**
 - قاعدة بيانات Aid Worker Security
 - قاعدة بيانات Security in Numbers Database (SiND)
- **على مستوى المقر الرئيسي**
 - منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)
 - InterAction (الولايات المتحدة الأمريكية)
 - Dutch Security Network
 - مجموعة منسقي شؤون الأمن في المنظمات غير الحكومية في المملكة المتحدة
 - CINFO: مجتمع الممارسة الأمنية (سويسرا)
 - الفريق العامل المعني بالأمن (إسبانيا) (Coordinadora Security Working Group)
 - منتدى الأمن الكندي المشترك بين الوكالات (Canadian Interagency Security Forum)
- **على المستوى الإقليمي**
 - منتدى الأمن والسلامة الإنسانية في منطقة الشرق الأوسط وشمال إفريقيا
 - منتدى الأمن الإقليمي لغرب إفريقيا
- **على المستوى القطري**
 - منظمة سلامة المنظمات غير الحكومية الدولية
 - (International NGO Safety Organisation) (INSO) ومكاتبها الإقليمية
 - المنتدى الإنساني الباكستاني
 - منتدى المنظمات غير الحكومية - جنوب السودان (NGO Forum - South Sudan)
- **مصادر أخرى**
 - اجتماعات خلية الأمن مع وكالات الأمم المتحدة، ضمن إطار عمل
 - (SLT) Saving Lives Together

بعض المعلومات التي تقدمها هذه المنتديات عامة (مفتوحة المصدر) في حين أن البعض الآخر قد يتطلب وجود العضوية. يجب على المنظمات التواصل مع المنتديات العالمية والإقليمية والمحلية و/أو الميدانية بشأن التنسيق المتعلق بالأمن ومشاركة المعلومات حسب الحاجة وعندما يكون ذلك متاحاً.

3.4 مصادر تحليل أنماط السياق الخارجية

“

”قد تجد المنظمات غير الحكومية أنه من المفيد مقارنة أنماط الحوادث مع اتجاهات المنظمات المشابهة. ويتطلب هذا النهج مشاركة بيانات الأنماط الرئيسية بين المنظمات في شكل مجهول المصدر ولا يسمح بتحديد هوية منظمة واحدة“.

يجب أن يأخذ مدراء الأمن والمحللون بعين الاعتبار تحليل معلومات الحوادث الداخلية وكذلك المعلومات الأمنية التي يتم جمعها خارجياً، ولا سيما من خلال شبكات مشاركة المعلومات.

تعطي معلومات الحوادث الخارجية معرفة سياقية أقوى للبيئة التشغيلية للمنظمات غير الحكومية.

إن استخدام التصنيفات الأساسية يسهل مقارنة المعلومات بين المنظمات. يتم تقديم التصنيفات الأساسية من قبل مشروع Aid in Danger ni Project.

راجع الأداة 2: تصنيف الحوادث



يقدم الجدول أدناه نبذة عن أربعة مصادر رئيسية توفر بيانات الحوادث و/أو الانماط الأمنية استناداً إلى معلومات الحوادث الأمنية التي يتم الحصول عليها من مصادر متعددة. ويلى ذلك معلومات أكثر تفصيلاً عن كل مصدر.

الاسم	المميزات الأساسية
قاعدة بيانات "Security Database" (AWSO) Aid Worker Humanitarian Outcomes والتي تشغلها	تقدم وصفاً للحوادث التي قتل فيها موظفون أو أصيبوا أو اختطفوا. ويقدم التقرير السنوي رؤى وتحليلات للأنماط العالمية.
قاعدة بيانات "Security in Numbers" (SiND) Database in Danger Project (AiD) مشروع الذي تقوم به منظمة Insight Insecurity	توفر قاعدة البيانات هذه نشرة إخبارية شهرية من الأحداث مفتوحة المصدر، ونظرة عامة على الأنماط التي تغطي نطاقاً واسعاً من الحوادث (تتجاوز تلك التي قُتل فيها الموظفون أو أصيبوا أو اختطفوا)؛ وتحليل للحوادث الأمنية التي تجمعها الوكالات وتجمعها. كما يوفر الوصول إلى البيانات عبر Humanitarian Data Exchange.
منظمة International NGO Safety Organisation (INSO)	تقدم معلومات عن الحوادث إلى المنظمات الأعضاء عن البلدان التي توجد فيها. كما يوفر نظام INSO لوحة تحكم تظهر بيانات الحوادث الرئيسية.
إطار عمل Saving Lives Together	يمثل إطار عمل (SLT) Saving Lives Together مبادرة مشتركة بين الأمم المتحدة والمنظمات الدولية والمنظمات غير الحكومية. حيث تتلقى المنظمات الشريكة التابعة لـ TLS مجموعة متنوعة من تقارير الحوادث من إدارة الأمم المتحدة لشؤون السلامة والأمن. (UNDSS)

قاعدة بيانات أمن موظفو الإغاثة

تسجل قاعدة بيانات أمن موظفو الإغاثة (AWSO)، وهي مشروع لمنظمة Humanitarian Outcomes الحوادث الأمنية الرئيسية ضد العاملين في مجال الإغاثة، مع تقارير عن الحوادث من عام 1997 حتى الوقت الحاضر. وتشكل هذه المبادرة، التي بدأت في عام 2005، المصدر العالمي الشامل الوحيد للإحصاءات المتعلقة بالهجمات الكبرى على عمليات الإغاثة المدنية، وتوفر الأدلة الموثقة للتحليل الأمني للبيئة المتغيرة فيما يتعلق بالاستجابة الإنسانية.

يتم جمع بيانات الحوادث من المصادر العامة، من خلال وسائل الإعلام المنتظمة / وسائل التواصل الاجتماعي الموثوقة، ومن المعلومات المقدمة مباشرة إلى المشروع من قبل منظمات الإغاثة والجهات الأمنية التشغيلية. كما ويحتفظ المشروع أيضاً باتفاقات مع عدد من الاتحادات الأمنية الإقليمية والميدانية لمشاركة المعلومات والتحقق من الحوادث بصورة مباشرة. يتم التأكد من صحة تقارير الحوادث والتحقق منها سنوياً مع جميع المنظمات الإنسانية ذات العلاقة على أساس مستمر. ويشمل ذلك الأمم المتحدة والمنظمات غير الحكومية والمنظمات غير الحكومية الدولية بالإضافة إلى اتحادات الأمن داخل البلد.

تتواجد قاعدة بيانات AWSO منذ خمس سنوات على شبكة الإنترنت، وهي قاعدة البيانات التفاعلية الوحيدة من نوعها والمتاحة للعامة. تسمح AWSO للمنظمات بتحميل مجموعة البيانات بأكملها، كما توفر برمجة واجهة التطبيقات للتطوير الخارجي للتطبيقات الأخرى التي تستخدم بيانات AWSO.



يستند التقرير السنوي لأمن موظفو الإغاثة إلى أدلة عملية من البيانات ويقدم أفكاراً وتحليلات بشأن الأنماط والتوصيات العالمية بشأن القضايا الأمنية التشغيلية الحساسة.

للمزيد من المعلومات أو للمشاركة بالمعلومات والتغييرات على AWS، يرجى إرسال بريد إلكتروني إلى info@humanitarianoutcomes.org.



مشروع Aid in Danger Project

يقوم مشروع Aid in Danger التابع لمنظمة Insecurity Insight بانتظام بمراقبة تقارير المصادر المفتوحة عن الحوادث التي تؤثر سلباً على تقديم الإغاثة الإنسانية، ويعمل مع منظمات/شركاء الإغاثة لجمع ودمج تقارير الحوادث الأمنية الخاصة بهم. يتم تخزين كافة البيانات في قاعدة بيانات Database Security in Numbers (SiND) لأغراض التحليل. وقد بدأ المشروع في عام 2008 كجزء من مبادرة Health Care in Danger التي نفذتها اللجنة الدولية للصليب الأحمر. ويسعى مشروع Aid in Danger إلى رصد آثار العنف والأعمال المتعمدة والتي تتعارض مع إيصال الإغاثة. يتتبع مشروع in Danger مجموعة من الحوادث التي تؤثر على إيصال المساعدات: من التهديدات بالعنف إلى القرارات الإدارية التي تؤدي إلى حظر التصاريح أو التأشيرات، وتدمير البنية التحتية، وتأثير الجريمة. كما يرصد المشروع أيضاً عمليات الخطف والوفيات والإصابات التي يتعرض لها موظفو الإغاثة.

إن قاعدة بيانات Database Security in Numbers (SiND) غير متاحة للجمهور وذلك لحماية سرية المنظمات المشاركة. ويتم إتاحة مجموعات من البيانات التي تحتوي على معلومات فرعية محددة بعد إزالة معلومات الهوية الشخصية منها، من خلال صفحة Insecurity Insight في [Humanitarian Data Exchange](https://www.humanitarian.org/).

ينشر مشروع Aid in Danger نشرات عامة شهرية للأحداث المبلغ عنها ذات المصدر المفتوح، وتحديثات منتظمة لتحليلات الأنماط ونظرة عامة على البيانات السرية للوكالة بالتعاون مع منتدى الأمن الأوروبي المشترك بين الوكالات (European Interagency Security Forum).

للمزيد من المعلومات حول مشاركة الوكالات / المنظمات، يرجى إرسال بريد إلكتروني إلى: info@insecurityinsight.org

المنظمة الدولية لسلامة المنظمات غير الحكومية (International NGO Safety Organisation)

تعتبر المنظمة الدولية لسلامة المنظمات غير الحكومية آلية التنسيق الأمني الرئيسية للمنظمات غير الحكومية العاملة في السياقات شديدة الخطورة، ولديها أكثر من 850 عضواً في جميع أنحاء العالم.

تأسست المؤسسة الخيرية البريطانية في عام 2011، وهي تعمل في الميدان لتزويد المنظمات غير الحكومية المسجلة معها بمجموعة من الخدمات المجانية بما في ذلك تتبع الحوادث في الوقت الحقيقي، والتقارير التحليلية والبيانات المتعلقة بالسلامة ورسم الخرائط، ودعم الحوادث الحرجة وإدارة الأزمات والسياسات الداخلية واستعراضات الموقع، وتوجيه الموظفين والتدريب على السلامة الشخصية، وإدارة الأمن، وإدارة الأزمات.

تعمل منصات المنظمة حالياً في أفغانستان والعراق وسوريا وفلسطين (غزة) والصومال وكينيا وجمهورية الكونغو الديمقراطية وجمهورية أفريقيا الوسطى والكاميرون ونيجيريا ومالي وأوكرانيا، مع وجود منصات جديدة تفتتح سنوياً.

يقتصر التسجيل لدى منظمة INSO على المنظمات غير الحكومية المحلية والدولية ويجب تقديم طلب التسجيل في بلد العمل الإغاثي. تعمل منصات INSO على تطبيق قواعد سلوك صارمة يشارك فيها الأعضاء المعلومات مع بعضهم البعض بشكل سري.



على الصعيد العالمي، تقدم المنظمة بيانات الإحصاء والمعلومات الدقيقة عن الحوادث الأمنية للمنظمات غير الحكومية في الوقت المناسب من خلال لوحة البيانات الرئيسية، وسيتم في عام 2018 إطلاق Conflict & Humanitarian – Data Centre (CHDC) - وهو قاعدة بيانات مركزية تحتوي على جميع الحوادث التي يتم جمعها عبر شبكة المنصات الميدانية.

مع أكثر من مليون إدخال أولي، فإن CHDC ستكون واحدة من أكبر المستودعات العالمية من نوعها وسوف تدعم البحوث السياقية طويلة المدى، فضلاً عن التحليل الاستراتيجي السريع.

إن المنظمات غير الحكومية المؤهلة وغير المسجلة مدعوة للاتصال بـ INSO عبر صفحة التسجيل الخاصة بها أو من خلال info@ngosafety.org

“

في بعض البلدان، يمكن مراجعة الحوادث الأمنية في سياق الأحداث التي أبلغ عنها INSO. وعلى الصعيد العالمي، يمكن للوكالات الاطلاع على قاعدة بيانات Aid Worker Security Database للأحداث الحرجة المتمثلة في اختطاف الموظفين أو إصابتهم أو وفاتهم. للوصول لمجموعة واسعة من الحوادث، يمكن للمنظمات أن تنضم إلى Security in Numbers Database – Aid in Danger



إطار عمل Saving Lives Together Framework

يمثل إطار Saving Lives Together Framework مبادرة مشتركة بين الأمم المتحدة والمنظمات الدولية والمنظمات غير الحكومية. تم الشروع فيه في عام 2006 ومن ثم تعديله وتنقيحه في عام 2015، وهو يقر بأن الأمم المتحدة والمنظمات الشريكة لها - المنظمات الدولية والمنظمات غير الحكومية - تواجه بشكل جماعي تهديدات أمنية ويسلط الضوء على أهمية التعاون "لضمان إيصال المساعدات الإنسانية والإنمائية بشكل آمن". والهدف من هذه الاتفاقية هو "تعزيز قدرة المنظمات الشريكة على اتخاذ قرارات مناسبة وتنفيذ ترتيبات أمنية فعّالة لتحسين سلامة وأمن الموظفين والعمليات".²⁴ وتتلقى المنظمات الشريكة في إطار SLT تقارير يومية عن الحوادث من إدارة الأمم المتحدة لشؤون السلامة والأمن (UNDSS).

تنظر توصيات إطار عمل SLT بشكل رئيسي في التعاون بين الأمم المتحدة والمنظمات غير الحكومية الدولية، وهي تقدم توجيهات مهمة للمنظمات من أجل لتعزيز التعاون في إدارة المعلومات المتعلقة بالحوادث.²⁵

ويمكن تحميل إطار SLT والتوجيهات من [هنا](#).

للمزيد من المعلومات، يُرجى الاتصال بإدارة الأمم المتحدة لشؤون السلامة والأمن (UNDSS) على المستوى القطري أو على المستوى العالمي من خلال التواصل مع:

السيد Lloyd Cederstrand، مكتب تنسيق الشؤون الإنسانية (OCHA) (التنسيق والاتصال التشغيلي): cederstrand@un.org

مركز اتصالات إدارة الأمم المتحدة لشؤون السلامة والأمن (UNDSS) (مساعدة الاتصالات في حالات الطوارئ على مدار الساعة): undsscomscen@un.org، الهاتف: +1 917 367 9438/9

المدير التنفيذي لمنتدى الأمن الأوروبي المشترك بين الوكالات (EISF): eisf-director@iesf.eu

اللجنة الدائمة المشتركة بين الوكالات (IASC). (2015). "إنقاذ الأرواح معاً - إطار عمل لتحسين الترتيبات الأمنية بين المنظمات الحكومية الدولية والمنظمات غير الحكومية والأمم المتحدة في الميدان. (أكتوبر 2015)". اللجنة الدائمة المشتركة بين الوكالات. لا تعني مبادرة SLT أن الأمم المتحدة تتحمل مسؤولية الأمن للمجتمع الإنساني ككل. لدى الأمم المتحدة موارد مثل طائرات الإجلاء أو معدات الاتصالات التي ستستخدمها كلما أمكن لدعم مجتمع المنظمات غير الحكومية، ولكن هذا الأمر ليس إلزامياً، وسيتم تمرير أي تكاليف خاصة به إلى المنظمة، ويتعين على المنظمة غير الحكومية تحمّل مسؤولية



الهدف الرابع: اتخاذ القرارات الاستراتيجية



يناقش هذا القسم إدارة معلومات الحوادث الأمنية في سياق اتخاذ القرارات الاستراتيجية، ولا سيما على المستويات الإقليمية أو المقر الرئيسي. والقصد من ذلك هو مساعدة منسقي شؤون الأمن والمحليين في مجال الأمن على تسجيل معلومات الحوادث الأمنية بطريقة منهجية، واستخدام معلومات تحليلات الاتجاهات، وإبلاغ أصحاب المصلحة الرئيسيين داخل المنظمة وخارجها عن النتائج. والهدف من ذلك هو إطلاع صانعي القرار الاستراتيجيين لضمان أخذ معلومات الحادث في الحسبان في جميع مستويات التخطيط التنظيمي والإجراءات والمشاريع. يغطي هذا القسم ما يلي:

- 4.1 التسجيل النظامي للحوادث: ما هو النظام الذي يتعين استخدامه؟
- 4.2 تحليل الاتجاهات للاسترشاد بها في اتخاذ القرارات الاستراتيجية
- 4.3 الهياكل التنظيمية لمناقشة قضايا الأمن الاستراتيجي
- 4.4 كيفية استخدام معلومات حوادث العنف الجنسي على المستوى الاستراتيجي
- 4.5 استخدام معلومات الحوادث الأمنية للدعوة الاستراتيجية

الأدوات ذات الصلة:

- ◀ الأداة 2: تصنيف الحوادث
- ◀ الأداة 9: أنظمة إدارة معلومات الحوادث الأمنية
- ◀ الأداة 10: حفظ الحوادث
- ◀ الأداة 11: التقنية المستخدمة في الإبلاغ عن الحوادث وتسجيلها
- ◀ الأداة 12: تحليل اتجاهات البيانات
- ◀ الأداة 13: الأسئلة الاستراتيجية المتعلقة باتخاذ قرارات إدارة معلومات الحوادث

يتمثل الهدف الرئيسي الرابع لإدارة معلومات الحوادث الأمنية في إرشاد وتوجيه عملية اتخاذ القرارات الاستراتيجية داخل المنظمة.

ينبغي إجراء تحليل منتظم على مستوى المقر الرئيسي لتحديد الاتجاهات والأنماط التي تساعد على اتخاذ القرارات الاستراتيجية على المدى الطويل بالنسبة للمنظمة بأكملها. والغرض من ذلك هو تقييم طبيعة الحوادث الأمنية المتغيرة، وفهم بيانات العمل الأكثر تحدياً، والتعرض الإجمالي للمخاطر في المنظمة، وتحديد أفضل الاستجابات الاستراتيجية.

وقد أصبح المنظور العالمي أكثر أهمية مع التحسينات التي شهدتها تقنيات الاتصالات وتوافر المعلومات في جميع أنحاء العالم. ولم يعد من الممكن النظر إلى الحوادث على أنها قضية قطرية محضة. على سبيل المثال، قد تؤدي حملة تنظيمية في منطقة واحدة إلى مظاهرات في مكتب على الجانب الآخر من العالم.

لدى تحليل معلومات الحوادث آثار على الإدارة الجيدة على نطاق أوسع، والتي يمكن أن تشمل القرارات حول:

- مكان التشغيل.
- كيفية التواصل حول البرامج.
- ما هي وثائق التأمين المطلوبة.
- إلى أي مدى ينبغي إدراج إدارة المخاطر الأمنية في الميزانية ضمن العمليات القطرية.

ويمكن أيضاً استخدام التحليل الأمني لإبراز الشواغل الأوسع نطاقاً بشأن المهام الأساسية للمنظمة والصعوبات في الوصول إلى السكان المستفيدين.

تقوم بعض المنظمات بهذا النوع من التحليل على أساس سنوي، بينما يجري بعضها الآخر ذلك بشكل متكرر أكثر. وبالإضافة إلى المراجعات المخططة مسبقاً، ينبغي إجراء مراجعات مخصصة كلما حدث تغيير كبير في مهمة المنظمة أو مواصفاتها أو سياقاتها التشغيلية. وتستفيد كل منظمة غير حكومية من مناقشة مواصفات الحوادث الأمنية بانتظام. ويتحقق هذا التحليل من خلال تدفق المعلومات الفعّال بين المكاتب الميدانية والمقر الرئيسي، ووجود نظام فعّال يسجل الحوادث المُبلغ عنها بطريقة منهجية وموحّدة لتيسير التحليل المقارن واتخاذ القرارات الاستراتيجية.

ينبغي أن يأخذ اتخاذ القرارات الاستراتيجية المتعلق بمعلومات الحوادث الأمنية في الاعتبار تحليل معلومات الحوادث الداخلية وكذلك المعلومات الأمنية التي تُجمع خارجياً، ولا سيما من خلال شبكات تبادل المعلومات. ويمكن أن تبرز مقارنة الاتجاهات الداخلية مع الاتجاهات الخارجية نقاط الضعف الداخلية الرئيسية وعناصر إدارة المخاطر الأمنية التي تتطلب معالجة داخل المنظمة.

4.1 التسجيل المنهجي للحوادث: ما هو النظام الذي ينبغي استخدامه؟

وجود نظام جيد لتسجيل وتخزين وتصنيف واسترجاع بيانات الحوادث الأمنية جزء أساسي من تحليل الحوادث الأمنية واتخاذ القرارات الاستراتيجية. ولدى المنظمات آليات مختلفة للإبلاغ عن الحوادث على المستوى القطري وجمعها وتسجيلها في موقع مركزي. وفيما يتعلق بالنظم الإلكترونية، فهناك العديد من الحلول التي تتراوح بين النماذج المجانية مفتوحة المصدر وسهلة التخصيص الذاتي إلى الأنظمة المصممة خصيصاً من قبل الشركات التجارية.

وبصرف النظر عن النظام الذي تستخدمه المنظمة، فمن المهم أن يكون نظام تسجيل الحوادث ورسم الخرائط مصمماً لتلبية احتياجات جميع المستخدمين، بدءاً من تقديم التقارير إلى تحليل الاتجاهات. ويمكن للتقنيات الجديدة أن تساعد في ذلك.

هناك نهجان يمكن للمنظمات غير الحكومية اتباعهما لاستخدام التقنية في تطوير نظام لتسجيل الحوادث ورسم الخرائط:

- حل قائم بذاته مدمج في خوادم ونظم المنظمة؛ أو
- "البرمجيات كخدمة" حيث يتم استضافة النظام من قبل مزود خدمة خارجي.

وستتوقف القرار بشأن النهج الذي ينبغي اتباعه على عوامل عدة مثل الاستراتيجية التقنية وحجم المنظمة، والعدد المحتمل للحوادث، والموارد، والقدرة على إدارة النظام، وحماية البيانات. ويمثل الجدول التالي ملخصاً لبعض الأنظمة المتاحة للإبلاغ عن الحوادث الأمنية التي تؤثر على المنظمة على المستوى المركزي وتخزينها وتحليلها.

النظام	الإبلاغ عن الحوادث وطريقة التسجيل	
يمكن أن يكون ذلك من خلال رسائل البريد الإلكتروني أو جداول بيانات أو وثائق جوجل، أو منصة جوجل مشتركة، أو برنامج شير بوينت (SharePoint). يمكن استخدام جدول بيانات لتصنيف المعلومات المقدمة في شكل مكتوب باستخدام حقول بيانات محددة يجب تعبئتها.	سرد مكتوب عن الحادث، مرتبط بجدول بيانات لتسجيل الحوادث باستخدام الترميز المنهجي	نظام مصمم ومُدار داخلياً
يمكن بناء نظام الإبلاغ عن الحوادث كامتداد للمنصات الحالية المستخدمة للبريد الإلكتروني، مثل شير بوينت (SharePoint). يمكن تخصيص المنصات الجغرافية القائمة على شبكة الإنترنت مثل Ushahidi لإنشاء نظام شامل للإبلاغ عن الحوادث وإدارة المعلومات.	نظام عبر شبكة الإنترنت باستخدام المنصات القائمة مفتوحة المصدر	نظام مصمم ومُدار داخلياً
توفر بعض الشركات الخاصة والمنظمات غير الربحية منصات على شبكة الإنترنت لإدارة معلومات الحوادث الأمنية.	الاشتراك في منصة لإدارة البيانات على شبكة الإنترنت	نظام مصمم ومُدار خارجياً
كلّف بعض المنظمات مزودي الخدمات الخارجيين بتطوير أنظمة إلكترونية خاصة بالمنظمة.	نظام مخصص على شبكة الإنترنت	نظام مصمم ومُدار خارجياً



راجع الأداة 9: أنظمة إدارة معلومات الحوادث الأمنية للحصول على جدول أكثر تفصيلاً يوضح الأنظمة المتاحة لإدارة المعلومات عن الحوادث وملخص لعيوب ومزايا هذه الأنظمة المختلفة.

