



دليل إدارة المخاطر الأمنية: الاستراتيجيات



تعرّف على كيفية تخطيط