يمكن للمنظمات الصغيرة أو المنظمات غير الحكومية ذات الموارد المحدودة أن تختار الأسلوبين الأولين لتسجيل الحوادث والإبلاغ عنها، وذلك بالنظر إلى بساطة وسهولة إعداد وصيانة هذه الأنظمة، فضلاً عن تكلفتها المنخفضة نسبياً. وقد تتناسب النظم الأكثر تقدماً مع المؤسسات الكبيرة التي تواجه عدداً كبيراً من الحوادث وتتطلب نظاماً مرناً يتوافق مع الاحتياجات المحددة للمنظمة.²⁶

أدوات تخزين الحوادث

يجب أن يحتوي النموذج الأساسي لتخزين الحوادث على المعلومات التالية:



- **البلد والمنطقة والموقع** - تحريّ الدقة والتحديد.
- **التاريخ والوقت المحدد في اليوم** - متى وقع الحادث، وكم من الوقت استمر، ومتى انتهى.
- **ما الذي حدث** - ملخص موجز ومختصر للحادث.
- **فئة الحوادث** - فئات تحليلية لتحليل اتجاه البيانات - انظر الأدوات 2 و 10 للخيارات المقترحة.
- **من المشارك في الحادث** - داخلياً وخارجياً - الضحية والدعم الإداري.
- **الإجراءات والقرارات المتخذة** - ملخص الإجراءات / القرارات الرئيسية المتخذة ومن قبل من.
- **التغييرات التشغيلية** - نظرة عامة على التغييرات الفورية التي تمت كرد الفعل على الحادث.
- **التحليل والتعليقات** - ملخص وثيقة التحليل بعد الحادث.
- **الوضع** - هل الحادث الأمني مستمر؟ هل تم توثيق جميع المعلومات؟



يقدم هذا الدليل أمثلة على أدوات تخزين الحوادث في إكسيل. ويمكن العثور على هذه الوثائق في إطار الأداة 2: تصنيف الحوادث والأداة 10: حفظ الحوادث.

ينبغي تحديد احتياجات التحليل والإحصاءات في المستقبل قبل تصميم أداة تخزين وحفظ الحوادث؛ يجب إنشاء أعمدة لتمكين تحليل الاتجاهات وتطوير الإحصاءات باستخدام إعدادات إكسيل.

أنظمة الإنترنت

- الوظائف الرئيسية التي قد تبحث عنها المنظمة في النظام الذي يعمل عبر شبكة الإنترنت:
- أن يكون بمثابة مستودع واحد للحوادث على شبكة الإنترنت.
- توفير التقارير الإلكترونية من أجهزة الحاسوب الأجهزة المحمولة المتصلة بالإنترنت.
- إخطار مجموعات مختلفة على أساس التفاصيل في تقرير الحادث المقدم.
- ضمان أمن البيانات - المعلومات المقدمة لا يمكن الوصول إليها إلا على أساس المراقبة، الحاجة إلى المعرفة.
- ضمان حماية البيانات أثناء تنقلها.
- ضمان وجود نسخ احتياطية للبيانات.

²⁶ سلامتها وأمنها الخاص وإدارتهما بالشكل المناسب. وينطبق الأمر نفسه أيضاً على إدارة معلومات الحوادث. دي بالاسيوس، جي (2017، مقل). إدارة المعلومات المتعلقة بالأمن: نظرة فاحصة على نظم الإبلاغ عن

الأمر الرئيسية التي يجب اتخاذ قرارات بشأنها:

- كيف سيقوم المستخدمون النهائيون بالإدخال في المستودع،
 - كيفية ضمان الوصول إلى المستودع على أساس الحاجة إلى المعرفة،
 - كيفية إبلاغ مجموعات مختلفة من الناس على أساس التفاصيل في تقديم الحادث،
 - كيفية ضمان تغطية المعلومات بشكل كامل ودقيق من مصدر الحادث،
 - كيفية التحقق من صحة المعلومات التي تم الحصول عليها إلكترونياً،
 - إلى أي مدى سيتم استخدام النظام في متابعة الحالة (هل سيكون مجرد مستودع أم أن هناك أيضاً مراحل متابعة؟)؛
 - ما هي أنواع وظائف التحليل التي يمكن إضافتها.
- الأمر الرئيسية التي يجب أن تكون موجودة قبل الشروع في تطوير نظام يعمل على شبكة الإنترنت:
- تعريف فئات الحوادث.
 - تعليمات واضحة للمستخدمين حول الفئات

من المهم من الناحية الفنية وبغض النظر عن الأدوات والأنظمة أن نحدد من يستطيع الوصول إلى البيانات المخزنة على المستوى الميداني والوطني والإقليمي والمقر الرئيسي. وتعتبر كلمات السر، والتشفيرات، ومجموعة المغلفة، وعمليات التحقق باستخدام الأقران للوصول أمثلة عن الطرق التي يمكن استخدامها لضمان تبادل المعلومات مع أصحاب المصلحة المناسبين. انظر "مقدمة - أمن المعلومات" لمزيد من التفاصيل حول أمن المعلومات.

انظر الأداة 11: التقنية المستخدمة في الإبلاغ عن الحوادث وتسجيلها للاطلاع على أمثلة وأوصاف الأنظمة الإلكترونية لتسجيل الحوادث والإبلاغ عنها.

4.2 تحليل الاتجاهات للاسترشاد بها في اتخاذ القرارات الاستراتيجية

وبمجرد توحيد معلومات الحادث في نظام مركزي واحد يشمل فئات تحليلية من الممكن إجراء تحليل أكثر استراتيجية للمعلومات الأمنية لتوجيه اتخاذ القرارات.

وينبغي لمديري الأمن، والمنسقين والمحللين تحويل البيانات إلى معلومات مفيدة. وسيتم مشاركة هذه المعلومات مع كبار الموظفين المعنيين في شكل اتجاهات وإحصاءات لدعم عمليات صنع القرار.

تصنّف معظم المنظمات حوادث الأمن والسلامة، حيث أن التصنيف يساعد على تحليل واستخراج الإحصاءات.

يمكن تقسيم البيانات حسب الفئات الرئيسية (الأداة 2: تصنيف الحوادث) وعرضها في شكل تقارير عامة عن تحليل الاتجاهات (الأداة 12: تحليل اتجاهات البيانات)

تعتمد طبيعة هذا التحليل على المستوى الاستراتيجي على عدد الحوادث الأمنية المُبلغ عنها داخل المنظمة. إذا كان عددها قليلاً، فقد تكون مذكرة مكتوبة تلخص الأحداث الرئيسية أفضل طريقة لتقديم الاتجاهات. أما إذا زاد عدد الحوادث المُبلغ عنها، فسيكون من المهم وضع نظام رصد ومراقبة أكثر انتظاماً يستند إلى الأرقام.

يمكن لقائمة الأسئلة التالية أن تساعد منسقي شؤون الأمن عند وضع استنتاجات وتوصيات إضافية على المستوى الاستراتيجي من أجل اتخاذ إجراءات في أعقاب التحليل الجيد للأحداث الأمنية الماضية.

- ما هي البلدان التي وقعت فيها؟
- بصفتك منسق شؤون الأمن في المقر الرئيسي، ما مدى رضاك عن كيفية استخدام المكاتب القطرية لمعلومات الحوادث الأمنية، بما في ذلك الحوادث الوشيكة، لأغراض التعلم وتحسين الممارسات؟
- ما هي الحوادث الأمنية التي تواجهها المنظمات الأخرى في نفس البلد وكيف يقارن ذلك بالحوادث المبلغ عنها داخل مؤسستك؟
- كيف أثرت الحوادث الأمنية على تقديم المساعدات؟
- هل يمكننا أن نعرف تكاليف أثر الحوادث الأمنية على إيصال المعونة؟
- ما هي الأسباب الرئيسية للحوادث الأمنية؟
- هل يمكن تصنيف أسباب الحوادث من حيث استراتيجية الاستجابة التي قد تكون ضرورية؟
- هل يمكننا استخدام البيانات لتحديد عتبة المخاطر التي ستكون منظمنا مستعدة لقبولها؟



انظر الأداة 13: الأسئلة الاستراتيجية المتعلقة باتخاذ قرارات إدارة معلومات الحوادث للحصول على قائمة كاملة بالأسئلة والإجراءات الموصى بها.

أداة تصوّر Google Earth Pro

يمكن أن يكون رسم الخرائط الجغرافية للأحداث أداة مفيدة لتصور الحوادث ودعم التحليل ورفع التقارير إلى الإدارة العليا داخل المنظمة. توجد خيارات متعددة لعرض المعلومات بصرياً. وإذا كان هذا هو الخيار المفضل، فإنه يجب تضمين التفاصيل الضرورية لتحديد الموقع الجغرافي ونوع الحادث كجزء من التقرير الأولي، حيث أن القيام بذلك بأثر رجعي ليس فعالاً أو دقيقاً.

إذا كانت المعلومات المناسبة متوفرة (مثل إحداثيات نظام تحديد المواقع العالمي، ورموز الألوان وأنواع الحوادث وما إلى ذلك)، فقد يكون الخيار البسيط لعرض موقع الحوادث هو تحويل وثيقة إكسيل إلى وثيقة KML ثم ربطه ببرنامج Google Earth Pro. إذا كانت وثيقة Excel-KML تحتوي على المعلومات المناسبة، فستتم الإشارة إلى الأحداث تلقائياً على خريطة غوغل.²⁷



تأكد من أن إعداداتك تضمن السرية عن طريق تقليل الوصول إلى المعلومات.

4.3 الهياكل التنظيمية لمناقشة قضايا الأمن الاستراتيجي

يمكن للمنظمات مناقشة قضايا الأمن من منظور استراتيجي في إعدادات متعددة.

فعلى سبيل المثال، قد ترتب لجنة إدارة المخاطر الأمنية اجتماعات منتظمة (على سبيل المثال مرة واحدة في السنة أو أكثر) تجمع فيها أعضاء مجلس الإدارة المعينين، والرئيس التنفيذي، ومنسق شؤون الأمن أو فريق الأمن، وربما المديرين الإقليميين. وكثيراً ما يتم تكليف أفراد الأمن بإعداد هذا الاجتماع، وتقديم الاتجاهات الأمنية ووضع جدول الأعمال للمناقشة.

²⁷ الحوادث". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

للحصول على توجيهات مفصلة حول عملية تحويل وثيقة إكسيل إلى KML، راجع الرابط التالي:

<https://www.earthpoint.us/ExcelTokml.aspx>

- في هذا النوع من الاجتماعات، قد يكون من المفيد تغطية ما يلي:
- اتجاهات الحوادث الأمنية على مدى السنوات الماضية، معروضة على النحو التالي:
 - جدول الحوادث الأمنية لكل بلد،
 - جدول الحوادث الأمنية لكل فئة،
 - جدول حول خطورة الحوادث (أي الأثر)،
 - جدول حول أسباب الحوادث،
 - تحليل عواقب الحوادث الأمنية المبلغ عنها، على سبيل المثال:
 - العواقب البشرية ذات التأثير النفسي و / أو البدني،
 - العواقب التشغيلية،
 - العواقب التنظيمية مثل تلك التي تؤثر على سمعة المنظمات غير الحكومية،
 - العواقب المترتبة على إدارة مخاطر الأمن.
 - توصيات حول كيفية ضمان استمرار العمل في هذه البيئات.
 - تقييمات السياق ومستويات الأمن التشغيلي.
 - معوقات الإبلاغ عن الحوادث في المنظمة.
 - دراسة حالة تبين موضوعاً هاماً ينبغي مناقشته مع الجميع، ويؤدي إلى وضع خطة عمل لحالات مماثلة في المستقبل (مثل خطة الاتصالات في حالة وقوع حوادث، أو الحاجة إلى إقامة علاقات مع السلطات المحلية، وما إلى ذلك).
 - مساحة لمعالجة أسئلة صانعي القرار التي تُقدّم إلى أفراد الأمن.



لمزيد من الأمثلة حول كيفية إعداد تحليل الأمن لاجتماعات المراجعة انظر [الأداة 12: تحليل اتجاهات البيانات](#).



ينبغي إدراج مراجعة الوثائق الأمنية، مثل عتبة المخاطر الأمنية التنظيمية، وإطار إدارة المخاطر الأمنية، واستراتيجية الأمن، وسياسة الأمن، وخطة إدارة الأزمات، وما إلى ذلك، كبنود من بنود جدول الأعمال لكل اجتماع حتى إذا كانت خطوة العمل هي "عدم الحاجة إلى اتخاذ أي إجراء". وهذا أمر مهم لتوثيق الإجراءات لأغراض واجب الرعاية.

4.4 كيفية استخدام معلومات حوادث العنف الجنسي على المستوى الاستراتيجي

إن أفضل طريقة يمكن للمنظمات اتباعها للتعامل مع حوادث العنف الجنسي ضد موظفيها هي التعلم من التجربة لضمان قيام المنظمة بتوفير أفضل حماية لموظفيها والاستجابة لهذه الأنواع من الحوادث في المستقبل. ولا يزال هذا الموضوع مادةً يصعب على الناس مناقشتها، لذا ينبغي للمنظمة أن تسعى بنشاط إلى خلق وترسيخ الثقة والانفتاح لمناقشة هذه الحوادث داخلياً.

وينبغي إجراء تحليل لمعرفة ما إذا كان الانفتاح والتطرق إلى حوادث العنف الجنسي مع وسائل الإعلام أو في المحافل العالمية مع الأعضاء الآخرين في مجتمع المنظمات غير الحكومية أمراً مفيداً واستراتيجياً.

“

إن الانفتاح على منصة أكبر يمكن أن يتيح أيضاً المجال للمنظمات غير الحكومية الأخرى لإجراء تغيير مماثل داخل المنظمات الخاصة بها، والمساهمة في زيادة شاملة في سلامة وأمن موظفي المنظمات غير الحكومية.”

إذا كان من الضروري استخدام تفاصيل حادث معين لتسليط الضوء على المشكلة والدروس المستفادة على الصعيد العالمي، فإنه يجب الحصول على موافقة الناجي المستنيرة. وحيثما كان ذلك ممكناً، ينبغي إشراك الناجي في هذه العملية وتوفير صوت توجيهي لإنشاء سرد حول الحادث والدروس المستفادة.

وحيثما يكون الناجي قد أعطى موافقة مستنيرة لمشاركة معلومات عن تجربته - على المستوى الميداني أو العالمي - فينبغي ضمان حصوله على دعم إضافي في الوقت الذي يتم فيه نشر المعلومات، بما في ذلك الإجازة لأغراض إنسانية والدعم النفسي والاجتماعي، وما إلى ذلك.

وتجدر الإشارة أنه يمكن تبادل معلومات الاتجاه والدروس المستفادة التنظيمية دون المساس بحقوق الفرد وهذا أمرٌ ينبغي تشجيعه وتعزيزه.

4.5 استخدام معلومات الحوادث الأمنية للدعوة الاستراتيجية

يجب على المنظمة أن تقرر بشكل استراتيجي، ما إذا كان سيتم استخدام معلومات الحوادث التي تم الحصول عليها داخلياً وربما أيضاً خارجياً، لأغراض الدعوة.

تفيد منظمات عديدة بوجود صعوبة متزايدة في تأمين المرور الآمن وتقديم المساعدات للمدنيين المحتاجين. ومع ذلك، فبدون وجود بيانات موحدة على نطاق القطاع عن هذه الحوادث، وفي غياب استراتيجية جماعية فعّالة بشأن كيفية التصدي للعوائق المتعمدة أو إفلات مرتكبيها من العقاب، لا يمكن لمعظم الوكالات إلا أن تشير إلى حالات منفردة ومنفصلة.

أحرزت المنظمات غير الحكومية تقدماً كبيراً في وضع استراتيجيات لإدارة المخاطر الأمنية للاستجابة للسياقات الأمنية المتغيرة باستمرار. غير أن هذا الأمر لم يقابله تأييد إنساني مشترك لمعالجة الشواغل التي تتجاوز استراتيجية إدارة المخاطر الأمنية التي تتبعها كل منظمة على حدة. وبالتالي، يظل حجم انعدام الأمن في مجال العمل الإنساني غير ظاهر، حيث يتم التعامل مع كل حالة بصمت، وفي معظم الحالات، نادراً ما يتم تقديم الجناة إلى العدالة. وهناك فرص لوضع استراتيجية للدعوة على نطاق القطاع لمعالجة الشواغل المعقدة.

فبعض الحوادث الأمنية تتجاوز ما تستطيع المنظمة السيطرة عليه وقد تتطلب حملة مشتركة للدعوة مع منظمات أخرى. فعلى سبيل المثال، يؤثر الاستخدام المتزايد للأسلحة المتفجرة في المناطق المأهولة بالسكان على أمن الموظفين ويعيق إيصال المعونة. وعندما لا تتخذ السلطات الوطنية التدابير اللازمة ضد مرتكبي هذه الجرائم، قد تحتاج المنظمات إلى طلب الدعم الدولي لإجراء تحقيقات أو للضغط من أجل الملاحقات القضائية.

وعلى الصعيد العالمي، من المهم أن يضمن قطاع المعونة إبلاغ أصحاب المصلحة الرئيسيين مثل المانحين وواضعي لسياسات ووسائل الإعلام والجمهور واطلاعهم بانتظام على المعلومات المتعلقة بالتحديات الناشئة عن السياقات الأمنية المتقلبة. وهناك حاجة إلى أدلة موثقة عن العنف ضد العاملين في مجال تقديم المعونة أو الحوادث التي تؤثر على إيصال المعونة لدعم الجهود الأوسع نطاقاً والرامية إلى تحسين حماية العاملين في مجال المعونة وعملياتهم، ولدعم

وصول السكان المحتاجين للإعانات دون أي معوقات. وبصورة أكثر شمولية، يمكن للقطاع الإنساني والإنمائي أن يفعل المزيد لتذكير الجهات المانحة وصانعي السياسات بالصعوبات التي تواجه العاملين في مجال الإغاثة عند تقديم المعونة في بيئات غير آمنة.

ومع ذلك، عندما تفكر المنظمات فيما إذا كانت ستنفذ حملات للدعوة والتأييد، يجب عليها أن تنظر في العواقب المحتملة على سلامة الموظفين وأمنهم، فضلاً عن النتائج المترتبة على تنفيذ البرنامج.

ما نوع البيانات المطلوبة للدعوة؟

هناك اتجاه سائد في وسائل الإعلام وغيرها من أصحاب المصلحة إلى طلب الأرقام التي توضح حجم المشكلة. ونتيجة لذلك، يتم بذل جهد كبير في محاولة تحديد عدد الأشخاص المتضررين. غير أن هذا ليس مطلوباً بالضرورة لمناقشة السياسات. فقد أظهرت الحملات السابقة أن وصف طبيعة المشكلة وجوهرها يمكن أن يكون قوياً بما يكفي لتشجيع التغيير. فقد بدأت حملة «الألغام البرية المضادة للأفراد»، على سبيل المثال، بالتركيز على عرض السياقات الفردية بتفاصيل من برامج اللجنة الدولية للصليب الأحمر في كمبوديا وأنغولا التي وضحت المشكلة بدلاً من تناولها من الناحية الكمية. أثر هذا الوصف الدقيق لتأثير الألغام البرية في الكثيرين، مما أدى إلى تحقيق الحملة نتائج باهرة.²⁸

يمكن استخدام الحوادث التي تؤثر على أمن المنظمات غير الحكومية لوصف طبيعة وأثر المشكلة حتى عندما لا يُعرف مدى تكرارها. ولدى مجتمع المساعدات فرص كبيرة للوصول إلى جمهور أوسع وصانعي السياسات الرئيسيين لاطلاعهم عن مدى صعوبة السياقات التي يعملون فيها ومدى تأثير الموظفين وعملهم فيها عن كيفية تأثر عملهم وموظفيهم.

تعتبر التقارير التي تصدرها المنظمات عن إدارة المخاطر الأمنية الخاصة بها من أكثر المصادر إقناعاً والتي تدل على تأثير انعدام الأمن في إيصال المعونة. حيث أن وجود البيانات في هذه التقارير من شأنه أن يوضح المشكلة بشكل أفضل من أي بيانات أخرى يتم جمعها خصيصاً لأغراض الدعوة. وقد يكون عدم الاستفادة من هذا المورد من أجل توفير حماية أفضل للموظفين، أو على الأقل توفير تمويل أفضل للسياسات المتعلقة بالأمن وتحسين التدريب الأمني للموظفين إضاعة لفرصة لا تعوّض.

يمكن أن يساهم توليد هذه البيانات مجتمعة في تعزيز الدعوة لحماية العاملين في مجال المعونة وبرامجها، وزيادة قبول المانحين لإدارة المخاطر الأمنية بصفتها تكلفة مباشرة ينبغي إدراجها في العروض.



ومن المهم عدم الكشف عن أسماء أشخاص محددين أو حالات معينة لأغراض إثبات وجهة نظر سياسية. واستخدام البيانات الجماعية يقلل من هذه المخاطر.

يمكن للإدارة العليا داخل المنظمات أن تدفع بهذا البرنامج من خلال الإسهام في تبادل البيانات مع المنظمات الأخرى وتعزيز الروابط بين موظفي الأمن وموظفي السياسات والدعوة داخل منظماتهم الخاصة. ويساعد هذا على ضمان استخدام الرؤى المستخلصة من تحليلات الحوادث الأمنية لمختلف المنظمات من قبل موظفي السياسات والدعوة استخداماً استراتيجياً.

دراسة حالة: Health Care in Danger ، اللجنة الدولية للصليب الأحمر

في عام 2008، كلّفت اللجنة الدولية للصليب الأحمر بإجراء دراسة في 16 بلدا لتوثيق كيفية تأثير العنف على تقديم الرعاية الصحية، باستخدام بيانات الحوادث من سياقات مختارة.²⁹ وأصبحت هذه الدراسة أول قاعدة أدلة للبدء في التصدي للعنف ضد العاملين في مجال الرعاية الصحية، والذي قد تم توضيحه من ذلك الحين من خلال العديد من دراسات الحالة الإضافية.³⁰ ومنذ ذلك الحين، تدير اللجنة الدولية للصليب الأحمر مشروع Health Care in Danger ، الذي يجمع بين التوعية والتوجيه العملي بشأن كيفية تحسين أمن العاملين في مجال الرعاية الصحية.³¹

وقد بدأت منظمات أخرى أيضاً في تناول هذه المسألة. ومنذ عام 2014، نشر عشرة من أعضاء التحالف المعني بالصحة في حالات النزاع (Safeguarding Health in Conflict Coalition) تقارير سنوية مشتركة عن الهجمات على الرعاية الصحية، وتجمع هذه التقارير بين البيانات والمعلومات من مختلف المنظمات لإبقاء هذه المسألة على جدول الأعمال العالمي.³² ويساعد أكثر من 20 عضواً في التحالف، بما في ذلك عدّة منظمات إنسانية، في نشر المعلومات لتشجيع توفير حماية أفضل للرعاية الصحية.³³

وفي عام 2016، نشرت منظمة الصحة العالمية (WHO) بيانات تتعلق بالهجمات على الرعاية الصحية على موقعها على شبكة الإنترنت.³⁴

وفي مايو / أيار 2016، اعتمد مجلس الأمن الدولي القرار رقم 2286 الذي وضع خارطة طريق لحماية الرعاية الصحية في حالات النزاع.³⁵

وتسلط هذه الأمثلة الضوء على أهمية الاستخدام الفعال للبيانات في وضع هذه المسألة الهامة في جدول الأعمال والاحتفاظ بها.

الفريق العامل المعني بحماية العمل الإنساني

ينظر الفريق العامل المعني بحماية العمل الإنساني في الخيارات المتاحة للعمل الجماعي من أجل حماية العاملين في مجال المعونة.³⁶ ويجمع الفريق العامل بين الممارسين من المنظمات الإنسانية العاملة وخبراء الأمن وخبراء الدعوة والأكاديميين ويشترك في رئاسته برنامج التدريب المتقدم للعمل الإنساني (Advanced Training Programme on Humanitarian Action) التابع لمبادرة هارفارد الإنسانية (Harvard Humanitarian Initiative) وبرنامج العمل لمكافحة الجوع (Action Against Hunger). والهدف من ذلك هو التغلب على ميل المنظمات الإنسانية للعمل في

²⁹ اللجنة الدولية للصليب الأحمر. (2011). دراسة حالة في 16 دولة: مشروع health care in danger .

اللجنة الدولية للصليب الأحمر

³⁰ للمزيد من المعلومات، انظر: <http://healthcareindanger.org/resource-centre/>

³¹ للمزيد من المعلومات، انظر: <http://healthcareindanger.org/hcid-project/>

³² للمزيد من المعلومات، انظر: <https://www.safeguardinghealth.org/>

³³ للاطلاع على قائمة المنظمات الإنسانية التي تدعم تحالف Safeguarding Health in Conflict Coalition،

³⁴ انظر الصفحة 2 هنا

انظر: <http://www.who.int/emergencies/attacks-on-health-care/en/>. نحيطك علماً بأنه سيتم تحديث هذا الموقع

قريباً. انظر أيضاً: ليبرمان، آي (2017). "منظمة الصحة العالمية تستعد لإطلاق قاعدة بيانات عبر شبكة الإنترنت لمتابعة

الهجمات ضد العاملين في الصحة". Devex

³⁵ الأمم المتحدة (2016). "مجلس الأمن الدولي يعتمد القرار 2286 (2016)، الذي يدين بشدة الهجمات على

المرافق الطبية، والموظفين في حالات النزاع". الأمم المتحدة

³⁶ AHTA (2016). "مشروع السياسة: حماية العمل الإنساني". AHTA

عزلة للاستجابة لهذه البيئة الصعبة على نحو متزايد من خلال التفكير الجماعي، وجهود الدعوة الأكثر قوة وأكثر اتساقاً في جميع أنحاء القطاع الإنساني، والإجراءات المشتركة لإعادة تأكيد احترام القانون الدولي الإنساني وحماية العمل الإنساني. ولكون القانون الدولي الإنساني مسؤولية الدول، فإنه لا يمكن الدفع بعجلة تغيير السياق إلاّ على الصعيد العالمي. خاصة وأن هذا السياق أصبح الآن أقل موثاقه للمساعدات الإنسانية من حيث الوصول إلى المدنيين المحتاجين.



من بين النتائج الأولية التي توصل إليها الفريق العامل ضرورة تحسين تبادل الحوادث الأمنية بصورة منتظمة من أجل المساعدة على تحديد الاتجاهات والأولويات الرئيسية. كما أشار الفريق العامل إلى أن قلّة التعاون والاتصال المباشر بين مديري المخاطر الأمنية وأقسام الدعوة في العديد من المنظمات من العقبات التي تعيق العمل بفعالية أكبر. ويسعى الفريق إلى العمل مع جهات التنسيق الأمنية وموظفي السياسات داخل المنظمات لتحديد الحالات التي يمكن فيها للدعوة المشتركة أن تدعم الاستجابة للشواغل الأمنية.

لمزيد من المعلومات حول مجموعة العمل يرجى التواصل مع:

Lise Fouquat: lfouquat@actioncontrelafaim.org

Pauline Chetcuti: pchetcuti@actioncontrelafaim.org

Julia Brooks: jbrooks@hsph.harvard.edu

Pauline Chetcuti: pchetcuti@actioncontrelafaim.org

Julia Brooks: jbrooks@hsph.harvard.edu

الفصل الثالث: الأدوات



يحتوي هذا القسم على أدوات إرشادية تدعم إدارة معلومات الحوادث الأمنية ويجب قراءتها واستخدامها جنباً إلى جنب مع المحتوى المكتوب في هذا الكتيب.

يتم تنظيم الأدوات على النحو التالي: (انقر على للوصول إلى الأداة)

- الأداة 1: شبكة التقييم الذي لإدارت احوالا تامومعه ةلأئيمه
- الأداة 2: تصنيف الحوادث
- الأداة 3: الحوادث التنظيمية أو الخارجية
- الأداة 4: نموذج الإبلاغ عن الحادث
- الأداة 5: شبكات تحليل الحوادث
- الأداة 6: كيفية إجراء الاستجواب الواقعي
- الأداة 7: الممارسة الجيدة في طريقة الإبلاغ عن حوادث مراعاة الفوارق بين الجنسين وآلية تقديم الشكاوى للإبلاغ عن الاستغلال والاعتداء الجنسين
- الأداة 8: خطة العمل
- الأداة 9: أنظمة إدارة معلومات الحوادث الأمنية
- الأداة 10: حفظ الحادث
- الأداة 11: التقنية المستخدمة في الإبلاغ عن الحوادث وتسجيلها
- الأداة 12: تحليل اتجاهات البيانات
- الأداة 13: أسئلة على المستوى الاستراتيجي لإدارة الحوادث

الأداة 1: شبكة التقييم الذاتي لإدارة معلومات الحوادث الأمنية



يرجى استخدام هذا الجدول كدليل للعناصر النموذجية لنظام إدارة معلومات الحوادث

أسئلة عامة	
كم عدد المكاتب الميدانية / القطرية / الإقليمية التي تعمل حالياً في منطقتك؟	
عدد الموظفين (الموظفين الدوليين، الموظفين المحليين، المتطوعين، الخ	
ما هو عدد منسقي شؤون الأمن الذين يعملون معك حالياً؟	
على مستوى المقر الرئيسي هل تشارك أحدهم مسؤولية تنفيذ إطار إدارة المخاطر الأمنية؟ إذا كانت الإجابة نعم، مع من؟ (الوظيفة)	
إطار إدارة المخاطر الأمنية	
هذا موجود لمنظمتي (نعم / لا / جزئياً)	
هل تم تحديد مسؤوليات اتخاذ قرارات إطار إدارة المخاطر الأمنية على جميع المستويات بوضوح؟	
هل تستخدم منظمتك معلومات عن السياق الأمني لأغراض السياسة العامة مثل التأييد والتواصل مع الجهات المانحة و/أو البرمجة؟	
إدارة الحوادث والأزمات	
هل لدى المنظمة سياسة لإدارة الحوادث والأزمات؟	
هل يتوفر إطار لإدارة الحوادث على المستوى الميداني / القطري (الإجراءات)؟	
هل يتوفر إطار لإدارة الحوادث في المقر الرئيسي (الإجراءات)؟	
هل يحتوي إطار إدارة الحوادث على شجرة الاتصالات؟	
هل يعالج إطار إدارة الحوادث "الحوادث الوشيكة"؟	
هل تدرب الموظفون على إدارة الحوادث و / أو الأزمات وهل تقومون بتمارين المحاكاة؟	
هل تستخدم المنظمة نظام إدارة الحوادث عبر شبكة الإنترنت؟	

هل تستخدم المنظمة معالج النصوص أو جداول البيانات كأساس في نظام إدارة الحوادث؟	
هل تم الاتفاق بشأن الاتصالات المتعلقة بالحوادث مع شركة التأمين الخاصة بالمنظمة؟	
هل يوجد رابط بين سياسة إدارة المخاطر الأمنية وسياسة الموارد البشرية في منظمته؟	
جمع معلومات الحادث	
هل لديك تعريف تنظيمي لمصطلح "الحادث"؟	
هل تستخدم منظمته فئات محددة لوصف مختلف أنواع الحوادث؟ إذا كان الأمر كذلك؛ هل يتم توحيدها مع الفئات المستخدمة من قبل المنظمات غير الحكومية الشريكة التي تعمل معها؟	
هل يوجد نموذج للإبلاغ عن الحوادث على مستوى الميداني/القطري؟ إذا كان الأمر كذلك؛ هل يتم توحيدها مع الفئات المستخدمة من قبل المنظمات غير الحكومية الشريكة التي تعمل معها؟	
هل يوجد إجراء لاستخلاص المعلومات العاطفية (تهدئة) على المستوى الميداني؟	
هل يوجد إجراء لاستخلاص المعلومات الواقعية على المستوى الميداني؟	
هل يوجد نظام تخزين آمن للمعلومات التي تم جمعها على المستوى الميداني؟	
هل يوجد نظام تخزين آمن للمعلومات التي تم جمعها على المستوى القطري/الإقليمي؟	
هل يوجد نظام تخزين آمن للمعلومات التي تم جمعها على مستوى المقر الرئيسي؟	
هل تقوم منظمته بجمع المعلومات حول الأحداث الخارجية (أي تلك التي لا تؤثر على منظمته)؟	
الإبلاغ عن معلومات الحوادث وتسجيلها	
هل يوجد إجراءات للإبلاغ عن الحوادث؟	
هل يوجد مبادئ توجيهية تدعم نموذج تقرير الحوادث؟	
هل يوجد شجرة تقارير واضحة لكل مكتب من المكاتب الميدانية؟	
هل يوجد قائمة بجهات الاتصال على المستوى الميداني /القطري؟	
هل يوجد نظام تسجيل على المستوى الميداني / القطري؟	
هل يوجد نظام تسجيل على المستوى الإقليمي؟	
هل يوجد نظام تسجيل على مستوى المقر الرئيسي؟	
هل تقوم بتسجيل الخسائر والأضرار التي تصيب البنية التحتية أو المعدات؟	
هل تقوم بتسجيل التهديدات الشفوية / الكتابية والتهديدات الإلكترونية في منظمته؟	

	هل تقوم بتسجيل العقوبات الإدارية؟
	هل تقوم بتسجيل العنف الجنسي (بما في ذلك التحرش)؟
	هل يتم الإبلاغ عن الحوادث المرتبطة بالعنف الجنسي باستخدام الإطار العادي لإدارة الحوادث؟
	هل تقوم بتسجيل الحوادث الوشيكة؟
	هل النظام آمن على جميع المستويات؟ هل البيانات آمنة؟
تحليل معلومات الحوادث	
	هل يوجد نموذج آخر للإبلاغ عن الحوادث يهدف إلى تقديم التوجيه بشأن المعلومات التي يتم جمعها لأغراض التحليل (على سبيل المثال، 72 ساعة بعد الحدث)؟
	هل يوجد شخص مسؤول عن تحليل الحادث على المستوى الميداني/القطري؟
	هل يوجد شخص مسؤول عن تحليل الحادث على المستوى الإقليمي؟
	هل يقوم شخص على مستوى المقر الرئيسي بتوفير التحليل والتحقق من نتائج التحليل الإقليمي/الميداني / القطري؟
	هل يمكنك القيام بتدريب الموظفين لتحسين مهاراتهم التحليلية؟ (ليس بالضرورة فيما يخص المسائل المتصلة بالأمن فقط)
	هل يوجد نظام على المستوى القطري لمطابقة المعلومات (مثلاً عن طريق جدول البيانات) وتحليل الحوادث؟
	هل تتم استشارة بعض الموارد الخارجية (أصحاب المصلحة أو المعلومات) أثناء التحليل على المستوى الميداني / القطري؟
	هل تتم استشارة بعض الموارد الخارجية (أصحاب المصلحة أو المعلومات) أثناء التحليل على المستوى الإقليمي؟
	هل تتم استشارة بعض الموارد الخارجية (أصحاب المصلحة أو المعلومات) أثناء التحليل على مستوى المقر الرئيسي؟
تبادل معلومات الحوادث	
	هل يوجد توجيهات أو سياسة عامة لتصنيف المعلومات في المنظمة؟
	هل توجد سياسة اتصالات داخلية على المستوى الميداني / القطري؟
	هل توجد سياسة اتصالات داخلية على المستوى الإقليمي؟
	هل توجد سياسة اتصالات داخلية على مستوى المقر الرئيسي؟
	هل المنظمة جزء من مجموعة أمن للمنظمات غير الحكومية على المستوى الميداني / القطري؟ (أمثلة)
	هل المنظمة جزء من مجموعة أمن للمنظمات غير الحكومية على المستوى الإقليمي؟ (أمثلة)
	هل المنظمة جزء من مجموعة أمن للمنظمات غير الحكومية على مستوى المقر الرئيسي؟ (أمثلة)

هل توجد سياسة اتصالات خارجية على المستوى الميداني / القطري؟	
هل توجد سياسة اتصالات خارجية على المستوى الإقليمي؟	
هل توجد سياسة اتصالات خارجية على مستوى المقر الرئيسي؟	
هل تستخدم المنظمة وسائل التواصل الاجتماعي للتواصل العام؟	
هل لدى المنظمة صلات مع أصحاب المصلحة والجهات المعنية في وسائل الاعلام؟	
هل لدى المنظمة نظام مطابقة الأطراف الفاعلة على المستوى الميداني / القطري؟	
هل لدى المنظمة نظام مطابقة الأطراف الفاعلة على المستوى الإقليمي؟	
هل لدى المنظمة نظام مطابقة الأطراف الفاعلة على مستوى المقر الرئيسي؟	
هل يتم ممارسة الاتصال الداخلي شفهيًا / كتابيًا؟	
هل يتم ممارسة الاتصال الخارجي شفهيًا / كتابيًا؟	
هل يتم على المستوى الميداني تسليم وثيقة لمنسق شؤون الأمن بما في ذلك معلومات الحادث؟	
هل يتم تدريب الموظفون على تبادل المعلومات بشأن الحوادث والسياسات التنظيمية؟	
هل يستفيد المدبرون التنفيذيون وأعضاء مجلس الإدارة من مشاركة المعلومات؟	
استخدام معلومات الحادث	
هل يوجد شخص معيّن مسؤول عن متابعة الإجراءات على المستوى الميداني / القطري (في منتصف المدة)؟	
هل يتم إجراء اتصالات متابعة بعد شهر واحد من الحادث (يمكن أن تختلف المستويات)؟	
هل يتم إجراء اتصالات متابعة بعد ٣ أشهر من الحادث (يمكن أن تختلف المستويات)؟	
هل يوجد متابعة لتطبيق الدروس المستفادة من قبل المقر الرئيسي؟	
هل تقوم منظمتك بالتحليل الكمي؟	
هل تقوم منظمتك بالتحليل النوعي؟	
هل يوجد نظام على المستوى القطري يقوم بتحليل البيانات الكمية حول الحوادث؟	
هل يوجد نظام على مستوى المقر الرئيسي يقوم بتحليل البيانات الكمية حول الحوادث؟	
هل يوجد اجتماعات على المستوى الميداني لتقديم توجيهات البيانات للموظفين؟	

	هل يوجد اجتماعات على المستوى القطري لتقديم توجهات البيانات للموظفين؟
	هل يوجد اجتماعات على مستوى المقر الرئيسي لتقديم توجهات البيانات للموظفين؟
	هل يوجد اجتماعات على المستوى الإقليمي لتقديم توجهات البيانات للموظفين؟
	هل يستشير موظفو البرنامج منسقي شؤون الأمن الميدانيين / القطريين؟
	هل يستشير موظفو البرنامج مستشار / مدير الأمن في المقر الرئيسي؟
	هل يتم عرض التحليل على المدراء التنفيذيين ومجلس الإدارة (على سبيل المثال الاتجاهات)؟
	هل تتم مشاركة معلومات اتجاهات البيانات مع أصحاب المصلحة الخارجيين؟
	هل تستخدم منظمتك اتجاهات البيانات في التأييد؟

الأداة 2: تصنيف الحوادث



يتم تقديم التعاريف التالية لمختلف أنواع الحوادث بشكل دلالي، ولا تحتاج المنظمات إلى استخدام جميع الفئات في إدارة معلومات الحوادث الأمنية. ومع ذلك، يتم تشجيعها على استخدام التعاريف الموحدة المقترحة لتيسير تبادل البيانات والمقارنات المشتركة بين الوكالات.

يتم تعريف الحوادث في فئات شاملة (مثل الحوادث، وسلطة العمل والجريمة وما إلى ذلك) وفئات فرعية مرتبطة بها. وقد تختار الوكالات استخدام الفئات الشاملة فقط أو الفئات الفرعية المحددة أو الفئات الشاملة والفئات الفرعية معاً.

تحقق الفئات الشاملة وظائف مختلفة. يصنف البعض الحدث حسب تأثيره (مثل الوفاة أو الضرر). ويصف البعض طبيعة الحدث (مثل العنف الجنسي)، في حين أن البعض الآخر يدرج بعض المعلومات عن مرتكب الجريمة بالإضافة إلى وصف طبيعة الحدث (مثل الإجراءات المتعلقة بالجريمة أو السلطة). ويصنف الآخرون السياق الذي وقع فيه الحدث (مثل انعدام الأمن العام) في حين يصف آخرون الوسائل (مثل استخدام الأسلحة). ويصنف آخرون استجابة الوكالة.

ويعتمد تحديد التصنيف الأنسب على التركيز التحليلي. حيث يمكن تناول حدث واحد من مجموعة متنوعة من وجهات النظر.

قد تكون أكثر من فئة شاملة ذات صلة معظم الأحداث. ويمكن التعامل مع الفئات الفرعية على أنها حصرية، مما يعني أنه في كثير من الأحيان لا يمكن تطبيق إلا واحدة فقط من الفئات الفرعية. قد يكون لمعظم الأحداث صلة مع أكثر من تصنيف واحد من الفئات الشاملة.

انظر أيضاً تعريف فئات الأحداث المستخدمة في تحليل الاتجاه الذي أجرته Insight Insecurity والبيانات المتعلقة "تبادل البيانات الإنسانية".



الفئة الشاملة	التصنيفات الفرعية	التعريف
حادث مرض كارثة طبيعية	حادث: الموت	أي حالة وفاة غير مقصود والتي لا يمكن أن تُعزى إلى أسباب طبيعية. وقد تتضمن أسباب الوفاة العرضية حوادث المركبات، والمضاعفات الناجمة عن الإصابات، إلخ.
	حادث: آخر	حادث عشوائي يؤدي إلى إلحاق الضرر بالموظفين و / أو الإضرار بممتلكات المنظمة.
	الحوادث: المركبات	تعرض مركبة تابعة للمنظمة إلى حادث، وتشمل المركبات أي شكل من أشكال النقل مثل على سبيل المثال لا الحصر السيارات والشاحنات، والحافلات والدراجات النارية، وما إلى ذلك.
	الحادث: الحرائق الطبيعية	الحرائق التي تلحق الضرر بالممتلكات أو تعرض الموظفين للخطر لأسباب طبيعية أو غير مقصودة. وقد يشمل ذلك حرائق الغابات أو الحرائق العرضية (مثل الحرائق الكهربائية أو تسرب الغاز)، وما إلى ذلك.
	المرض	المقصود هنا أي مرض خطير يصيب الموظف.
	الكوارث الطبيعية	الكوارث الطبيعية الفعلية والمتوقعة التي تحدث، أو التي من المتوقع أن تحدث، في المدينة أو البلد التي يوجد فيها مكتب المنظمة. وقد تشمل الكوارث الطبيعية الزلازل، والبراكين، والأعاصير، والأضرار الناجمة عن العواصف (البرد والفيضانات وغيرها)، والفيضانات، والتسونامي، إلخ.
عمل السلطة	إساءة استعمال السلطة	استخدام صلاحيات تشريعية أو تنفيذية أو غيرها من الصلاحيات المسموح بها من قبل المسؤولين الحكوميين لتحقيق مكاسب خاصة غير مشروعة. يشكل الفعل غير القانوني الذي يقوم به صاحب مكتب إساءة استعمال السلطة إلا إذا كان القانون يرتبط ارتباطاً مباشراً بأدائهم لواجباتهم الرسمية.
	حظر الوصول	أعمال (أ) تمنع المنظمة من الوصول إلى المستفيد أو المستفيدين المحتملين للأنشطة المقررة أو توفير الخدمات المباشرة أو أعمال (ب) تمنع المستفيدين من الوصول إلى الخدمات التي تقدمها المنظمة.
	التهم	قيام سلطات البلد المضيف بالاتهام بالمخالفات.
	تطبيق وإنفاذ القوانين	تطبيق القوانين القائمة أو الجديدة، أو الأوامر التنفيذية، أو القرارات، أو القوانين التي يكون لها عند تطبيقها تأثير فعلي على تقديم المساعدة. وقد يشمل ذلك مصادرة المعدات، ووضع الأشخاص / المنظمات على قوائم المراقبة، وما إلى ذلك.
	الاعتقال: (انظر التهم والاعتقال والسجن)	اعتقال الموظفين. ويجب أن يكون الطرف الذي يقوم بالاعتقال يعمل بصفة حكومية (مثل الشرطة) من أجل التفريق بين هذه الحادثة وبين حادث احتجاز الرهائن. وعادة ما تتم الاعتقالات عقب التهم الرسمية.
	التهم (Charges)	التهم القانونية الرسمية التي تصدرها السلطة الحكومية والتي تؤكد أن موظفاً أو منظمة قد ارتكب جريمة.

الفئة الشاملة	التصنيفات الفرعية	التعريف
عمل السلطة	نقاط تفتيش	نقطة تفتيش غير حدودية أو على الحدود، والتي تتم إقامتها في المناطق الخاضعة لسيطرة المجموعات العسكرية أو شبه العسكرية أو المسلحة لمراقبة حركة الأشخاص والمواد التي تؤثر على إيصال المعونة.
	الحرمان من الحصول على تأشيرة	التأخير أو رفض تقديم ختم رسمي أو تأشيرة أو تصريح من نوع آخر لمنح الإذن بدخول بلد أو إقليم داخل البلد والمطلوب لتقديم المعونة.
	الاحتجاز	إبقاء موظف قيد الاحتجاز قبل اتهامه رسمياً أو دون توجيه أي تهمة رسمية؛ ويشمل الاحتجاز المؤقت لساعات أو أيام.
	الطرد	قانون لإجبار الموظف أو المنظمة على مغادرة البلد أو الإقليم.
	الغرامة	الأموال التي يجب أن تدفعها المنظمة كعقوبة على عدم اتباع الأنظمة أو القانون.
	الإغلاق القسري	أمر بواسطة الحكومة أو غيرها من السلطات لوقف العمليات في البلد أو الإقليم؛ ويشمل الإغلاق الذي يؤثر على برنامج واحد أو برامج متعددة.
	الإجراءات الحكومية	الإجراءات التي تتخذها الحكومة المضيفة أو المانحة والتي لها تأثير مباشر أو غير مباشر على القدرة المالية للوكالة على تقديم المعونة؛ وتشمل تجميد الأموال، وفرض الضرائب، أو إنهاء الدعم.
	الحبس	احتجاز موظف في مكان رسمي معروف أو غير معروف، مثل السجن، وغالباً بعد توجيه اتهامات رسمية.
	سنّ القوانين	يشير إلى سنّ والتصويت على القوانين أو الأوامر التنفيذية أو المراسيم أو الأنظمة التي يكون لها عند تطبيقها تأثير محتمل أو فعلي على تقديم المعونة. ويمكن أن يشمل ذلك على سبيل المثال إجراءات التسجيل المقيدة، أو أنظمة الاستيراد، أو الكشف المنتظم عن المصادر المالية.
	التحقيق	التحقيق أو فحص الوقائع المتعلقة بالادعاءات الموجهة ضد الموظفين أو المنظمة.
الجريمة	تفتيش الملكية	تفتيش الملكيات من قبل السلطات الخارجية.
	الجريمة: السطو المسلح	السرقه تحت تهديد السلاح أو السرقات التي يحمل فيها المجرمون الأسلحة النارية التي قد تؤثر على العاملين أو الممتلكات.
	الجريمة: الحرائق	أي حرائق تدمر الممتلكات أو التي تعرض الموظفين للخطر، وتشمل الحرائق المتعمدة على سبيل المثال لا الحصر: افتعال الحرائق باستخدام الأجهزة الحارقة، أو التخريب المتعمد للأنظمة الكهربائية أو خطوط الغاز / الخزانات، واستخدام أي مواد سريعة الاشتعال لتدمير الممتلكات.

الفئة الشاملة	التصنيفات الفرعية	التعريف
الجريمة الحوادث ذات الدوافع الجنائية التي تؤثر على الوكالة أو على ممتلكات الموظفين.	الجريمة: الابتزاز	التهديد أو الابتزاز أو التلاعب بشخص ما لإرغامه على القيام بشيء ما ويشمل الحصول على شيء ولا سيما المال عن طريق القوة أو التهديد.
	الجريمة: الاقتحام	الدخول بصورة غير قانونية إلى مباني أو مركبات وكالات المعونة بقصد السرقة.
	الجريمة: الاقتحام	اقتحام مقر الموظفين بقصد السرقة. تحدث إذا كان الأفراد نائمين أو غير مدركين للاقتحام.
	الجريمة: سرقة السيارات/الاختطاف	الحادث الذي يتم فيه الاستيلاء على سيارة فيها موظف يعمل في المنظمة أو سيارة مملوكة للمنظمة.
	الجريمة: الهجوم الإلكتروني	الاستغلال المتعمد لأنظمة الحاسوب والمشاريع والشبكات التقنية مما يسفر عن آثار مدمرة تعرض البيانات للخطر وتؤدي إلى الجرائم الإلكترونية.
	الجريمة: الاحتيال	خداع غير مشروع أو جنائي يقصد به تحقيق مكاسب مالية أو شخصية.
	الجريمة: الاقتحام	الدخول غير المشروع أو غير المصرح به إلى مباني وكالة المعونة أو المركبات أو مساكن الموظفين من قبل المجرمين أو المدنيين (ولا يكون هذا الدخول من قبل سلطات الدولة).
	الجريمة: النهب	السرقة خلال الاضطرابات والعنف وأعمال الشغب أو غيرها من الاضطرابات.
	الجريمة: القرصنة	الهجوم والسطو على السفن في البحر أو القوارب في الأنهار.
	الجريمة: السرقة	الأحداث التي (أ) لا يكون فيها الجاني مسلحاً (ب) والتي يكون فيها الموظف حاضراً أثناء الحادثة وعلم تأمر بالسرقة (ج) والتي تؤخذ فيها الممتلكات.
	الجريمة: سرقة الممتلكات	أي الحالة التي تُسرق فيها الممتلكات الشخصية من موظف أو مكان دون أن يكون ضحية الجريمة مدركاً لما حصل وكيف أخذت الممتلكات.
	الجريمة: سرقة ممتلكات المنظمة	أي الحالة التي تُسرق فيها الممتلكات (تكون قيمتها محددة مسبقاً) من المنظمة دون أن يُلاحظ الموظف كيف أخذت الممتلكات.
	الجريمة: التخريب	التدمير المتعمد أو إلحاق الأضرار بممتلكات الوكالة أو الموظفين.
الضرر أي ضرر يلحق بممتلكات الوكالة.	الأضرار التي لحقت بالممتلكات	أي ضرر أو أذى يزيد عما هو محدد سابقاً ويصيب ممتلكات المنظمة سواء عن غير قصد (كالحوادث الطبيعية والحوادث وما شابه) أو عن قصد (مثل أعمال الشغب التي تسبب أضراراً في الممتلكات وما شابه).

الفئة الشاملة	التصنيفات الفرعية	التعريف
الوفاة أي حالة وفاة حدثت للموظفين لأي سبب كان.	الوفاة: حادث	(انظر الحوادث)
	الوفاة: القتل المتعمد (القتل)	انظر القتل أو الإصابة أو الاختطاف
	الوفاة: الطبيعية	أي حالة وفاة يمكن أن تعود إلى سبب طبيعى، مثل النوبة القلبية، والمرض، أو السكتة الدماغية.
	الوفاة: الانتحار	الحالة التي يقوم فيها الموظف بإنهاء حياته بنفسه وبشكل طوعي.
انعدام الأمن العام الحوادث المرتبطة بالسياق العام والتي تسبب انعدام الأمن وتؤثر بشكل مباشر أو غير مباشر على تقديم المعونة. يمكن أن تؤثر بشكل مباشر أو لا على الوكالة، وموظفيها أو البنية التحتية.	انعدام الأمن العام: النشاط المسلح	الأعمال التي تتضمن استخدام الأسلحة من قبل الدولة أو قوات غير تابعة للدولة أو جهات مسلحة منظمة.
	انعدام الأمن العام: الهجوم على وكالة أخرى	الهجوم الذي تُبلغ عنه وكالة أخرى من وكالات المعونة والذي لا يؤثر على الوكالة مباشرة.
	انعدام الأمن العام: الانقلاب	الانقلابات والعصيان وغيرها من أشكال التمرد التي تقوم بها قوة مسلحة. ويعرف الانقلاب بأنه محاولة (عادة ما تكون مسلحة) لإطاحة الحكومة واستبدالها سواءً كانت ناجحة أم لا، أو عنيفة أم لا. وقد تكون محاولة الانقلاب زعزعة سياسية.
	انعدام الأمن العام: تبادل إطلاق النار / القتال	أي حالة يتعرض فيها الموظف أو ممتلكات الوكالة لهجوم أو تبادل لإطلاق النار بين طرفين مسلحين أو أكثر. في هذه الحالة، لا يكون الموظفون المعنيون والممتلكات هدفاً للهجوم.
	انعدام الأمن العام: المظاهرات	أي مظاهرة (بما في ذلك الاحتجاجات والمسيرات، والاعتصامات، والإضرابات، وما شابه) عادة ما تكون غير عنيفة. وتعرف أيضاً بتجمهر الناس لغرض سياسي أو اجتماعي.
	انعدام الأمن العام: إطلاق النار	إطلاق النار المتعمد على أشخاص آخرين من غير موظفي الوكالة (انظر أيضاً: القتل أو الإصابة أو الاختطاف واستخدام الأسلحة: الأسلحة النارية)
	انعدام الأمن العام: الإضراب / عدم الظهور	قرار متعمد من قبل الموظفين بعدم الحضور للعمل لأسباب أخرى غير المرض.
	انعدام الأمن العام: الاضطرابات	الاضطرابات المدنية والسياسية، فضلاً عن السلوك الذي يؤدي إلى الاضطراب وتجمهر الناس. ويشمل هذا السلوك النهب وانتفاض السجون وإضرام الحشود للثيران والقتال العام مع الشرطة (عادة بواسطة المتظاهرين).
	القتل أو الإصابة أو الاختطاف: الاستيلاء / احتجاز رهائن	أي الحادث الذي يتم فيه الاستيلاء عنوة على الموظفين. وقد تنطوي هذه الحادثة على طلب فدية.
القتل أو الإصابة أو الاختطاف أي حادث يتسبب بمقتل أو إصابة أو اختطاف أحد الموظفين.	القتل أو الإصابة أو الاختطاف: الضرب	الحادث الذي يتعرض فيه أحد الموظفين للاعتداء، وعادة ما يتم الضرب بأجزاء الجسم (قبضة اليد، القدمين) أو بأشياء (العصي أو أشياء حادة).
	القتل أو الإصابة أو الاختطاف: القتل	حالات الوفاة التي تتم عمداً، على سبيل المثال عن طريق إطلاق النار، والاعتداء الجسدي، والتسميم، وغيره. ولا تشمل حالات الوفاة المتعمدة حالات الانتحار.

الفئة الشاملة	التصنيفات الفرعية	التعريف
القتل أو الإصابة أو الاختطاف أي حادث يتسبب بمقتل أو إصابة أو اختطاف أحد الموظفين. الأحداث الحرجة عادة.	القتل أو الإصابة أو الاختطاف: الاختفاء	الحوادث التي يختفي أو يُفقد فيها أحد الموظفين: مقارنة بين الاختفاء والاختطاف: أ) حسب الجهة الفاعلة: تميل الجهات الفاعلة الغير حكومية تميل إلى الاختطاف في حين تميل الجهات الفاعلة الحكومية أو الرسمية إلى "إخفاء" الناس الذين يشار إليهم باسم "المفقودين". ب) حسب ما يفعله الجاني للإبلاغ عن أخذ الموظف: حيث يميل المختطفون إلى تقديم مطالب (مثل الفدية)، في حين يفقد الاتصال نهائياً مع الأشخاص المختفين والمفقودين. ج) حسب الدافع: عادة ما يتم الاختطاف لتقديم مطالب محددة بينما يتم إخفاء الأشخاص لإسكات أحد الموظفين، غالباً لأسباب سياسية.
	القتل أو الإصابة أو الاختطاف: التعذيب	تشويه أو إصابة جسدية بطريقة متعمدة، والتي تعبر بوضوح عن تعذيب الموظفين.
	القتل أو الإصابة أو الاختطاف: الجروح أو الإصابات	الحادث الذي يصاب خلاله أحد موظفين بإصابات. وتتضمن معظم الجروح التي تدرج تحت هذه الفئة الجروح والإصابات التي تسبب فيها الأسلحة وليس الضرب.
الدافع تصنيف دوافع الفاعل	الدافع: الهجوم	الهجمات التي تستهدف مباشرة الوكالة.
	الدافع: المكان الخطأ أو الوقت الخطأ	الهجمات التي لم تكن موجهة إلى الوكالة أو موظفيها، والتي تأثر بها الموظفون أو ممتلكات الوكالة نظراً لما حدث بالقرب مثل هجوم عام أو هجوم موجه ضد كيان آخر أو أفراد آخرين.
الحوادث الوشيكة الحوادث التي كان يمكن أن تتسبب في الأذى أو تعيق إيصال المساعدات. وتشمل أي حالة قد أوشك فيها وقوع الحادث، بالقرب من الموظف/ وكالة المعونة / البرنامج، أو الحالات التي تمكن فيها المتضررون من تجنب أي ضرر جسيم. (وإذا نتج ضرر عن هذه الحوادث، فيتم تصنيفها تحت: القتل أو الإصابة أو الاختطاف	الحوادث الوشيكة: الجريمة	وقع الحادث الوشيك في سياق حدوث الجريمة.
	الحوادث الوشيكة: الأسلحة المتفجرة	وقعت الحوادث الوشيكة في سياق تفجير سلاح متفجر (مثل تفجير أحد المبني المجاور، أو تفجير في مطعم يرتاده موظفو الوكالة). تسجيل أحداث معينة بدلا من الاستخدام العام للأسلحة المتفجرة في بيئة غير آمنة.
	الحوادث الوشيكة: القتل أو الإصابة أو الاختطاف	الحادث الوشيك الذي كاد أن يتسبب بقتل أو إصابة أو خطف أحد الموظفين.

التعريف	التصنيفات الفرعية	الفئة الشاملة
إجلاء الموظفين لأسباب طبية، تشمل عموماً الإصابات أو الأمراض التي لا يمكن التعامل معها على نحو كافٍ في مستشفى محلي، أو مكتب الطبيب أو مركز العلاج.	الإجراءات الأمنية: الإجلاء: الطبي	الإجراءات الأمنية الإجراءات المتخذة من قبل الوكالات للتصدي لحالات انعدام الأمن، أو عند وقوع حادث أمني.
إخلاء الموظفين لأسباب أمنية. علماً بأن الإخلاء يشير إلى نقل الموظفين من البلد التي يعملون فيها. وتسمى عملية تحويل الموظفين إلى مكان آخر داخل البلد لأسباب أمنية بإعادة التوطين.	الإجراءات الأمنية: الإجلاء: الغير طبي	
بقاء الموظفين في مكانهم حتى اجتياز الخطر أو حتى وصول المزيد من المساعدة.	الإجراءات الأمنية: الإصابات	
فرض حظر التجول في المدينة أو البلد الذي يوجد فيها مكتب للمنظمة.	الإجراءات الأمنية: فرض حظر التجول	
قرار بإغلاق المكتب استجابة لسياق الأمن العام أو حدث معين.	الإجراءات الأمنية: إغلاق مكتب	
عملية المراقبة النشطة لحالة أمنية بهدف تغيير التدابير الأمنية.	الإجراءات الأمنية: المراقبة المستمرة	
عملية تعديل أنشطة الخطة إلى حد كبير من خلال توقيف نشاط أو برنامج معين.	الإجراءات الأمنية: توقيف البرنامج	
عملية نقل الموظفين إلى مدينة أخرى أو مكتب آخر داخل بلد العملية لأسباب أمنية.	الإجراءات الأمنية: الترحيل	
فرض قيود على السفر من شأنها أن تؤثر على الموظفين. هذا النوع من الأحداث شبيه باستشارة السفر، وقد يكون نتيجة للاضطرابات السياسية أو الاجتماعية، وتفشي الأمراض، أو الكوارث الطبيعية.	الإجراءات الأمنية: تقييد السفر، دون حظر التجول	العنف الجنسي أي حادث يتعرض فيه الموظف لأي شكل من أشكال العنف الجنسي.
السلوك العنيف في الجانب الجنسي.	العنف الجنسي: السلوك الجنسي العدواني	
محاولة الاتصال الجنسي بشخص آخر دون موافقته.	العنف الجنسي: محاولة الاعتداء الجنسي	
الاتصال الجنسي (عن طريق الفم أو المهبل أو الشرج) ضد إرادة ودون موافقة الشخص.	العنف الجنسي: الاغتصاب	
الاتصال الجنسي بشخص آخر دون موافقته.	العنف الجنسي: الاعتداء الجنسي	
الإغراءات التي تتضمن الصفير والصراخ و/أو لفظ عبارات ذات إيحاءات جنسية صريحة أو ضمنية غير مرغوبة.	العنف الجنسي: التعليقات الجنسية غير المرغوب فيها	
اللمسات ذات الطابع الجنسي غير المرغوب فيها بغض النظر عن شدة اللمس. يمكن أن تتضمن تحسس أو تدليك أو لمس أو إمساك أي جزء من جسم شخص آخر.	العنف الجنسي: اللمس الجنسي غير المرغوب فيه	

الفئة الشاملة	التصنيفات الفرعية	التعريف
العنف الجنسي أي حادث يتعرض فيه الموظف لأي شكل من أشكال العنف الجنسي.	العنف الجنسي: التحرش الجنسي	الإغراءات الجنسية غير المرحب بها وطلب الحصول على خدمات جنسية وغير ذلك من السلوك اللفظي أو الجسدي ذو الطابع الجنسي الذي يؤثر على توظيف الشخص المستهدف. على سبيل المثال: أ) جعل القيام بهذا السلوك شرطاً ضمناً أو صريحاً لتوظيف الفرد أو (ب) استخدام قبول أو رفض هذا السلوك من قبل الفرد كأساس لقرارات التوظيف التي تؤثر على هذا الفرد أو ج) استخدام هذا السلوك للتدخل في أداء عمل الفرد أو خلق بيئة عمل تخويفية أو عدائية أو هجومية.
التهديد التهديدات المباشرة أو غير المباشرة التي تقوم بها جهة حكومية أو غير حكومية من أجل عرقلة إيصال المساعدات.	التهديد: التحرش وجهاً لوجه	الأحداث التي يتعرض فيها الموظف لمضايقات مباشرة من قبل شخص أو مجموعة من الأشخاص (مثل التحرش بالأنشطة أو برامج الوكالة)
	التهديد: التخويف وجهاً لوجه	الأحداث التي يتعرض فيها الموظف للترهيب مباشرة من قبل شخص أو مجموعة من الأشخاص (مثلاً رؤية الموظف لأعمال الترهيب على يد العناصر المسلحة التي تقوم بدوريات بالقرب من نقاط توزيع الأغذية)
	التهديد: التهديدات وجهاً لوجه	الأحداث التي يكون فيها الموظف مهدداً مباشرة من قبل شخص أو مجموعة من الأشخاص؛ وينبغي أن تشمل شكلاً من أشكال عدم الامتثال (مثل التهديد بالانتقام لعدم إشراك شخص ما في نشاط الوكالة)
	التهديد: التهديد عن بُعد ضد وكالة	الأحداث التي تتلقى فيها الوكالة أو أحد الموظفين تهديداً لا يكون وجهاً لوجه ولكن بواسطة آلية عن بُعد (مثل البريد الإلكتروني أو الرسائل القصيرة أو الهاتف أو تهديدات عامة صادرة على موقع ويب، أو وسائل التواصل الاجتماعي (تويتر، فيسبوك). ويمكن أن تتضمن تهديدات مباشرة مثل مناداة وصياح المدنيين أثناء المظاهرات.
	التهديد: المخاطر المتعلقة بالسمعة	الأحداث التي تنطوي على مخاطر متصورة أو حقيقية أو فعلية أو محتملة تمس بالوكالة / (شعارها أو صورتها أو سمعتها).
	التهديد: التهديد بالإغلاق	الأحداث التي تنطوي على خطر الإغلاق الإجباري لنشاط أو برنامج أو وكالة.
	الشاهد	الأحداث التي يشهد فيها الموظف اعتداءً أو جريمة على موظف آخر أو أفراد أسرته أو أحد المستفيدين.
استخدام الأسلحة سجلات أنواع الأسلحة التي استخدمت في هذه الحادثة، والتي تؤثر على الموظفين أو البنية التحتية أو تقديم المعونة	استخدام الأسلحة: المتفجرات: القنابل الجوية	الأسلحة المتفجرة التي تطلق من الجو بما في ذلك الأسلحة الحارقة باستثناء القنابل العنقودية، والصواريخ أرض-أرض.
	استخدام الأسلحة: المتفجرات: القنابل العنقودية	الأسلحة المتفجرة التي تُطلق من الجو أو من الأرض، والتي يخرج منها الذخائر الصغيرة.
	استخدام الأسلحة: المتفجرات: القنابل اليدوية	جهاز متفجر صغير يلقي باليد، مصمم لينفجر بعد الأثر أو بعد فترة محددة من الوقت.

التعريف	التصنيفات الفرعية	الفئة الشاملة
انفجار الألغام الذي يكون له علاقة بالموظفين.	استخدام الأسلحة: المتفجرات: الألغام	استخدام الأسلحة سجلات أنواع الأسلحة التي استخدمت في هذه الحادثة، والتي تؤثر على الموظفين أو البنية التحتية أو تقديم المعونة
أي أسلحة متفجرة أخرى غير مدرجة فيما سبق.	استخدام الأسلحة: المتفجرات: أخرى	
جهاز تفجيري مرتجل موجه عن بُعد مثل القنابل التي تترك على جانب الطريق وتتفجر عند اقتراب الهدف منها.	استخدام الأسلحة: المتفجرات: جهاز تفجيري مرتجل موجه عن بُعد	
تشمل الصواريخ أو قذائف الهاون أو القذائف التي تطلق من نظام إطلاق متحرك أو ثابت، بما في ذلك القنابل الصاروخية.	استخدام الأسلحة: المتفجرات: المتفجرات التي تطلق من السطح	
الأجهزة المتفجرة المحمولة، مثل الحزام الناسف الانتحاري والمتفجرات في حقيبة تحمل على ظهر.	استخدام الأسلحة: المتفجرات: جهاز متفجر مرتجل محمول	
الأجهزة المتفجرة التي تنقلها المركبات، مثل السيارات المفخخة أو المركبات التي تحتوي على عبوات ناسفة.	استخدام الأسلحة: المتفجرات: جهاز متفجر	
أي استخدام للأسلحة البيولوجية في مدينة أو بلدة يوجد فيها مكتب للمنظمة.	استخدام الأسلحة: البيولوجية	
أي استخدام للأسلحة الكيميائية في مدينة أو بلدة يوجد فيها مكتب للمنظمة.	استخدام الأسلحة: الكيميائية	
أي استخدام للأسلحة النووية، سواء كانت متفجرة أو غير ذلك، في مدينة أو بلد يوجد فيها مكتب للمنظمة.	استخدام الأسلحة: النووية	
أي استخدام للأسلحة الإشعاعية التي توصف عادة باسم "القنابل القذرة" في مدينة أو بلدة يوجد فيها مكتب للمنظمة. وتتراوح الحوادث المحتملة ذات الصلة بالأسلحة الإشعاعية من الهجمات على محطات الطاقة النووية، إلى الهجمات التي تشنها الأجهزة النووية التي يمكن بناؤها من مواد إشعاعية مسروقة.	استخدام الأسلحة: الإشعاعية	
أي استخدام للأسلحة النارية أو الأسلحة المحمولة باليد التي تشمل موظفي المنظمة أو ممتلكاتها.	استخدام الأسلحة: الأسلحة النارية الصغيرة	الاحتلال
الاستيلاء على أي مبنى أو مستودع أو مجمع للمنظمة من قبل المدنيين أو موظفين حكوميين.	احتلال مكاتب المنظمة	
حادث لا يمكن وصفه بشكل كاف من قبل أي من فئات الحوادث المحددة مسبقا في هذه القائمة. لاحظ أنه إذا تم تحديد هذه الفئة، يجب على المراسل تقديم وصف كامل للحادث في حقل "وصف الحادث".	حوادث أخرى	حوادث أخرى

الأداة 3: الحوادث التنظيمية أو الخارجية



ستركز المنظمات في كثير من الأحيان على الإبلاغ عن الحوادث الداخلية وتسجيلها (أي تلك الحوادث التي لها تأثير على المنظمة وموظفيها وممتلكاتها وسمعتها) ولن تدرج الحوادث الخارجية (أي الحوادث التي تؤثر على المنظمات الأخرى) في نظامها الخاص بالإبلاغ والتسجيل. وعلى المنظمة أن تحدد الحوادث التي تؤثر على المنظمة وتقرر ما إذا كان ينبغي الإبلاغ عن الحوادث الخارجية وتسجيلها أيضاً.

وفيما يلي مثال عن شبكة وضعتها إحدى المنظمات للمساعدة في تقييم ما يمكن اعتباره حادثاً تنظيمياً وما لا يمكن اعتباره كذلك. إن المثال أدناه قابل للتكيف والتغيير استناداً إلى سياسات وإجراءات أمن المنظمة. يرجى تحري النسخة الفارغة أدناه.

الشخص المعني	ساعات العمل		هل تأثرت سلع المنظمة		المؤهلات
	نعم	لا	نعم	لا	
موظفون خارج أوطانهم (التعيينات الدولية)	X		X		حادث تنظيمي
	X			X	حادث تنظيمي
		X	X		حادث تنظيمي
		X		X	إذا لم يكن هناك عنف: لا إذا كان مع عنف: نعم
موظفون في بلدهم الأصلي (موظفون محليون)	X		X		حادث تنظيمي
	X			X	حادث تنظيمي
		X	X		حادث تنظيمي
		X		X	حادث غير تنظيمي
	X		X		حادث تنظيمي
أصحاب المصلحة الخارجيين الذين تعاقدت معهم المنظمة	X			X	حادث غير تنظيمي
		X	X		اعتماداً على نوع الحادث والسلع، وأثر الحادث: نعم أو لا
		X		X	حادث غير تنظيمي

المؤهلات	هل تأثرت سلع المنظمة		ساعات العمل		الشخص المعني
	لا	نعم	لا	نعم	
					موظفون خارج أوطانهم (التعيينات الدولية)
					موظفون في بلدهم الأصلي (موظفون محليون)
					أصحاب المصلحة الخارجيين الذين تعاقدت معهم المنظمة

الأداة 4: نموذج الإبلاغ عن الحوادث



ينظر هذا النموذج إلى المعلومات الأكثر إلحاحاً واللازمة لإدارة الحوادث الأمنية والتحليل الأولي.

الرقم المرجعي للحدث	
موثوقية المصدر وصحة تقدير المعلومات ³⁷ (وفقاً للمصفوفة المعتمدة):	

1. تفاصيل الاتصال الخاصة بالكاتب	
كاتب التقرير:	الاسم الكامل، الوظيفة (العلاقة بالمنظمة إذا كان من خارجها)
هل كاتب التقرير هو الموظف الذي شارك في الحادث؟	نعم / لا
التاريخ:	تاريخ التقديم (ورقم النسخة من التقرير إن لم يكن التقرير الأول)
2. معلومات عامة عن الحادث	
الموقع:	تفاصيل دقيقة عن موقع الحادث (بما في ذلك إحداثيات الموقع إن أمكن)
البرنامج القطري:	تفاصيل دقيقة عن برنامج (برامج) المنظمات غير الحكومية المتأثرة بالحادث
3. تصنيف الحادث	
نوع الحادث:	مقصود أو عرضي؛ داخلي خاص بالمنظمة أو خارجي؛ اختطاف؛ سرقة؛ نهب؛ ابتزاز. حادث مرور؛ إلخ

³⁷ يمكن ذكر هذا الأمر إما في بداية كل تقرير أو كملاحظة ضمن محتوى التقرير

4. تحديد خطورة الحادث	
حادث وشيك (كاد أن يقع)	أي حالة كاد أن يقع فيها حادث أمني ولكنه لم يقع، أو أي حادث وقع بالقرب من موظف مساعدات / وكالة / برنامج، أو الحوادث التي تمكن المتأثرون بها من تجنب الإصابة بأضرار جسيمة.
حادث غير حرج	لم يكن الناس خلاله مهددين جسدياً و / أو نفسياً. لم تنجم عنه أي إصابات.
حادث متوسط الخطورة	لقد تعرض الناس خلاله للتهديد الجسدي و / أو النفسي. إصابات طفيفة لا تتطلب المتابعة الطبية الممتدة.
حادث خطير	إصابات خطيرة تتطلب المتابعة الطبية الممتدة. تهديد خطير للسلامة البدنية و / أو النفسية.
حادث قاتل	وفاة أحد موظفي المنظمة كنتيجة مباشرة للحادث.
لا يزال مجهولاً	
5. وصف الحادث	
تقديم لمحة موجزة ودقيقة عن الحدث.	
6. الضحية (الضحايا)	
الأسماء الكاملة:	يُرجى توضيح ما إذا كانت الضحية موظف دولي أو محلي؟
الموظفون المحليون / الدوليون:	ما هي جنسيته؟
الجنس:	ذكر (ذكور) أو أنثى (إناث)
العمر:	كم عمر الضحية (الضحايا)؟
تفاصيل أخرى ذات صلة بالحالة:	هل كان الشخص يعاني من إعاقة أو مرض قد يكون له تأثير على الحادث؟
الأقدمية والمنصب في المنظمة:	منذ متى كان الشخص يعمل على البرنامج؟ منصب / مسؤولية الضحية داخل المنظمة.
حالة الضحية الحالية:	غير مصاب، مُصاب (حدد الخطورة، جسدية أو نفسية) أو ميت.
7. الشهود	
حدد الاسم الكامل (الأسماء) ومعلومات الاتصال بالأشخاص الموجودين عند وقوع الحادث والذين يمكنهم المساعدة في توضيح الحقائق.	

8. الإجراء الفوري المتخذ في أعقاب الحادث

جهات الاتصال الداخلية:	من الذي تم إبلاغه داخلياً عن الحادث (البرنامج / المهمة)؟
جهات الاتصال الخارجية: الجهات المانحة: منظمات إنسانية / إنمائية أخرى: وسائل الإعلام: أخرى:	ما هي السلطات الخارجية (إدارة محلية أو وطنية و / أو قضائية، عسكرية) التي تم الاتصال بها في أعقاب الحادث؟
الإجراءات المتخذة التي تؤثر على البرامج:	يترتب على الحادث عواقب على البرنامج مثل تخفيض عدد الموظفين أو وقف الأنشطة أو البرنامج ككل.
الإجراءات المتخذة التي تؤثر على الموظفين المشاركين:	المتابعة / استخلاص المعلومات / المشورة / كان أو لا يزال ضرورياً للموظفين المشاركين في الحادث.

9. التحليل الأولي - الخطر (المخاطر) على البرنامج

المخاطر التشغيلية:	إذا كان الحادث ينطوي على مخاطر جديدة أو يزيد أحد المخاطر الموجودة مسبقاً لعمليات المنظمة، يرجى التحديد. ما هي إجراءات التخفيف التي تم اتخاذها؟
مخاطر على الموارد البشرية:	إذا كان الحادث ينطوي على مخاطر جديدة أو يزيد أحد المخاطر الموجودة مسبقاً لموظفي المنظمة، يرجى التحديد. ما هي إجراءات التخفيف التي تم اتخاذها؟
المخاطر المالية/المادية:	إذا كان الحادث ينطوي على مخاطر جديدة أو يزيد أحد المخاطر الموجودة مسبقاً على المستوى المالي أو على ممتلكات المنظمة، يرجى التحديد. ما هي إجراءات التخفيف التي تم اتخاذها؟
المخاطر القانونية / المخاطر على السمعة:	إذا كان الحادث ينطوي على مخاطر جديدة أو يزيد أحد المخاطر الموجودة مسبقاً على المستوى القانوني أو على صورة المنظمة، يرجى التحديد. ما هي إجراءات التخفيف التي تم اتخاذها؟
أخرى:	

10. دعم المقر الرئيسي

وضح ما إذا كان دعم المقر الرئيسي ضرورياً، وإذا كان الأمر كذلك، فما هو نوع الدعم المطلوب.

أداة 5: تحليلات الحوادث



ستوجّه هذه الشبكات تحليل أسباب الحوادث والآثار المترتبة عنها، وكيفية تنفيذ الإدارة والمتابعة أثناء وبعد هذا التحليل الأولي.

1. تحديد أثر الحادث

مدة الحادث	كم من الوقت استمر الحادث؟
نوع السياق	وفقاً للتصنيفات المستخدمة في تنظيم السياق والنوع ومستوى العنف.
المرحلة الأمنية	كما هو محدد في الوثائق الأمنية في المنظمة.
تقدير الخسائر	
خسائر المنظمة	
الأموال	حدد التكاليف المباشرة للحادث التي تكبّدها المنظمة نتيجة للحادث (أرقام).
المعدات	حدد إذا ما كانت المعدات /الممتلكات قد تعرضت للتلف والضرر وأعطِ قيمتها.
المستندات	حدد إذا ما كانت الوثائق الحساسة (مثل قائمة موظفين) مفقودة أو أي شيء يستخدم لتوثيق المستندات (مثل الأختام) مفقوداً.
أخرى	
الشخصية	
الأموال	حدد المبالغ النقدية التي فقدها الموظفون أثناء الحادث.
المعدات	حدد إذا كانت معدات تابعة للموظفين قد تضررت خلال الحادث وما قيمتها.
المستندات	حدد حالة الوثائق الشخصية المفقودة الخاصة بالموظفين.
أخرى	حدد ما إذا كان قد تم إنجاز استخلاص المعلومات
استخلاص المعلومات العاطفية	العاطفية أم لا. اذكر التاريخ.

2. تحديد أسباب الحادث

العوامل المساهمة المحتملة (الإجابات المتعددة ممكنة) هل الحادث متصل بـ ؟		
نوع النشاط	يرتبط الحادث بنوع عمل المنظمة.	حدّد
عدم قبول برنامجنا	وقع الحادث نتيجة لعدم قبول البرنامج	حدّد
عدم كفاية التدابير المتخذة للحماية	وقع الحادث نتيجة لعدم اتخاذ تدابير الحماية	حدّد
عدم الامتثال لقواعد الأمن و / أو إجراءات التشغيل الموحدة	وقع الحادث نتيجة لعدم الامتثال للقواعد الأمنية و/أو الإجراءات	حدّد
التهور / عدم اليقظة	وقع الحادث نتيجة للتقصير أو عدم يقظة الفريق	حدّد
الافتقار إلى معدات الاتصالات	وقع الحادث نتيجة للافتقار إلى (غياب أو قصور) معدات الاتصالات اللازمة لأمن وسلامة الفريق	حدّد
الصراع (النزاعات) داخل الفريق	وقع الحادث نتيجة لصراع بين عضوين أو عدة أعضاء في الفريق	حدّد
عدم الكفاءة / عدم السيطرة على قيادة المركبة	وقع الحادث نتيجة لعدم قدرة السائق على إدارة نقل المتورطين في الحادث	حدّد
السلوك غير اللائق	وقع الحادث نتيجة للسلوك غير الملائم الذي أبداه شخص واحد أو عدة أعضاء في الفريق (انتهاك مدونة قواعد السلوك، أو ارتداء ملابس غير مناسبة، إلخ).	حدّد
تغير السياق	وقع الحادث نتيجة لتغير الحالة العامة (أي السياق)	حدّد
الصراعات الثقافية الخارجية	وقع الحادث نتيجة للصراعات الموجودة من قبل في المجتمع مثل المواجهات العرقية أو الدينية	حدّد
أخرى	اذكر عوامل إضافية غير مدرجة هنا والتي ربما قد تكون أسهمت في الحادث	

3. تحديد الأنماط والإجراءات المحتملة

السؤال / العملية	الإجابة	الآثار المحتملة (استناداً إلى التقييم)	إجراءات الوكالة المحتملة
1- هل وقع هذا الحادث من قبل وما مدى تشابهه؟	نعم	التهديد الدقيق (يتضح من الوثائق الداعمة)	الإبلاغ عن التقييمات، والاستمرار في استخدامها كأساس للقرارات الأمنية
	لا	التهديد معيب (يتضح من الوثائق الداعمة)	تغيير التقييمات والممارسات الأمنية التي تعتمد عليه
	لا	التهديد الذي عفا عليه الزمن (يتضح من الوثائق الداعمة)	تغيير التقييمات والممارسات الأمنية التي تعتمد عليه
2 - ما هي النتيجة في حال اتباع الإجراءات المناسبة؟	إيجابية	تم اتباع الإجراءات المناسبة	تعزيز الإجراءات
	سلبية	موظفون محظوظون	إعادة النظر في الإجراءات
		ممارسات أمنية خاطئة	إعادة النظر في الممارسات الأمنية
		ارتفاع احتمال المخاطر	التواصل مع الموظفين تدريب / إعادة تدريب الموظفين
3- ما هي النتيجة في حال عدم اتباع الإجراءات المناسبة؟	إيجابية	إجراءات غير ملائمة	إعادة النظر في الإجراءات أو تطبيقها على جميع الحالات
	سلبية	موظفون محظوظون	إعادة النظر في الإجراءات
		الافتقار إلى المعرفة بالإجراءات، ربما للأسباب التالية:	النظر في سبل تحسين إبلاغ الموظفين عن الإجراءات المناسبة
		- عدم تقديم إحاطة أمنية للموظفين الجدد. - عدم وجود خطة أمنية (خطط الطوارئ وإجراءات التشغيل الموحدة). - عدم الاهتمام بتزويد الموظفين بإحاطة عن الأمن والوصول إلى الخطة الأمنية. - قلة الوقت وعدم تشجيع الموظفين على قراءة الخطة الأمنية.	
		الفشل في محاولات متابعة الإجراءات، وربما للأسباب التالية:	إعادة النظر في الإجراءات والتدريب وكفاية المعدات
		- الإجراءات معقدة مما يجعل من الصعب تذكرها واتباعها. - تتطلب الإجراءات تدريبات لم يتم تقديمها. - تتطلب معدات ليست متاحة بشكل دائم.	
		يعترض الموظفون على الإجراءات، وقد يكون ذلك للأسباب التالية:	إعادة النظر في الممارسات المناسبة المتعلقة بالأمن
		- الإجراءات غير ملائمة. - الحاجة للمزيد من التدريب لإقناع الموظفين بأهمية الإجراءات. - ممارسات التوظيف غير مناسبة. - قلة آليات فرض الإجراءات داخل الوكالة.	

4. تحليل إدارة الحادث

تقديم التقارير لمديري البرامج	ما مدى نجاح نقل المعلومات؟ هل تم التقييد بالحدود الزمنية للمنظمة؟
شجرة الاتصالات	ما مدى نجاح نقل المعلومات داخل الموقع الميداني ككل؟ هل عملت شجرة الاتصالات بشكل صحيح؟
الأدوار والمسؤوليات	هل يعرف المدراء ما يجب القيام به وفقا للمسؤوليات والمهام المناطة بهم؟
التحديد المسبق للأشخاص الرئيسيين قبل وقوع الحادث	هل سبق أن حددنا بوضوح الأشخاص الرئيسيين (الخارجيين والداخليين) الذين ساعدونا في إدارة الحادث؟ هل حاولنا الاتصال بمؤسسة / سلطة لمساعدتنا؟ هل حددنا الشخص المسؤول (الأشخاص) الرئيسيين؟ قم بتحديد جهة الاتصال هذه.
التواصل بين الميدان-المقر الرئيسي-الميدان	كيف كان التواصل بين المقر الرئيسي والميدان؟ ما الذي نحتاج إلى تحسينه؟
أخرى	

الأداة 6: كيفية إجراء الاستجواب الواقعي



ينبغي أن تبدأ عملية الاستجواب الواقعي بعد الترتيب للإسعافات الأولية أو العلاج الطبي (البدني والنفسي) للشخص أو للأشخاص المعنيين. من المهم أيضاً عند الترتيب لاستجواب واقعي لأغراض جمع المعلومات مراعاة المبادئ الأساسية للإسعافات الأولية النفسية: حيث ينبغي استخلاص المعلومات عند ضمان توافر الأمن المادي والنفسي الأساسي، وخلق مساحة آمنة، وتمكين الناجين وتوخي الوضوح فيما يتعلق بإجراءات العملية والتوقعات والمتابعة وما إلى ذلك.³⁸

وينبغي عدم الخلط بين الاستجواب الواقعي والاستجواب العاطفي (يعرف أيضاً باسم defusing). ليس الغرض من المعلومات الواردة أدناه محاولة تدريب القراء على الاسعافات الأولية النفسية أو جعلهم محققين محترفين. إنما هي قائمة نصائح لإجراء مقابلات آمنة ومفيدة لتقصي الحقائق في نطاق أغراض الإبلاغ الحادث. حيث ينبغي معالجة الحوادث المسببة للصدمات من قبل المحترفين أو الموظفين المدربين ضليعين في تقديم الاسعافات الأولية النفسية (PFA).

عند بدء الاستجواب لاستخلاص المعلومات الواقعية، ذكّر جميع المعنيين أن الغرض منه هو التعلّم والوقاية وليس إيجاد الأخطاء.

الاستعداد لاستخلاص المعلومات:

- تحديد الشخص الذي سيجري الاستجواب.
- تحديد الشخص الذي سيتم استجوابه لاستخلاص المعلومات، وينبغي أن تحدد الإجراءات التنظيمية إذا ما كان على الموظفين المتورطين في الحادث التواجد معاً أو الحضور بشكل منفصل. ويمكن أن يشير الإجراء إلى أنه ينبغي اتخاذ القرار بشأن هذا الخيار على أساس كل حالة على حدة، وذلك تبعاً لطبيعة الحادث والقيود اللوجستية. وفي حين أن تنظيم استجواب استخلاص المعلومات الجماعي لديه العديد من المزايا (مزايا لوجستية، وأخرى متعلقة بالسرد)، إلا أنه يمكن أيضاً أن يؤدي إلى إعادة كتابة الحادث "وتغيير الحقائق" (يمكن أن يؤثر الشهود والضحايا على بعضهم البعض، وقد تختلف تصوراتهم، وقد يخشى الموظفون إبداء الآراء حول الأسباب والمسؤوليات أمام الآخرين، إلخ).
- إعلام الأشخاص الذين سيتم استجوابهم بمن سيكون حاضراً أثناء استخلاص المعلومات.

38 للمزيد من المعلومات حول الإسعافات الأولية النفسية، انظر المبادئ التوجيهية لمنظمة الصحة العالمية على هذا الرابط

- تحديد مكان آمن لإجراء استجواب استخلاص المعلومات. قم باختيار مكان آمن ومريح للفرد مثل قاعة مؤتمرات أو مكتب خاص.
- السماح للشخص الذي سيتم استجوابه لاستخلاص المعلومات باقتراح أفضل وقت للقيام بذلك (مراعاة القيود الأخرى) وذلك تمهيداً مع إجراءات الإبلاغ الخاصة بمنظمتك.
- قم بإعداد الأسئلة الخاصة بك، والتي يمكن أن تتبع نموذج الإبلاغ عن الحوادث وتغطي نفس العناصر. قد لا تحتاج إلى طرح هذه الأسئلة أثناء المقابلة ولكن يمكنك استخدامها لإرشادك إذا أردت ذلك ويجب أن تكون الأسئلة مفتوحة.
- ممارسة الوعي الذاتي من خلال تحديد انحيازك المحتمل، ووضع ذلك جانباً أثناء إجراء الاستجواب، والقيام بالتحليل لاحقاً.

خطوات استخلاص المعلومات:

1. قم بإجراء المقابلة في مكان هادئ وخاص. لا تنسَ ملاطفته عند وصوله وتقديم كوب من الماء أو الشاي أو القهوة والتأكد من أنه ليس متعباً وأنه قد تم استجوابه عاطفياً.
2. اذكر بأن الغرض من استخلاص المعلومات هو تقصي الحقائق وليس البحث عن الأخطاء.
3. لا تعطي وعوداً بالسريّة ولكن أخبر الفرد أنك سوف تشارك المعلومات فقط مع أولئك الذين عليهم معرفتها.
4. أخبر الشخص بشكلٍ تقريبي عن مقدار الوقت الذي سيستغرقه استخلاص المعلومات.
5. اطلب من الفرد إعادة سرد روايته لما حدث دون مقاطعة. لا تنسَ تدوين الملاحظات أو تسجيل ردوده.
6. اسأل أسئلة توضيحية لتعبئة المعلومات المفقودة. استخدم أسئلة مفتوحة.
7. قم بإعادة سرد المعلومات التي تم الحصول عليها مرة أخرى على الشخص لتصحيح أي تناقضات.
8. اسأل الشخص عما كان قد يمكن تفاديه في الحادث مع التركيز على الظروف والأحداث التي سبقت الحادث. يمكن أن يساعد هذا في التحليل.
9. تجنّب التعبير عن أفكارك أو آرائك أو استنتاجاتك حول الحادث أو ما يقول الشخص.
10. قم بإبلاغ الشخص الذي تمت معه المقابلة حول الخطوات المقبلة.
11. أشكر الشخص على وقته.
12. استكمل توثيق استخلاص المعلومات عن طريق إكمال نموذج تقرير الحادث.

أمثلة على الأسئلة المفتوحة:

- أين كنت في وقت وقوع الحادث؟
- ماذا كنت تفعل في ذلك الوقت؟
- هل لاحظت أي شيء غير اعتيادي؟
- ماذا رأيت أو سمعت؟
- كيف كانت الظروف البيئية (الطقس، والضوء، والضوضاء، إلخ) في ذلك الوقت؟
- ما الذي كان يفعله الموظفون المصابون في ذلك الوقت؟
- برأيك، ما هو سبب الحادث؟
- كيف يمكن، في رأيك، منع وقوع حوادث مماثلة في المستقبل؟
- هل كان هناك أي شهود آخرين؟ هل تعرف أسماء الشهود الآخرين؟
- ما هي علاقتك بالأشخاص الآخرين المشاركين في الحادث؟
- ما هي التفاصيل الأخرى التي ترغب في مشاركتها؟

ما الذي يجب تفاديه:

- تخويف الشخص أو مقاطعته أو الحكم عليه.
- مساعدة الفرد في الإجابة على الأسئلة.
- طرح أسئلة توجيهية.
- طرح العديد من الأسئلة في نفس الوقت.
- التورط عاطفياً في الاستجواب.
- التسرع في الاستنتاجات.
- الكشف عن اكتشافات التحقيق.
- تقديم وعود لا يمكن الوفاء بها.

التحليل:

من أجل تمكين الأشخاص وإعطائهم الفرصة لتبادل التعليقات الثاقبة، نقترح أن تطلب منهم تحليل الحوادث أثناء استخلاص المعلومات. ومع ذلك، تذكر أن حكمهم على الأمور يمكن أن يتأثر بالحدث الذي تسبب لهم بالصدمة. ويتعين على الشخص الذي أكمل تقرير الحادث تحليل أسباب الحادث. إن الغرض من استخلاص المعلومات هو تقصي الحقائق لتحديد جميع العوامل المساهمة في وقوع الحادث.

وقد تساعدك الأسئلة التالية في تحليل العوامل المساهمة:

- هل كانت إحدى الظروف الخطرة عاملاً مساهماً؟
- هل كان الموقع عاملاً مساهماً؟
- هل كان الإجراء عاملاً مساهماً؟
- هل كان غياب معدّات الوقاية الشخصية أو معدّات الطوارئ عاملاً مساهماً؟
- هل كانت إجراءات التشغيل الموحدة عاملاً مساهماً وهل ينبغي تحديثها لتعكس حقيقة جديدة على أرض الواقع؟
- هل كانت ديناميكيات الفريق عاملاً مساهماً، وما هو شعورك حول ما يمكننا القيام به لتحسين ذلك؟

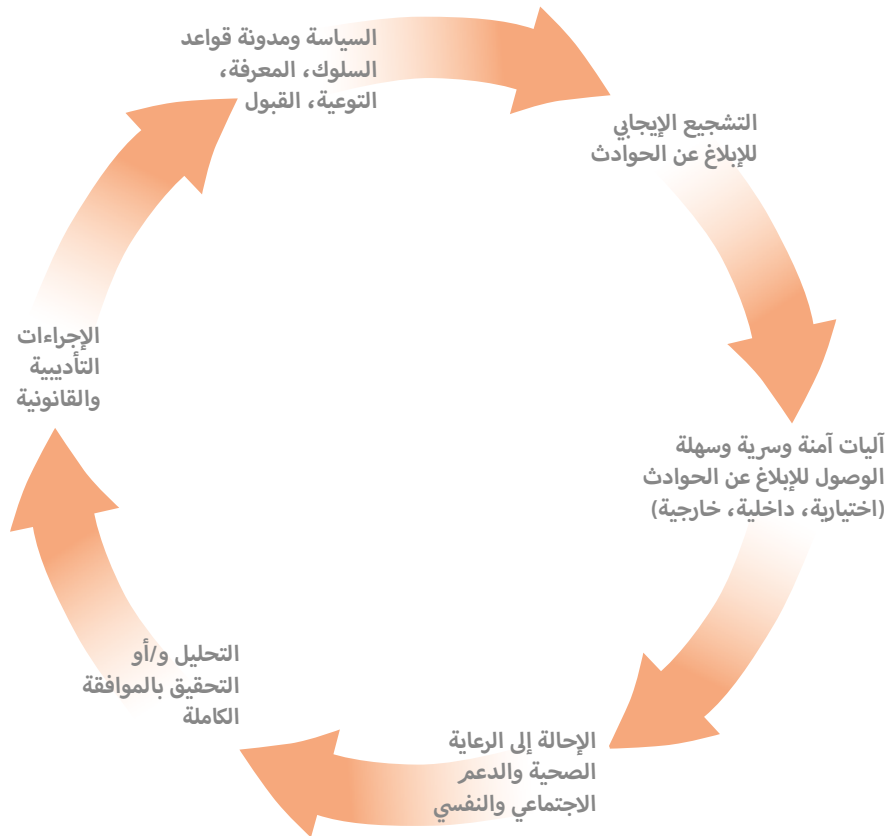
لا تساعد عبارات مثل "كان الموظفون مهملين" أو لم يتبع الموظف إجراءات السلامة"، "الوقت الخطأ، المكان الخطأ" على الوصول إلى السبب الجذري للحدث. ولتجنب هذه الاستنتاجات المضللة ركز على سبب وقوع الحادث مثل: لماذا لم يتبع الموظف إجراءات السلامة؟".



الأداة 7: الممارسات الجيدة للإبلاغ عن الحوادث ذات الصلة بالاعتبارات الجنسانية وآليات الشكاوى للإبلاغ عن الاستغلال والانتهاك الجنسيين (SEA)

توفر هذه الأداة ملخصاً للممارسات الجيدة في الإبلاغ عن الحوادث ذات الصلة بالاعتبارات الجنسانية والاستغلال والانتهاك الجنسيين (SEA). ويمكن لهذه الممارسات أن توجّه المنظمات أثناء تطوير وتكييف أنظمتها.

دورة الإبلاغ عن الحوادث الحساسة³⁹



³⁹ تم استخلاص هذه الأداة من مقالة بيرسو (2012)، الجنسانية والأمن: المبادئ التوجيهية لتعميم مراعاة الجنسانية في إدارة

السياسة:

تعتبر السياسة الأساس الذي يقوم عليه الإبلاغ الجيد عن الحوادث وقد تتضمن شرط الكشف والإبلاغ عن المخالفات. وينبغي التركيز بوجه خاص على تعزيز الإبلاغ عن الحوادث. ينبغي أن يكون الإبلاغ عن حوادث معينة إلزامياً باستثناء الحالات التي يكون فيها الإبلاغ خياراً بالنسبة للشخص مثل حوادث التحرش والعنف القائم على نوع الجنس (GBV). (يندرج الاستغلال والانتهاك الجنسيين (SEA) في إطار مدونة سلوك وسياسات مختلفة. ومن واجب الموظفين الإبلاغ عن حوادث الاستغلال الجنسي والإيذاء وإلا فقد يواجهون إجراءات تأديبية. انظر أدناه لمزيد من المعلومات).

الوعي:

يجب أن يكون الموظفون على دراية عمّا يشكّل حادثاً مع التركيز بشكل خاص على الحالات والحوادث التي لا يتم التطرق إليها بشكل كبير مثل التحرش والعنف القائم على نوع الجنس، أو الحوادث الوشيكة، أو الحوادث الصغيرة. يمكن تعزيز الوعي من خلال خلق بيئة من الارتياح والثقة في الإبلاغ عن الحوادث أثناء التوجيهات والدورات التدريبية والاجتماعات، وما إلى ذلك. كما يجب على الموظفين معرفة حقوقهم وخياراتهم.

خيارات/إجراءات الإبلاغ عن الحوادث:

ينبغي إنشاء قنوات عدة للإبلاغ عن الحوادث. الأمر الذي سيتيح خيارات إضافية للموظفين اعتماداً على مستوى الراحة أو الحاجة إلى السرية. تشمل الخيارات (على سبيل المثال لا الحصر): الإبلاغ الإلكتروني من خلال شبكة الإنترنت الخاصة بالوكالة، خط هاتف ساخن (مدفوع الرسوم أو مجاني)، جهات، والقنوات التي تتجاوز بعض مستويات الإدارة (في الحالات حيث يتم الإبلاغ عنها) إلخ.

استخدام جهات الاتصال:

يجب اختيار جهات الاتصال بعناية وتدريبها استناداً إلى صفاتها الشخصية وقدراتها، وقدرتها على الحفاظ على السرية والموضوعية. إن وجود عدد من جهات الاتصال المختلفة (الدولية والوطنية، ذكورا وإناثا) من شأنه أن يزيد من الراحة ويسهل الحصول على التقارير.

التحليل/التحقيقات:

سيتم لاحقاً استخدام متابعة الحوادث لاسترشاد تحليل المخاطر، أو تدابير الحد من المخاطر أو مستويات وعي الموظفين. وقد يكون من الضروري إجراء بعض التحقيقات الداخلية من قبل موظفين مدربين بشكل جيد في حالة انتهاك السياسات الداخلية، وسيطلب ذلك إبلاغ السلطات المحلية / الشرطة لإجراء تحقيق خارجي في حالة حدوث خرق مؤكد للقوانين المحلية.

الإجراءات التأديبية:

في حالة وجود سلوك سيء من جانب الموظف (تبعاً لشدة الحادث، والقوانين المحلية بما في ذلك قوانين العمل)، ينبغي اتخاذ تدابير تأديبية ويجب تطبيقها بشكل منظم على الموظفين المحليين / الوطنيين / الدوليين / ذكورا وإناثاً.

الذاكرة المؤسسية:

تجنب توظيف أي شخص لديه سوابق في ارتكاب أي نوع من الحوادث الخطيرة بما في ذلك الفساد والتحرش الجنسي أو العنف الجنسي، بما في ذلك الاستغلال الجنسي والاعتداء الجنسي والعنف المنزلي. قد يبدو ذلك أمراً بديهياً، ولكن تاريخاً طويلاً من الأدلة القولية

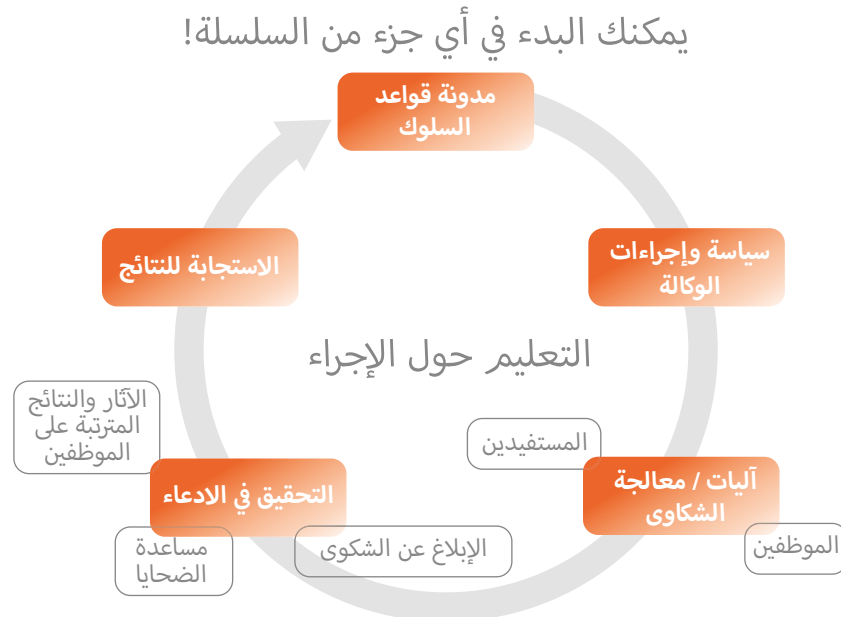
يشير إلى حالات إعادة تعيين الجناة في مكاتب قطرية مختلفة - أحيانا حتى من قبل نفس الوكالة. إذا سمحت القوانين ذات الصلة التي تحكم أصحاب العمل والموظفين، يمكنكم التنسيق مع الوكالات الأخرى لإنشاء نظام لتبادل المعلومات حول الموظفين الذين تم إنهاء عقودهم بسبب المضايقة والعنف الجنسي و / أو الاستغلال والاعتداء الجنسيين. ولا بد من الاستعانة بالممارسات التي تشمل الفحوص المرجعية والفحص الدقيق.

إطار الاستغلال والانتهاك الجنسيين

مبادئ الاستغلال والاعتداء الجنسيين المحددة من قبل اللجنة الدائمة المشتركة بين الوكالات (IASC):

- يعتبر الاستغلال والانتهاك الجنسيين من قبل العاملين في المجال الإنساني من التصرفات المشينة، وبالتالي فهي سبب لإنهاء التوظيف.
- يحظر أي نشاط جنسي مع الأطفال (الأشخاص الذين تقل أعمارهم عن ١٨) بغض النظر عن سن الرشد أو سن الرشد محلياً ولا يعتبر الإخطاء في السن الطفل دفاعاً.
- يحظر تبادل المال، أو السلع أو التوظيف أو الخدمات مقابل الجنس، بما في ذلك الخدمات الجنسية أو أي شكل آخر من السلوكيات المذلة أو المهينة أو الاستغلالية.
- ويشمل ذلك تبادل المساعدة التي تعود في الأساس إلى المستفيدين.
- العلاقات الجنسية بين العاملين في المجال الإنساني والمستفيدين محبطة للغاية لأنها تستند إلى ديناميكيات السلطة غير المتكافئة بطبيعتها. وهذه العلاقات تضعف مصداقية ونزاهة عمل المعونة الإنسانية.
- في حال ساورت أحد الموظفين مخاوف وشكوك بشأن قيام أحد زملائه باعتداء جنسي أو استغلال جنسي، سواءً كان ذلك الشخص في نفس الوكالة أم لا، فإن عليه الإبلاغ عن ذلك من خلال آلية الإبلاغ المعمول بها في وكالته.
- إن العاملين في المجال الإنساني ملزمون بإنشاء والمحافظة على البيئة التي تمنع الاستغلال والاعتداء الجنسيين وتعزز تنفيذ مدونة قواعد السلوك الخاصة بهم. يتحمل المديرون على كافة المستويات مسؤولية دعم وتطوير نظام الحفاظ على هذه البيئة.

دورة الإبلاغ عن الاستغلال والانتهاك الجنسيين⁴⁰



الأداة 8: خطة العمل لمتابعة الحادث



تسرد هذه الأداة الأسئلة التي يتعين تضمينها في خطة المتابعة التي ينبغي تنفيذها عقب كل حادث، بصرف النظر عن حدّته.

الرقم المرجعي للحادث: #

وصف الإجراء الذي يتعين اتخاذه بمصطلحات دقيقة	الإجراء الواجب اتخاذه (سطر واحد لكل إجراء)
في أي مستوى، اسم أو منصب	بواسطة من
من سيشارك، داخل أو خارج المنظمة	مع من
التكاليف التقديرية والاحتياجات، وإجراءات الشراء في المنظمة	الخدمات اللوجستية المطلوبة والميزانية
متى يجب تنفيذ الإجراء؟ تاريخ محدد أو مراجعة دورية؟	متى
هل المدير هو المسؤول عن ذلك؟ أو منسق شؤون الأمن؟ شخص آخر	من المسؤول عن تنفيذ الإجراء
من قبل من وبأي تاريخ؟	المراجعة والتحقق من الصحة
توقيع الموظفين المشاركين في التنفيذ والرقابة	التوقيع

وضع الحادث
وضع إدارة الحوادث

الأداة 9: أنظمة إدارة معلومات الحوادث الأمنية



الأنظمة المتاحة للإبلاغ وتسجيل وتخزين وتحليل الحوادث الأمنية التي تُمس المنظمة على المستوى المركزي.

تسجيل الحوادث وطريقة الإبلاغ عنها	النظام	المزايا	العيوب	عوامل الإنشاء وتكاليف التشغيل
سرد مكتوب عن الحادث	- رسائل البريد الإلكتروني - ورقة جوجل - منصة Shared Google شير بوينت (SharePoint)	تكلفة الإعداد والإنشاء منخفضة جداً.	يعمل بشكل جيد فقط في حال استخدامه بشكل منهجي. المخاطر: - عدم القدرة على الوصول إلى المعرفة الفنية، وفي بعض الأحيان تعذر الوصول في الأوقات التي يغادر فيها الموظفون. - عدم اتساق التقارير. مع ما يترتب على ذلك من آثار على صعوبة مقارنة المعلومات. - يتطلب وقت إدخال طويل أثناء عملية التحليل.	تكلفة الوقت الذي يقضيه الموظفون في إنشاء النظام. تكلفة الوقت الذي يقضيه الموظفون في كتابة التقارير السردية. تكلفة الوقت الذي يقضيه الموظفون في تحويل المعلومات إلى شكل منتظم. تكلفة الوقت الذي يقضيه الموظفون في إجراء التحليل، والذي من المرجح أن يستغرق وقتاً طويلاً لأن النظام نفسه لا يدعم التحليل

تسجيل الحوادث وطريقة الإبلاغ عنها	النظام	المزايا	العيوب	عوامل الإنشاء وتكاليف التشغيل
جداول بيانات إكسيل لتسجيل الحوادث باستخدام الترميز المنهجي	رسائل لإعداد جدول بيانات إكسيل للحقول التي سيتم تسجيلها. يمكن استخدام جدول بيانات إكسيل لتصنيف المعلومات المقدمة بشكل منظم ومكتوب.	تكلفة الإعداد والإنشاء منخفضة. لا يوجد تكلفة مستشارين لأن بالإمكان إنجاز العمل بسهولة من داخل المنظمة. يمكن أن تعمل هذه بشكل جيد جداً مع المنظمات التي تبدأ تسجيل الحوادث والتي لديها عدد محدود من الحوادث التي تستدعي التسجيل والإدارة.	يمكن أن يصبح من الصعب إدارتها عند اتباع العديد من فئات وأنواع الأحداث. تتطلب هذه الجداول إجراء التحليل يدوياً ما قد يستغرق وقتاً طويلاً. وحده الشخص المخوّل بالوصول إلى جدول البيانات يميل إلى معرفة وفهم النظام. انخفاض الحافز لدى الموظفين لكتابة التقارير حيث انهم غير مدركين لآلية التسجيل.	تكلفة الوقت الذي يقضيه الموظفون في تطوير نظام إكسيل مناسب. تكلفة الوقت الذي يقضيه الموظفون في ترجمة المعلومات المكتوبة إلى فئات ذات ترميز. تكاليف تنفيذ التحليل من قبل الموظفين
الاشتراك في منصة إلكترونية لإدارة البيانات	تقدم بعض الشركات الخاصة وبعض المنظمات غير الربحية منصات عبر شبكة الانترنت لإدارة معلومات الحوادث الأمنية.	أنظمة فعالة ضمن وظائف التحليل المدمج. تمنح معظم النظم مستويات مختلفة من الدخول مصممة خصيصاً للموظفين الميدانيين وكذلك الإدارة العليا. يتم الاستعانة بمصادر خارجية للنظر في الشؤون التقنية. تزيد قدرة الموظفين الميدانيين على الدخول المباشر من تحفيز الإبلاغ. تضمن توفير المزيد من المعلومات المنهجية حيث يستخدم الجميع نفس النظام بنفس التعليمات. تقلل من عبء العمل على موظفي التحليل في المقر الرئيسي حيث يمكن أن يكون التحليل وظيفة مدمجة النظام.	تكاليف التشغيل الشهرية. قد يكون من الصعب أو المكلف طلب تغييرات لتكييف النظام مع المتطلبات الخاصة بالمنظمة.	رسوم الاشتراك.

تسجيل الحوادث وطريقة الإبلاغ عنها	النظام	المزايا	العيوب	عوامل الإنشاء وتكاليف التشغيل
نظام مصمم خصيصاً على الانترنت	كلّفت بعض المنظمات بتطوير أنظمة إلكترونية خاصة بالمنظمة. تمكنت بعض المنظمات من استخدام النظم القائمة وبناء الإبلاغ عن التقارير إضافة إلى المنصات الحالية المستخدمة للبريد الإلكتروني، مثل شير بوينت (SharePoint)	يستجيب هذا النظام للاحتياجات التنظيمية والتعاريف الداخلية. إذا كان متصلاً بالنظم القائمة، قد يتعلم الموظفون كيفية استخدامه بشكل أسرع بكثير.	تكون تكاليف التطوير العالية إذا كان هناك حاجة إلى متخصصين في تقنية المعلومات من خارج المنظمة. إذا استطاعت المنظمات الاستعانة بقسم تقنية المعلومات فستكون التكاليف أقل. يمكن أن تكون تكلفة الصيانة عالية إذا لزم الاستعانة بمستشاري تقنية المعلومات من خارج المنظمة، وستكون التكاليف أقل إذا نفذت الصيانة من قبل قسم تقنية المعلومات.	تكاليف التطوير والصيانة.

الأداة 10: تخزين الحادث



الهيكل الأساسية عند استخدام جداول البيانات إكسيل لتخزين الحوادث

إن تصميم هيكل مثالي لتخزين معلومات الحوادث الأمنية على جدول إكسيل مهمة صعبة للغاية. فوجود مجموعة كبيرة ومتنوعة من الحوادث التي ينبغي النظر فيها من أجل اتخاذ القرارات الاستراتيجية المتعلقة بسياق الأمن والمعلومات التفصيلية المطلوبة في بعض الجوانب يجعل من المستحيل وضع هيكل بسيط واحد يتماشى مع جميع الحالات والأوضاع. ويتمثل التحدي في إيجاد التوازن الصحيح بين إبقاء هذه الهياكل بسيطة وقابلة للتطبيق بعد تخزين المعلومات الأساسية اللازمة وضمان وجود تفاصيل كافية لجعل المعلومات مفيدة أثناء تقديم التوصيات المتعلقة بالسياسات.

يوفر هذا الدليل مثالين مختلفين عن كيفية تخزين معلومات الحوادث على جدول بيانات إكسيل. ونوصي المنظمات التي تصمم جداول البيانات الخاصة بها بالنظر في كل من الأمثلة المشتركة وأخذ العناصر الأكثر ملاءمة لأولوياتها الخاصة. يُرجى مراجعة الأدوات الأخرى للتعاريف المقترحة في مختلف المجالات.

يمكن الاطلاع على هذين الجدولين وتحميلهما من صفحة RdeR الخاصة بالمشروع. يُرجى النظر في العناصر التالية:

- جدول بيانات SiND لفئات الأحداث
- نموذج سجل الحوادث

فيما يلي المبادئ الأساسية التي يجب مراعاتها عند تصميم جدول بيانات إكسيل لمعلومات الحوادث الأمنية.

وحدات التحليل

كل سطر في جدول بيانات إكسيل يخزن وحدة رئيسية واحدة من المعلومات وفي معظم الحالات سيكون هذا الحدث. يشير كل سطر إلى حدث فريد، ويتم استخدام الأعمدة لتقديم التفاصيل حول الحدث.

يمكن اتباع الطرق التالية من أجل تخزين وحدات أخرى من المعلومات، مثل معاملة الموظفين كوحدات فردية (بدلاً من عدد مرتبط بحدث)، أو تسجيل التفاصيل عن المواد المفقودة أو تتبع الاستجابات:

- إنشاء صفحة ثانية/ثالثة/رابعة على مصنف إكسيل خاص 'بالموظفين' أو 'المواد' أو 'الاستجابة'. في جداول البيانات الجديدة هذه يخزن كل سطر المعلومات الفردية لكل

شخص وكل عنصر تالف أو مفقود أو كل استجابة وما إلى ذلك. وبالتالي فإن كل جدول بيانات فيه وحدة مختلفة. في حال تأثر أربعة موظفين في حادث واحد فإن جدول بيانات الحادث سيكون فيه سطر واحد (وحدة واحدة) للحادث ولكن أربعة سطور (أربع وحدات) للموظفين (انظر الأمثلة أدناه). إذا تعرضت سيارتان للضرر في الحادث فإن "جدول المواد" سيحتوي سطرين، واحد لكل سيارة وهكذا يصبح كل موظف وسيارة وحدة قائمة بذاتها، ويمكن استخدام هذه الصفحات لتخزين التفاصيل التي قد تكون مفيدة في التحليل الشامل.

- وتتمثل ميزة هذا النظام في أنه يسهل تقديم تحليل مفصل يتجاوز وصف الحادث ومن الممكن أيضاً استخدام القوائم المنسدلة لفئات حصرية يتم اختيارها لكل فرد. وتحتوي الصفحة على معلومات إضافية موجودة بشكل أكثر كثافة. والجانب السلبي لهذا النظام هو أن البيانات تصبح أكثر تعقيداً.
- إذا تم فتح جداول بيانات إضافية فمن الضروري استخدام أرقام تعريفية فريدة لكل حادث في العمود الأول لضمان إمكانية ربط المعلومات مرة أخرى به.

- دمج وحدة مختلفة (مثل الموظفين والمواد) في الصفحة التي تكون وحدة التحليل فيها هي الحادث. ويمكن القيام بذلك عن طريق إنشاء سلسلة من الأعمدة الإضافية في كل مرة تتغير فيها وحدة العد من الحادث إلى الموظفين أو المواد أو الاستجابة. ويمكن استخدام ألوان مختلفة للإشارة إلى ذلك.

- على سبيل المثال، يمكن أن تشمل الأعمدة عدد الموظفين المتضررين من الحادث من خلال العديد من الأعمدة الإضافية حسب الحاجة لتصنيف جميع الموظفين بمعلومات إضافية، والتي يجب بعد ذلك تقسيمها إلى أعمدة خيارات متعددة (انظر جدول قاعدة بيانات أمن العاملين كمثال حول كيفية تسجيل معلومات مفصلة عن الموظفين بجانب بعضها البعض).

بعض الاختلافات في المعلومات عند استخدام صفحات إكسيل وحيدة أو متعددة

تظهر الأمثلة أدناه نفس المعلومات حول أربعة أشخاص متضررين في حادث واحد تخزنه وحدة التحليل 'الحادث' ووحدة التحليل 'الموظفين'. يتطلب تخزين المعلومات حول الموظفين في جدول بيانات وحدة التحليل فيه هي الحادث المزيد من الأعمدة لتخزين تفاصيل أقل. كما أنه من غير الممكن تخزين التفاصيل حول الأفراد (سيكون من الصعب جداً إضافة معلومات عن العمل وعمّا إذا كان التأمين قد غطى الاستشارة المقدمة بعد الحادث). إذا تم استخدام الموظفين كوحدة التحليل، فمن السهل تسجيل معلومات أكثر تفصيلاً. ويمكن أن يساعد هذا التفصيل الإضافي في تحديد الاتجاهات أو تحديد توصيات محددة للعمل، على سبيل المثال تلك المتعلقة بتغطية التأمين.

صفحة واحدة لوحات الحادث:

وحدة التحليل	عدد الموظفين المتضررين	أثنى	ذكر	موظف دولي	موظف وطني	آخر	حالات الوفاة	جرحي
1 الحادث	4	1	3	1	2	1	1	3

صفحات متعددة لوحداث مختلفة (مثل الموظفين أو المواد أو الاستجابة):

وحدة التحليل	معرفة الحادث الفريد	نوع الجنس	الحالة	العمل	الأثر	تغطية التأمين للاستشارة
1 الموظف	1 الحادث	أنثى	موظف دولي	موظف مهني	إصابة	مغطى
2 الموظف	1 الحادث	ذكر	موظف وطني	سائق	وفاة	غير قابل للتطبيق
3 الموظف	1 الحادث	ذكر	موظف وطني	موظف مهني	إصابة	غير مغطى
4 الموظف	1 الحادث	ذكر	متطوع	متطوع	وفاة	غير مغطى

خيارات متعددة أو حصرية بشكل متبادل

يمكن تسجيل المعلومات كخيارات متعددة (ينطبق أكثر من وصف واحد) أو كخيارات متبادلة حصرية (يمكن تطبيق خيار واحد فقط).

- **خيارات متعددة** في أعمدة بجوار بعضها البعض. يمثل كل عمود سمة معينة ويُستخدم جدول البيانات للإشارة إلى أن الخيار المحدد ينطبق على الحادث. ويمكن إجراء ذلك باختيار "نعم" أو رقم (مثل "1") أو خيار من القائمة المنسدلة. بالنسبة للخيارات التي لا تنطبق، فإما تُترك فارغة (عمل أقل من حيث الترميز) أو يتم تحديدها على أنها لا تنطبق عن طريق اختيار 'لا ينطبق' أو "0" (وهذا يجعل من السهل التحقق من أن الأرقام الإجمالية صحيحة وإيجاد الأخطاء أيضاً).
- **يتم عرض الخيارات الحصرية بشكل متبادل** في شكل خيارات قائمة منسدلة يمكن اختيارها عند تعبئة المعلومات في عمود معين. تتيح لك القوائم المنسدلة تسجيل معلومات إضافية وضمان الاتساق في الهجاء. ومع ذلك، ينبغي أن تستخدم في حالة إذا كان خيار واحد فقط قابل للتطبيق. راجع جدول بيانات فئات الحوادث لـ SiND للاطلاع على أمثلة عن القوائم المنسدلة.
- **يمكن دمج الخيارات المتعددة والحصرية بشكل متبادل** في إدارة البيانات ويمكن أن يحتوي جدول البيانات المصمم بشكل جيد على سلسلة من الأعمدة التي تعرض خيارات متعددة (على سبيل المثال، قد يتم تطبيق كل الخيارات أو بعضها على كل حادث ويتم تعبئة الأعمدة كما هو مطلوب). وتحتوي هذه الخيارات على قائمة مرتبطة بخيارات القائمة الحصرية بشكل متبادل (على سبيل المثال، في كل مرة يتم فيها اختيار أحد الخيارات لا يشير النظام إلى "نعم" أو "رقم" فقط بل يحدد الفئة الفرعية ضمن الخيار). للاطلاع على مثل هذا النظام راجع جدول بيانات فئات الحوادث لـ SiND.

الأداة 11: التقنية المستخدمة في الإبلاغ عن الحوادث وتسجيلها



كل نظام للإبلاغ والتسجيل مختلف عن الآخر ولديه مزاياه وعيوبه. وسيعتمد النموذج الأنسب لمنظمة محتملة على مستوى القدرات التقنية لدى الوكالة وحجم العمليات وحجم الموارد المالية وإلخ.

انظر إلى الجدول أدناه لمقارنة بعض نظم الإبلاغ عن الحوادث عبر شبكة الإنترنت.⁴¹

مستوى حماية البيانات	رسوم يائنة متكاملة	مصمم خصيصاً	المعيار	البرمجيات كخدمة	قائم بذاته	مرخص	مصدر مفتوح (مجاني)	الرسوم	
••			•		•		•		Ushahidi
••	•		•	•		•		•	SIMSON
••	•		•		•		•		Open DataKit
••	•		•	•	•	•		•	SharePoint
••	••	•		•		•		•	NAVEX Global™
••	•	•				•		•	IRIS
••	•	•				•			RIMS

•• لم تُحلّل

يعرض القسم التالي مزايا وعيوب النظم المستخدمة حالياً من قبل المنظمات التي أسهمت في هذا الدليل. لمزيد من المعلومات حول أي من هذه الأنظمة، يُرجى اتباع الروابط المقدمة.

⁴¹ تم استخراج بعض الأدوات التي تمت مشاركتها في هذه الأداة من مقال غير منشور لمنتدى الأمن الأوروبي المشترك بين الوكالات (EISF): دو بالاسيوس، جي (2017). "إدارة المعلومات الأمنية: نظرة فاحصة على نظم الإبلاغ عن الحوادث". لمنتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

SharePoint

هو تطبيق على شبكة الإنترنت يتكامل مع نظام Microsoft Office. وهو يُباع أساساً كنظام لإدارة وتخزين الوثائق غير أنه منتج قابل للضبط والتخصيص بشكل كبير، وتستخدمه المنظمات بطرق وأشكال مختلفة. على الرغم من ضرورة شراء رخصة لاستخدامه، إلا أن بعض منتجات Office 365 Microsoft مجانية للمنظمات غير الربحية. SharePoint نظام يمكن استخدامه لتبادل المعلومات بأشكال مختلفة فمن الممكن إنشاء نماذج على الإنترنت متاحة فقط للمستخدمين المرخص لهم.

المزايا	القيود
لكونه من منتجات ميكروسوفت فإن SharePoint يتوافق مع برامج معالجة البيانات مثل وورد، إكسيل، بوربوينت وغيرها، وهذا يسمح للمنظمة بترحيل البيانات من النظام إلى هذه التطبيقات بسهولة وتبادل وتحليل المعلومات باستخدام البرامج المألوفة وقد لا تحتاج إلى تثبيت برامج جديدة أو تدريب الموظفين على استخدام برامج جديدة. ويمكن إدارة تطوير النظام داخلياً من قبل فريق تقنية المعلومات المسؤول عن تطوير وصيانة SharePoint.	على الرغم من أنه من الممكن تشغيل عمليات المسح باستخدام SharePoint، إلا أنه ليس من البرمجيات المصممة خصيصاً لإعداد التقارير أو تجميع البيانات. لا يوجد تمثيل البيانات في مخططات بشكل افتراضي في النظام، ويمكن الحصول على هذه الخاصية من خلال تثبيت عنصر مكمل إضافي.

Ushahidi

تم إعداد برنامج Ushahidi لمطابقة تقارير العنف في كينيا أثناء وبعد أعمال العنف التي أعقبت الانتخابات في عام 2008. يمكن إرسال التقارير عبر عدد من البرامج بما في ذلك شبكة الإنترنت أو البريد الإلكتروني أو الرسائل النصية أو وسائل التواصل الاجتماعي مثل تويتر. وبعد تلقي هذه التقارير يمكن مراجعتها من قبل المشرف من أجل التحقق من المحتوى والموافقة عليه بحيث يمكن أن تظهر في خريطة صفحته الرئيسية.

Ushahidi برنامج مجاني ومفتوح لجمع المعلومات والتصوّر ورسم الخرائط التفاعلية ويمكن تخصيص نموذج التقرير بحيث تتمكن المنظمة من جمع المعلومات المهمة بالنسبة لها، وبمجرد التحقق من صحة التقارير يصبح من الممكن رؤيتها ظاهرة في خريطة مجمعة حسب فئة الحوادث المحددة مسبقاً. يمكن برمجة المنصة لتنبيه مدراء الأمن في حال الإبلاغ عن حادث جديد حتى يتمكنوا من تقديم الدعم للضحايا والتحقق من صحة التقرير. ويمكن لبرنامج Ushahidi أيضاً تنبيه المستخدمين الآخرين بمجرد التحقق من صحة التقرير.

المزايا	القيود
الميزة الرئيسية لبرنامج Ushahidi هو أنه يمكن تحميله من شبكة الإنترنت مجاناً وأن تثبيت النظام ليست معقداً حيث أن المنظمة تقرر مكان تثبيت البرنامج وتبقى البيانات تحت سيطرة المنظمة.	العيب الرئيسي في Ushahidi هو أن التمثيل الإحصائي للمعلومات الواردة في قاعدة البيانات غير مدمج في النظام، وينبغي الجمع بين الحلول الخارجية لهذا الغرض. وهو حل ممتاز لجمع البيانات ولكن هناك حاجة إلى موارد أخرى لتحليل البيانات، لم تعد منصة Ushahidi تخضع للتطوير بعد الآن، الأمر الذي يمكن أن يتسبب في مشكلات مع التقنيات الأخرى ذات الصلة التي تستمر في التطور. ويمكن حل هذه المشكلات المحتملة من قبل موظفي تقنية المعلومات.

SIMSON

صُمم نظام SIMSON خصيصاً للمنظمات غير الحكومية من قبل مركز السلامة والتنمية (CSD). SIMSON نظام للإبلاغ عن الحوادث الأمنية عبر الإنترنت يمكّن المستخدمين من رؤية الحوادث المُبلّغ عنها ممثلة على خريطة. لا تحتاج المنظمات غير الحكومية التي تستخدم SIMSON إلى تثبيت البرنامج أو كتابة رموز أي برنامج. كما يوفر مركز السلامة والتنمية (CSD) الدعم لتشغيل البرنامج وإدارة النسخ الاحتياطية. يمكن ترتيب الحوادث حسب الفئات والتنظيم والموقع والإطار الزمني وغيرها من المعلومات ذات الصلة بالأمن والمؤشرات. يتلقى المستخدمون تنبيهات عبر البريد الإلكتروني حول تقارير الحوادث الجديدة تبعاً لمناصبهم في المنظمة وحقوقهم في الوصول إليها. يمكن تحليل الحوادث في SIMSON باستخدام الرسوم البيانية والجدول. كما يمكن تحليل الحوادث في SIMSON باستخدام الرسوم البيانية والجدول ويمكن أيضاً تحميل بيانات الحوادث في ملف إكسيل. ويمكن رفع الوثائق وتقارير الحوادث ومشاركتها حسب ما ترتأى المنظمة مع أصحاب المصلحة الآخرين مثل شركات التأمين أو غيرها من المنظمات غير الحكومية. هناك إجراء خاص "بالحوادث الحساسة" يقتضي إبلاغ الموظفين المعيّنين فقط في المنظمة. ويكون هذا الإجراء ذو صلة عند التعامل مع حوادث الاعتداء الجنسي على سبيل المثال.

لمعرفة المزيد، يمكن تحميل نظرة عامة عن SIMSON من الموقع الإلكتروني لمركز السلامة والتنمية (CSD) على هذا الرابط.

المزايا	القيود
النظام جاهز للاستخدام، وهو موجه للمنظمات غير الحكومية ويدعمه مركز السلامة والتنمية (CSD)، ولذلك فإن المنظمات لا تحتاج إلى استثمار الموارد في تطويره وصيانته وحفظ النسخ الاحتياطية. يمكن تحليل بيانات الحوادث في نظام SIMSON أو عن طريق ترحيل البيانات إلى ملف إكسيل.	وعلى الرغم من أن مركز السلامة والتنمية (DSC) يضمن للمنظمات التي تستخدم النظام بأنها ستكون الوحيدة القادرة على رؤية تقارير الحوادث الخاصة بها إذا رغبت في ذلك، غير أن المنظمات قد ترغب في التحكم في بياناتها المتعلقة بالأمن والحوادث وقد تتردد في تفويض هذه المسؤولية إلى أطراف ثالثة. وقد لا يكون تصميم نموذج الإبلاغ خصيصاً للاحتياجات المحددة للمنظمة أمراً سهلاً.

المنظمة الدولية للرؤية العالمية (WVI) وشركة NAVEX Global

أنشأت المنظمة الدولية للرؤية العالمية (WVI) بالشراكة مع شركة NAVEX Global، مزود خدمات الإبلاغ عن المخاطر العالمية الدولية نظاماً إلكترونياً للإبلاغ عن الحوادث والمظالم والتحرش وغيرها. ويتجاوز هذا النظام مجرد التواصل بشأن الحوادث الأمنية ويشمل عناصر أخرى من نهج إدارة المخاطر مثل الفساد والدعاوى القضائية والسمعة وما إلى ذلك ويأتي بعدة لغات. تقوم NAVEX Global بتكييف نظام التقارير مع احتياجات وخصائص المنظمة التي تستخدمه. ويسمح نظام الإبلاغ عن الحوادث بإدخال مجموعة متنوعة من المصادر ويمكن لجميع موظفي المنظمة الدولية للرؤية العالمية أن يقدموا تقاريرهم مباشرة في المنصة لأنها تعمل أيضاً بمثابة نظام للإبلاغ عن المخالفات.

ولمعرفة المزيد عن نظام الإبلاغ عن الحوادث في المنظمة الدولية للرؤية العالمية، انظر الوثيقة التالية.

المزايا	القيود
إن الجمع بين نموذج الإبلاغ عن الحوادث وقناة الإبلاغ عن المخالفات وآلية تقديم الشكاوى الخاصة بالمستفيدين وما إلى ذلك يؤدي إلى تقليل التنوع المحتمل للنظم المستخدمة لأغراض مماثلة. ويساعد الدعم المقدم من شركة مختصة في الأخلاقيات وامثال الإدارة في وضع بيانات الإبلاغ عن الحادث في منظورها مع مجالات إدارة المخاطر الأخرى.	قد يكون النموذج مفصلاً نسبياً بالرغم من مزاياه الكثيرة، الأمر الذي قد يثني الموظفين عن الإبلاغ لطول العملية، وهو من الحلول التي لا يمكن إلا للمنظمات الكبيرة تحمل تكاليفه.

IRIS

تعتمد منصة IRIS على برنامج Ushahidi، وهي منصة يمكن استخدامها للإبلاغ عن الحوادث من خلال شبكة الإنترنت وتصور أماكن وقوع تلك الحوادث على الخريطة. ومن الممكن تخصيص نموذج الإبلاغ عن الحادث لتلبية احتياجات المنظمة باستخدام هذا النظام.

ويمكن استخدام المنصة "كبرنامج" أو "خدمة"، فضلاً عن إمكانية تثبيته في خوادم المنظمة مما يتيح السيطرة الكاملة على البيانات المُبلّغ عنها، ولا يمكن إلاً للمستخدمين المسجلين فقط الوصول إلى الواجهة، ويمكن تحديد امتيازات مختلفة حسب نوع المستخدم. ويمكن تقديم التقارير من خلال واجهة على شبكة الإنترنت أو من خلال اتصال ذو نطاق ترددي منخفض.

البرنامج متعدد اللغات ويمكن تصنيف التقارير بشكل افتراضي أو حسب الحقوق المخصصة. ويمكن تنبيه المديرين والمستخدمين الآخرين عند الإبلاغ عن الحوادث الجديدة بحيث يتم تقديم الدعم الفوري للضحايا مع إبلاغ بقية الفريق لاتخاذ الإجراءات المناسبة.

يمكن استخراج البيانات من المنصة وإدخالها في برامج تصور البيانات بحيث يمكن استخدام الإحصاءات المتعلقة بالحوادث لاستخلاص الدروس المستفادة وتقديم التوصيات والإحاطة الأمنية واستخدام المعلومات الأساسية المتعلقة بتحليل المخاطر وما إلى ذلك.

المزايا	القيود
يتميز هذا البرنامج بسهولة تثبيته واستخدامه، وإمكانية تخصيصه العالية إضافة إلى الطريقة التي يتم بها جمع المعلومات. يعتمد IRIS على الإصدار الثاني من Ushahidi الذي يمكن تطويره لاستيعاب احتياجات الإبلاغ الخاصة بالمنظمات التي تستخدمه لتواكب التطورات والتقنيات الجديدة وجعلها متوافقة مع النظم الأخرى الموجودة. عدد مستخدمي البرنامج غير محدود وهو يعمل دون رخصة، وبالتالي فإن المنظمات لا تدفع إلاً مقابل التثبيت والتخصيص. يمكن نقل البيانات القائمة حول الحوادث إلى البرنامج مجرد تثبيته.	يجب أن يتم تطوير الرابط بين قائمة المستخدمين والدليل النشط للمنظمة ولكن يمكن إنشاء المستخدمين الواحد تلو الآخر ويمكن الوصول إلى المعلومات المتاحة خلال العملية. تم تصميم البرنامج الأصلي لتبادل المعلومات المُبلّغ عنها على نطاق واسع. على الرغم من إمكانية إنشاء حساب مستخدم "للشخص المُبلّغ فقط"، إلاً أنه يجب التخطيط بعناية للحد من الوصول إلى المعلومات.

RIMS

توفر خدمة إدارة الحوادث من جمعية إدارة المخاطرة (RIMS) نظاماً بسيطاً وسهل الاستخدام يستخدم بشكل أساسي وصف الحادث على أساس الاختبار. يسمح البرنامج لفئات مصممة خصيصاً بترميز مختلف جوانب الحوادث، فمن الممكن إعداد الرسوم البيانية. هذه المنصة متاحة باللغة الإنجليزية فقط.

في المثال الذي تم عرضه، تم استخدام النظام بشكل رئيسي من قبل قسم الموارد البشرية حول التأمينات. وكان استخدام نظام تحليل الحوادث الأمنية محدوداً. ولذلك، لم يكن من الممكن الحكم على مدى فعالية هذا النظام إذا ما تم إنشاؤه بشكل كامل لخدمة احتياجات إدارة معلومات الحوادث الأمنية بما يتجاوز وصف الحوادث القائم على الاختبار، ولا سيما التحليل.

المزايا	القيود
هذا النظام سهل الاستخدام. ويمكن للموظفين استخدامه للإبلاغ عن الحوادث دون الكثير من التدريب. فمن السهل إعداد حقول مخصصة والتصفح في الموقع بسلاسة. هو من الأنظمة السهلة التي يمكن الوصول إليها بسرعة لتخزين الأوصاف الأمنية للحوادث.	اعتمد المثال المعروض بشكل أساسي على وصف الحوادث القائم على النصوص. لا يرسل النظام التنبيهات لمستخدميه.

الأداة 12: تحليل ومقارنة اتجاهات البيانات



التوجيه عند مقارنة بيانات اتجاهات المنظمة مع بيانات أوسع نطاقاً عن الحوادث الأمنية.

الأسئلة والاعتبارات الرئيسية

- ما هي أوجه الشبه والاختلاف في الاتجاهات بين منظمكم وتلك التي تظهر في البيانات المجمعة؟
- لماذا هناك أوجه الشبه والاختلاف؟ انظر في كل جانب من الجوانب التي تمت ملاحظاتها بشكل منفصل واطرح الأسئلة التالية:
- لماذا أرى أوجه شبه أو اختلاف في هذه الفئة الفرعية من أنواع الحوادث؟
- هل هذا بسبب البيئة الخارجية العامة؟
- كيف تتأثر هذه الاتجاهات بالبلدان التي تعمل فيها منظمكم أو البرامج التي تنفذها منظمكم؟
- هل يمكن أن تكون أي من هذه الاختلافات نتيجة لممارسات الإبلاغ (الخاصة بك أو تلك الخاصة بالمنظمات الأخرى)؟
- ما هو نوع الحوادث الذي يوجد بكثرة في منظمكم؟
- ما هو نوع الحوادث الذي لا يوجد بكثرة في منظمكم؟
- ابحث عن أوجه الشبه في الاتجاهات وحاول إعطاء تفسير لأوجه الشبه هذه.
- انظر إلى الاختلافات. حاول اقتراح توضيح لها.
- تأكد من توخي الدقة. إذا كنت متأكداً من صحة أمر ما، أذكر ذلك. أما إذا كنت تعتقد أن ذلك الأمر صحيح ولكنك لا تملك دليلاً عنه، قم باستخدام اللغة/المفردات التي تشير إلى هذا، مثل "تشير البيانات"، أو "يبدو من المعلومات المتاحة".
- قم بتحديد الاتجاهات الرئيسية:
- ما هي الاتجاهات الرئيسية التي يمكن رصدها؟
- هل تشير البيانات إلى أي اتجاهات ناشئة يجب على المنظمات أن تأخذها في الاعتبار؟
- قم بوصف الاتجاهات بدقة قدر الإمكان.
- هل هذه الاتجاهات عالمية؟
- هل هناك اتجاهات في بلد معين؟
- ما هي فئة الأحداث الأمنية التي تشير إليها هذه الاتجاهات؟
- كن دقيقاً قدر الإمكان من خلال تسمية أنواع الحوادث التي ترى زيادة فيها، وأين يمكن أن تحدث. وإذا كان بإمكانك، قم بتقديم تفاصيل عن الأشخاص أو الأشياء التي يمكن تتأثر بشكل خاص من هذه الحوادث.

- فكّر في الاتجاهات العامة لسياق المعونة العامة كما هو مبين في تحليل الاتجاهات أو على النحو الظاهر في البيانات سواء على المستوى العالمي أو القطري. حاول وصف السياق العام لتقديم المعونة والتغييرات الحديثة والتهديدات أو الاتجاهات الناشئة.
- فكّر في الاختلافات في الاتجاهات بين بيانات منظمتك وبيانات الوكالات الأخرى (باستثناء تلك الناتجة عن الاختلافات في التقارير). انظر في البلدان التي تعمل فيها منظمتك، ما هي البرامج التي تقدمها منظمتك؟ وما هي نقاط الضعف أو نقاط القوة في إطار إدارة المخاطر الأمنية في منظمتك؟
- إذا كنت تقوم بذلك للمرة الثانية أو الثالثة، فكّر في الاختلافات بين أحدث البيانات والتحليلات السابقة. وصف التغييرات واقتراح تفسيرات.
- قم بتحديد الإجراءات الواجب اتخاذها:
- هل طرأت أية أسئلة من النظر إلى البيانات والتي يمكنك متابعتها؟
- من يمكنه مساعدتك في معرفة المزيد؟
- تواصل مع مزود خدمات الاتصالات / المكتب القطري / الإقليمي واطرح عليهم أسئلة للحصول على معلومات واقعية حول اتجاهات البيانات.
- فكّر فيما ستضعه في خطة العمل التي ستنفذها على مدى الأسابيع / الأشهر القادمة.

إعداد خطة العمل

- هل تشير البيانات إلى أن منسق شؤون الأمن عليه اتخاذ تدابير محددة؟
- هل تشير البيانات إلى أنه ينبغي إضافة المخاطر الناشئة الجديدة أو الحالات التي تم تصعيدها إلى النماذج التي سيتم التباحث فيها مع الموظفين؟
- هل تشير البيانات إلى أنه ينبغي التركيز بشكل خاص على نوع معين من الأحداث أثناء التدريب في سياق معين؟
- هل تسلط البيانات الضوء على مخاطر محددة ينبغي مناقشتها بمزيد من التفصيل مع منسقي شؤون الأمن القطريين والإقليميين لمعرفة ما إذا كانت هناك حاجة إلى أي تغييرات في السياسة؟
- هل تسلط البيانات الضوء على القضايا التي ينبغي رفعها إلى مستويات أعلى داخل المنظمة؟
- هل يشير تحليلك للبيانات أن منظمتك بحاجة إلى تحسينات في إدارة معلومات الحوادث الأمنية على مستوى ما داخل المنظمة؟

القضايا المحتملة التي يتعين إبلاغ الزملاء عنها سواء في الميدان أو على مستوى الإدارة العليا / مجلس الإدارة

- اذكر الاتجاهات المحددة التي يجب مراقبتها عن كثب واقتراح أن يتم وضعها على جدول أعمال المراجعة العادية.
- سلط الضوء على مخاطر معينة ومحددة واقتراح مناقشة داخلية حول الحد المقبول لمخاطر أنواع معينة من الأحداث في سياق معين، وذلك للمساعدة في صياغة سياسة واضحة.
- اقترح أنشطة محددة لإدارة المعلومات الحوادث الأمنية المحسنة والتي ستعزز قدرة المنظمة على تحديد الاتجاهات وطلب المضي قدماً لتنفيذ عناصر محددة (انظر شبكة التقييم للاطلاع على العناصر المحددة التي يمكن تحسينها).

الإبلاغ عن استنتاجاتك النهائية وخطة العمل

- قم بإعداد وثيقة موجزة وواضحة مع:
- ذكر المصادر والطرق المستخدمة.
- الإشارة إلى أنك أخذت في الاعتبار البيانات وأن لديك ثقة في النتائج التي توصلت إليها (يمكنك أن تذكر أنك تعمّدت عدم النظر في جانب معين لأنك تعتقد أن القيام بذلك سيكون نتيجة للتحيّز في التقارير).
- إعداد قائمة واضحة للاتجاهات التي تظن أنها مصدر قلق. واختيار ثلاثة كحد أقصى. إذا كانت هذه ممارسة منتظمة، قم بإدراج الاتجاهات الرئيسية من التحاليل السابقة.
- إدراج الإجراءات التي توصي بها:
- لنفسك من خلال تحديد ما كنت تقوم به وهي في عملية القيام أو ما سوف تقوم به. القيام خلال الأشهر المقبلة بتلبية الاحتياجات المحددة:
- للزملاء الآخرين (على مستوى الميدان أو المستوى الأعلى). ضع مهمة واحدة للآخرين من خلال اقتراح ما يمكنهم القيام به لتسهيل العملية والمساهمة التي ستحتاج إليها منهم.

قم بمقارنة البيانات مع البيانات المجمعة من *Insecurity Insight* خلال *Aid in Danger Security in Numbers Database* وذلك باستخدام تحليل الاتجاهات المنشور أو عبر الاطلاع على تبادل البيانات الإنسانية، بالإضافة إلى بيانات الحوادث الأمنية الخاصة بك.

يمكنك الاطلاع هنا عن مثال عن تقرير تحليل مشترك بين الوكالات لبيانات الاتجاهات.

الأداة 13: الأسئلة الاستراتيجية المتعلقة باتخاذ قرارات إدارة معلومات الحوادث



بعد النظر بشكل جيد في أنواع الحوادث الأمنية التي وقعت ومتى وقعت، قم بإلقاء نظرة على البيانات وفكر ما إذا كانت تلك البيانات تشير إلى الحاجة لإجراءات متابعة. يمكنك طلب معلومات إضافية وإنهاء تقرير الحادث الأمني مع توصيات محددة.

يمكن لقائمة الأسئلة التالية أن تساعد منسقي شؤون الأمن أثناء وضع الاستنتاجات والتوصيات الإضافية على المستوى الاستراتيجي من أجل اتخاذ إجراءات في أعقاب تحليل جيد لأحداث أمنية حدثت في السابق.

أسئلة ينبغي التفكير فيها عند النظر في تحليل بيانات الحادث الأمني	إجراءات المتابعة الممكنة	التوصيات المحتملة للإجراءات التي يتعين إضافتها في نهاية تقرير التحليل
1 - ما هو أنواع الحوادث الأمنية التي شهدتها الموظفون والمنظمة؟ 2 - ما هي البلدان التي وقعت فيها هذه الحوادث؟		
هل تقوم منظمتنا بإعداد الموظفين بشكل كاف لنوع الأحداث المحتمل أن يتعرضوا لها؟	حاول معرفة إلى أي مدى يتم إعداد الموظفين بشكل كاف لمواجهة أنواع الأحداث التي يتم التعرض لها. حاول معرفة تكلفة الدورات ذات الصلة وأصف الميزانية المقدرة.	تتمثل التوصية في اقتراح الحاجة إلى دورات تدريبية ودورات توعية للموظفين العاملين في السياقات المتأثرة بأنواع محددة من الحوادث.
هل يغطي التأمين الاستجابات المطلوبة للموظفين أو الاستجابات اللازمة للتعامل مع الأضرار المادية؟	اعرف من الموظفين إذا ما حصلوا على الاستشارة المهنية بعد الحادث أو إذا ما رغبوا في الحصول عليها. اعرف إذا ما كان التأمين يغطي مثل هذه الاستشارات. اعرف إذا كان استبدال المواد المفقودة أمراً سهلاً أو مكلفاً (التأمين أو غيرها).	تتمثل التوصية في اقتراح النظر في فجوات تغطية التأمين. اقتراح استراتيجية للتعامل مع الخسائر المادية في السياقات القطرية التي يبدو أن هذا الأمر يشكل فيها خطراً متزايداً.

أسئلة ينبغي التفكير فيها عند النظر في تحليل بيانات الحادث الأمني	إجراءات المتابعة الممكنة	التوصيات المحتملة للإجراءات التي يتعين إضافتها في نهاية تقرير التحليل
3 - بصفتك منسق شؤون الأمن في المقر الرئيسي، ما مدى رضاك عن طريقة استخدام المكاتب القطرية للحوادث الأمنية والحوادث الوشيكة للتعلم من الأخطاء وتحسين الممارسات؟ 4 - ما هي الحوادث الأمنية التي تواجهها المنظمات الأخرى في نفس البلد وكيف يمكن مقارنة ذلك مع الحوادث المبلغ عنها داخل منظمتك؟		
هل هناك مكاتب قطرية لا تقدم تقارير منتظمة للمقر الرئيسي؟	قم بإجراء محادثة مع الموظفين الرئيسيين لمعرفة لماذا تم الإبلاغ عن عدد قليل من الحوادث أو لماذا لم يتم الإبلاغ عنها بتاتا.	مراجعة تعليمات حول كيفية وتوقيت الإبلاغ. تغيير نظام التقارير بطريقة تشجع على الإبلاغ المنتظم.
هل هناك مكاتب قطرية تعاني من أنواع معينة من الحوادث؟ كيف تقارن هذه الحوادث مع تلك التي تعاني منها منظمات أخرى؟	قم بإجراء محادثة مع الموظفين الرئيسيين لمعرفة سبب وقوع حوادث معينة بشكل متكرر أو عدم حدوثها مطلقاً.	دعم أفضل من الإدارة العليا للإشارة إلى فوائد التقارير المنهجية.
5 - كيف أثرت الحوادث الأمنية على إيصال المعونة؟ 6 - هل يمكننا أن نضيف تكاليف أثر الحوادث الأمنية على تكاليف إيصال المعونة؟		
هل أبلغ زملائك عن مدى تسبب الحوادث في تعطيل عملك؟	قم بإجراء محادثات مع الزملاء بشأن أفضل الطرق الممكنة لوصف أثر الحوادث الأمنية على إيصال المعونة.	إضافة معلومات عن كيفية تأثير الحوادث الأمنية على إيصال المعونة.
هل قام زملاؤك بحساب تكلفة الخسارة من حيث وقت الموظفين ومن حيث الخسائر المادية؟	قم بإجراء محادثات مع الموظفين حول أفضل الطرق لحساب تكلفة الخسارة في وقت الموظفين والسلع المادية.	إضافة معلومات حول تكاليف الحوادث الأمنية إلى العمليات.
هل أبلغ زملائك عن مدى تأثير الحادث الأمني على إمكانية الوصول؟	قم بإجراء محادثات مع الموظفين لوصف تأثير الأمن على الوصول إلى المستفيدين، وكيف أن المخاوف الأمنية تعيق الوصول إلى عدد كبير من الأشخاص.	إضافة معلومات عن كيفية تأثير الحوادث الأمنية على إمكانية الوصول إلى السكان المستفيدين.
7 - ما هي السياقات الرئيسية للحوادث الأمنية؟ 8 - هل يمكن تصنيف سياق الحوادث حسب استراتيجية الاستجابة التي قد تكون ضرورية؟		
كم عدد الحوادث قد حدثت بسبب الفشل في وضع استراتيجية قبول جيدة؟	قم بإجراء المحادثات داخل المنظمة حول أفضل استراتيجيات القبول وكيفية تنفيذها بفعالية.	تسمية المنطقة أو السكان المستهدفين الذين يحتاجون إلى استراتيجية أفضل للقبول.
في أي الجهات تمت ملاحظة فشل القبول؟ الجهات الفاعلة غير الحكومية، السلطات، المستفيدين، الموظفين، المتعاقدين أو غيرهم؟	اقترح دورات تدريبية محسنة في استراتيجية القبول للموظفين المبعوثين إلى بلد معين وذلك للتعامل مع جهات معينة.	

أسئلة ينبغي التفكير فيها عند النظر في تحليل بيانات الحادث الأمني	إجراءات المتابعة الممكنة	التوصيات المحتملة للإجراءات التي يتعين إضافتها في نهاية تقرير التحليل
7 - ما هي السياقات الرئيسية للحوادث الأمنية؟ 8 - هل يمكن تصنيف سياق الحوادث حسب استراتيجية الاستجابة التي قد تكون ضرورية؟		
كم عدد الحوادث التي حدثت بسبب عدم احترام الموظفين للقواعد أو اللوائح أو بسبب السلوك غير المسؤول؟	قم بإجراء المحادثات داخل المنظمة حول أفضل طريقة لتعزيز مدونة قواعد سلوك الموظفين وضمان التقيد بالإجراءات الأمنية.	طلب إعداد قائمة الجوانب السلوكية التي قد تدرج في مدونة قواعد السلوك والتي يتعين على الموظفين مراعاتها.
كم عدد الحوادث التي قد تحدث بسبب العوامل الشخصية التي تتعلق بأصل أو خلفية أو عرق الموظفين؟	قم بإجراء المحادثات داخل المنظمة حول كيفية معالجة عوامل الخطر ذات الصلة بالحياة المنزلية أو الأصل العرقي أو غير ذلك من العوامل الخاصة.	تحديد مجالات السلوك التي لم يحترم فيها الموظفون القواعد واقتراح آلية لتحسين إنفاذها.
كم عدد الحوادث التي وقعت لأن الموظفين أو المنظمة كانوا في المكان الخطأ في الوقت الخطأ؟	قم بإجراء المحادثات داخل المنظمة لمعرفة إلى أي مدى تكون المنظمة على استعداد لقبول المخاطر العامة المتصلة بالإرهاب أو الجريمة أو غيرها من الحوادث التي لا تستهدف المنظمة على وجه التحديد.	وضع قائمة تشمل السياقات والبلدان التي قد تكون بحاجة إلى سياسات وإجراءات محددة والتي قد تشمل ما يلي: • كيفية الاستجابة إذا كان موظف عرضة للعنف المنزلي. • كيفية الاستجابة عندما يكون هناك خطر متعلق بالتمييز العرقي أو العنف. • ما هي مدونة قواعد السلوك الأخلاقية التي يمكن توقعها من الموظفين المحليين في حال تأثير المصالح التجارية أو سياسة الأسرة الممتدة على الموظفين.
كم عدد الحوادث التي وقعت نتيجة لعمل الجهات الحكومية؟	قم بتحديد الجهات الفاعلة الحكومية المسؤولة في الوثائق الداخلية وحاول تحديد السبل الممكنة لإجراء الحوار مع هذه الجهات الفاعلة.	اقتراح السبل الممكنة لمتابعة المحادثات من قبل الممثلين القطريين أو الإدارة العليا باستخدام القنوات الدبلوماسية أو دعم الوكالات الأخرى (مثل اللجنة الدولية للصليب الأحمر).
كم عدد الحوادث التي وقعت نتيجة لعمل الجهات الحكومية؟	قم بتحديد الجهات الفاعلة الحكومية المسؤولة في الوثائق الداخلية وحاول تحديد السبل الممكنة لإجراء الحوار مع هذه الجهات الفاعلة.	تحديد المجالات التي يمكن أن تنظر المنظمة فيها لأغراض إطلاق حملة الدعوة مع الآخرين، مثل قصص البنية التحتية أو الإفلات من الملاحقة القضائية.

أسئلة ينبغي التفكير فيها عند النظر في تحليل بيانات الحادث الأمني	إجراءات المتابعة الممكنة	التوصيات المحتملة للإجراءات التي يتعين إضافتها في نهاية تقرير التحليل
9 - هل يمكننا استخدام البيانات لتحديد عتبة الخطر التي ستكون منظمنا على استعداد لتقبلها؟		
ما هو نوع القرارات التي تم اتخاذها خلال فترة قيد التحليل، والتي تشكل مؤشراً لعتبة الخطر التي ستكون المنظمة على استعداد لاتخاذها؟	عليك التفكير بشكل نقدي فيما يخص اتخاذ القرارات الخاصة بك، وفيما يتعلق بالمخاطر الأمنية. ما هي المبادئ والعتبات التي تستند إليها؟	التوصية بوضع عتبة محددة بوضوح حول المخاطر التي ينبغي إبلاغ الموظفين عنها.
ما مدى اتساق عملية اتخاذ القرار بين مختلف السياقات؟	قم بإجراء المحادثات مع الموظفين الآخرين في المنظمة، وانظر إذا كان يمكنك استخدام نفس المبادئ والعتبات.	
هل هناك علاقة بين الحوادث الأمنية المبلغ عنها والقرارات المحددة التي تم اتخاذها؟		

قائمة المراجع

- ATHA. (2016). "مشروع سياسة: حماية العمل الإنساني". ATHA. متاح عبر:
<http://www.atha.se/policy-project-protection-of-aid-workers>
- آير، آر. (2010). "تحدي إدارة المعلومات: إحاطة عن أمن المعلومات للمنظمات غير الحكومية الإنسانية في الميدان".
 منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2014/09/0119-Ayre-EISF-2010-The-Information-Management-Challenge-A-Briefing-on-Information-Security-for-Humanitarian-Non-Governmental-Organisations-in-the-Field.pdf>
- بيكلي، إس. (2017). "إدارة المخاطر الأمنية: دليل أساسي للمنظمات غير الحكومية الصغيرة".
 منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/>
- بوث، بي. (2010). "إدارة الأزمات في الحوادث الحساسة". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2014/09/0121-Buth-2010-Crisis-Management-of-Critical-incident-2010.pdf>
- دافيدسون، إس. (2013). "إدارة الرسالة: إدارة الاتصالات ووسائل الإعلام في الأزمات الأمنية".
 منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2014/09/1140-Davidson-2013-Managing-the-Message-Communication-and-media-management-in-a-security-crisis.pdf>
- دايفس، جاي وآخرون (2017). "الأمن: مجموعة أدوات لإدارة الأمن لوكالات المعونة الإنسانية".
 النسخة الثانية. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
https://www.eisf.eu/wp-content/uploads/2017/03/2124-EISF-2017-Security-to-go_a-risk-management-toolkit-for-humanitarian-aid-agencies-2nd-edition.pdf
- دي بالاسيوس، جي (2017، مقبل). إدارة المعلومات المتعلقة بالأمن: نظرة فاحصة على نظم الإبلاغ عن الحوادث". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)
- ديك، آي. (2010). "إنشاء مصطلحات أمنية مشتركة للمنظمات غير الحكومية: دراسة مقارنة".
 مبادرة إدارة الأمن. متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2014/09/0647-Dick-2010-Creating-Common-NGO-Security-Terminology-A-Comparative-Study.pdf>

إيرث بوينت (Earth Point). "من إيكسيل إلى KML - عرض ملفات إكسيل على Google Earth". إيرث بوينت. متاح عبر:

<https://www.earthpoint.us/ExcelToKml.aspx>

هولشر، كاي، ميكليان، جاي، وإتش إم نيغارد. (2015). "فهم الهجمات على موظفي المساعدات الإنسانية". المعهد الدولي لبحوث السلام في أوسلو. اتجاهات النزاع. متاح عبر: http://file.prio.no/publication_files/prio/Hoelscher,%20Miklian,%20Nyg%C3%A5rd%20-%20Understanding%20Attacks%20on%20Humanitarian%20Aid%20Workers,%20Conflict%20Trends%206-2015.pdf

اللجنة الدولية للصليب الأحمر. (2011). دراسة حالة في 16 دولة: مشروع health care in danger. اللجنة الدولية للصليب الأحمر. متاح عبر: https://www.icrc.org/eng/assets/files/reports/report-hcid-16-country-study-2011-08-10.pdf?_hstc=163349155.76b9edd98545ef10cf2630f8704dd68b.1500037719517.1500037719517.1500838137193.2&_hssc=163349155.2.1500838137193&_hsfp=520750989

InterAction. (2010). دليل InterAction. لمعالجة الاستغلال والانتهاك الجنسيين. InterAction. متاح عبر: <https://www.interaction.org/sites/default/files/2010.6%20-%20Step%20by%20Step%20Guide%20-%20Comments%20Version.pdf>

اللجنة الدائمة المشتركة بين الوكالات (IASC). (2008). التوجيه التشغيلي حول مسؤوليات قادة القطاع/المجموعة ومكتب تنسيق الشؤون الإنسانية (OCHA). منظمة الصحة العالمية. متاح عبر: http://www.who.int/hac/network/global_health_cluster/iasc_operational_guidance_on_information_management_v3.pdf

اللجنة الدائمة المشتركة بين الوكالات (IASC). (2015). "إنقاذ الأرواح معاً - إطار عمل لتحسين الترتيبات الأمنية بين المنظمات الحكومية الدولية والمنظمات غير الحكومية والأمم المتحدة في الميدان. (أكتوبر 2015)". اللجنة الدائمة المشتركة بين الوكالات. متاح عبر: <https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0>

اللجنة الدائمة المشتركة بين الوكالات (IASC). (2015). "مبادئ توجيهية لإدماج التدخلات المتعلقة بالعنف القائم على نوع الجنس في العمل الإنساني: الحد من المخاطر، وتعزيز القدرة على التكيف والمساعدة على التعافي". متاح عبر: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/femm/dv/gbv_toolkit_book_01_20_2015/gbv_toolkit_book_01_20_2015_en.pdf

اللجنة الدائمة المشتركة بين الوكالات (IASC). (2016). "الحماية من الاستغلال والانتهاك الجنسيين (PSEA) التعاون بين الوكالات فيما يخص آليات الشكاوى القائمة على المجتمع: إجراءات التشغيل الموحدة العالمية. اللجنة الدائمة المشتركة بين الوكالات. متاح عبر: <http://reliefweb.int/report/world/protection-sexual-exploitation-and-abuse-psea-inter-agency-cooperation-community-based>

المنظمة الدولية لتوحيد المقاييس (أيزو). (2009). ISO 31000:2009: إدارة المخاطر - المبادئ والتوجيهات

المنظمة الدولية لتوحيد المقاييس (أيزو). (2014) ISO/IEC 27000:2014: تقنية المعلومات - تقنيات الأمن - أنظمة إدارة أمن المعلومات - لمحة عامة ومفردات

Irish aid (2013). المبادئ التوجيهية لـ Irish aid فيما يخص إدارة مخاطر الأمن والسلامة المهنية في المنظمات غير الحكومية. ALNAP. متاح عبر: <http://www.alnap.org/resource/11229>

كيمب، إيه وميركالباخ، إم (2011)، هل يمكنك التعرض للمقاضاة؟ المسؤولية القانونية لمنظمات المعونة الإنسانية الدولية تجاه موظفيها. مبادرة إدارة الأمن. متاح عبر: <https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/>

كيمب، إيه وميركالباخ، إم (2016): واجب الرعاية: مراجعة أحكام قضية دينيس ضد مجلس اللاجئين النرويجي وأثارها. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر: <https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/>

ليبرمان، إيه (2017). "منظمة الصحة العالمية تستعد لإطلاق قاعدة بيانات عبر شبكة الإنترنت لمتابعة الهجمات ضد العاملين في الصحة". Devex. متاح عبر: <https://www.devex.com/news/who-readies-to-launch-online-database-tracking-health-worker-attacks-90331#.WWYjVPrtmqh.twitter>

مارتنسون، جاي. (2010). "دروس هامة من حملة الألغام الأرضية". البنك الدولي. متاح عبر: <https://blogs.worldbank.org/publicsphere/important-lessons-landmine-s-campaign%20>

ميركالباخ، إم. (2017). المبادئ التوجيهية الطوعية بشأن واجب الرعاية للموظفين المدنيين المعارين. وزارة الخارجية الاتحادية السويسرية، ووحدة تحقيق الاستقرار، ومركز عمليات السلام الدولية. متاح عبر: http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf

نويرت، إم (2016). الوقاية والسياسة وقائمة تدقيق الإجراءات: الاستجابة للعنف الجنسي في المجال الإنساني والإنمائي. Report the Abuse. متاح عبر:
<http://www.reporttheabuse.org/take-action/preventing-sexual-violence/>

نويرت، إم (2017). "لماذا ينبغي علينا معالجة العنف الجنسي في أماكن العمل الإنسانية؟". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/news/why-should-we-address-sexual-violence-in-humanitarian-workplaces/>

بارلوف، إيه. (1995). "نحو حظر عالمي للألغام الأرضية". المجلة الدولية للصليب الأحمر. متاح عبر:
<https://www.icrc.org/eng/resources/documents/article/other/57jmmj.htm>

بيرسود، سي. (2012). الجنسانية والأمن: مبادئ توجيهية لتعميم مراعاة المنظور الجنساني في إدارة المخاطر الأمنية. منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2014/09/1137-Persaud-2012-Gender-and-Security-Guidelines-for-Mainstreaming-Gender-in-Security-Risk-Management.pdf>

Red R UK ومنتدى الأمن الأوروبي المشترك بين الوكالات (EISF). (2016). تقرير: الإدماج وأمن موظفي المعونة من المثليات والمثليون ومزدوجو الميل الجنسي ومغايرو الهوية الجنسانية. Red R UK. متاح عبر:
<https://www.eisf.eu/wp-content/uploads/2016/08/2091-RedR-and-EISF-2016-REPORT-INCLUSION-AND-SECURITY-OF-LGBTI-AID-WORKERS-WORKSHOP-22-01-2016.pdf>

التحالف المعني بالصحة في حالات النزاع (Safeguarding Health in Conflict Coalition). (2017). "يجب للإفلات من العقاب أن ينتهي: هجمات على الصحة في ٣٢ بلداً من الصراع في 2016". متاح عبر:
<https://www.safeguardinghealth.org/sites/shcc/files/SHCC2017final.pdf>

Saving Lives Together. (2016). "مبادئ توجيهية لتنفيذ إطار عمل Saving Lives Together". يوليو 2016. متاح عبر:
<https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/>

شافير، جاي ومورفي، بي (2010). التعاون الأمني: دليل الممارسات الفضلى. وحدة الأمن لدى ItnerAction - ItnerAction. متاح عبر:
https://acceptanceresearch.files.wordpress.com/2010/10/interaction_security-collaboration-best-practices-guide-201111.pdf

الأمم المتحدة (2016). "مجلس الأمن الدولي يعتمد القرار 2286 (2016)، الذي يدين بشدة الهجمات على المرافق الطبية، والموظفين في حالات النزاع". الأمم المتحدة. متاح عبر: <https://fas.org/irp/doddir/army/fm2-22-3.pdf>

الجيش الأمريكي. (2006). الدليل الميداني رقم 2-22.3 لعمليات الذكاء البشري. متاح عبر: <https://www.un.org/press/en/2016/sc12347.doc.htm>

فان براينت، كاي. (2001). التقرير رقم 9 لفريق السياسات الإنسانية: تعميم الإدارة التنظيمية للأمن والسلامة "فريق السياسات الإنسانية / معهد التنمية الخارجية. متاح عبر: <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/297.pdf>

فان براينت، كاي (2010). "GPR8 - إدارة الأمن التشغيلي في البيئات العنيفة، النسخة المعدلة. شبكة الممارسات الإنسانية / معهد التنمية الخارجية. متاح عبر: http://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

وانبرو-جونز، إيه. وديكسون، إم. (2014). "إنقاذ الأرواح معاً": استعراض الممارسات القائمة في مجال التنسيق الأمني بين المنظمات غير الحكومية والأمم المتحدة في الميدان. مجموعة أدوات التنسيق. متاح عبر: <http://www.coordinationtoolkit.org/wp-content/uploads/Saving-Lives-Together-Review-of-NGO-and-UN-Security-Coordination-Practices.pdf>

منظمة الصحة العالمية. مؤسسة صدمات الحرب (World Vision International)، والمنظمة الدولية للرؤية العالمية (World Vision International). الإسعافات الأولية النفسية: دليل للعمال الميدانيين. منظمة الصحة العالمية. متاح عبر: http://www.who.int/mental_health/publications/guide_field_workers/en/

منظمة الصحة العالمية. (2017). الهجمات على الموقع الإلكتروني لـ Health Care. متاح عبر: <http://www.who.int/emergencies/attacks-on-health-care/en/>

ويل سي. (2016)، "دروس مستفادة من قطاع الطيران: ما الذي يمكننا تعلّمه في إدارة المخاطر الأمنية في القطاع الإنساني؟". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر: <https://www.eisf.eu/news/lessons-from-the-aviation-industry-what-can-we-learn-for-humanitarian-security-risk-management/>

ويليامسون، سي. (2017). "إدارة الأشخاص في الأمن: مجموعة أدوات الإدارة الموجهة لوكالات المعونة الإنسانية". منتدى الأمن الأوروبي المشترك بين الوكالات (EISF). متاح عبر: <https://www.eisf.eu/news/people-management-and-security-risk-management/>

معلومات إضافية

المنظمات

RedR UK منظمة غير حكومية إنسانية دولية تدعم الجهات الفاعلة الإنسانية عبر العالم من خلال توفير التدريب والدعم الفني. تأسست RedR عام 1980 كقائمة عضوية، وأصبحت مع مرور الوقت وكالة رائدة في بناء القدرات في هذا القطاع، حيث تصل خدماتها إلى عشرات آلاف الخبراء الإنسانيين ومئات المنظمات عبر العالم. لدى منظمنا تواجد دولي متمثل في مكاتبنا في المملكة المتحدة والسودان وكينيا والأردن. ونحن نقدم دوراتنا التدريبية للعاملين في القطاع الإنساني على الصعيد العالمي انطلاقاً من مراكزنا الإقليمية تلك.

تعتبر منظمة RedR UK من الوكالات الرائدة في تقديم التدريب ودعم بناء القدرات في القطاع الإنساني، حيث تدرب أكثر من 7000 عامل في القطاع في أكثر من 55 دولة كل عام. تمكنت UK RedR بفضل خبراتها الكبيرة التي اكتسبتها على مدى أكثر من 35 عاماً من العمل في دعم عشرات آلاف الموظفين والعاملين الإنسانيين من أن تصبح الرائدة في تعليم البالغين في هذا المجال. تنطوي خبراتنا على تقديم برامج بناء القدرات التي تشمل التدريب الشخصي، والتوجيه والإرشاد، وتمارين المحاكاة الميدانية، والنشر، والاستشارات قصيرة المدى، والتعليم الإلكتروني. كما أسهمنا أيضاً بالإضافة إلى برامجنا التعليمية عالية المستوى في فعالية توفير التعلم في القطاع. إن خبرة RedR UK في تقديم وإدارة برامج بناء القدرات الإنسانية المبتكرة تجعل منها الشريك الأمثل لإدارة مشروع "إدارة معلومات الحوادث الأمنية".

Insecurity Insight عبارة عن مجموعة من نخبة الخبراء المختصين في استخلاص وتحليل "البيانات حول الأشخاص في خطر" (data on people in danger)، والذين لديهم سجل إنجازات حافل في تطوير أحدث وأفضل أنظمة مراقبة الحوادث للمجتمع الإنساني. عملت Insecurity Insight منذ عام 2009 بالتعاون مع الوكالات الإنسانية من أجل تطوير آلية لمشاركة بيانات ومعلومات حوادث الوكالات وتحليلها بسريّة تامة.

European Interagency Security Forum (منتدى الأمن الأوروبي المشترك بين الوكالات) شبكة مستقلة لمنسقي شؤون الأمن تمثل حالياً 85 منظمة غير حكومية إنسانية مقرها أوروبا وتعمل على الصعيد الدولي. يلتزم هذا المنتدى بتحسين أمن عمليات الإغاثة وموظفيها. وهو يسعى إلى زيادة وصول الوكالات الإنسانية إلى الأشخاص المتضررين من حالات الطوارئ بشكل آمن. يتمثل محور عمله في إجراء الأبحاث وتطوير الأدوات التي تعزز الوعي والتأهب والممارسات الجيدة. يسهل المنتدى التبادل بين المنظمات الأعضاء والجهات الأخرى مثل الأمم المتحدة والمانحين والمؤسسات الأكاديمية والبحثية، والقطاع الخاص ومجموعة واسعة من المنظمات غير الحكومية الدولية. يسعى منتدى الأمن الأوروبي المشترك بين الوكالات ليصبح المرجع العالمي للممارسات التطبيقية والمعرفة الجماعية، ومن محاوره تطوير الأبحاث التطبيقية لإدارة المخاطر الأمنية في القطاع الإنساني.

جهات الاتصال

لمشاركة المصادر ومعرفة المزيد حول المشروع، يُرجى التواصل مع:

RedR UK

Marine Menier: marine.menier@redr.org.uk

Insecurity Insight

Christina Wille: christina.wille@insecurityinsight.org

EISF

Lisa Reilly: eisf-director@eisf.eu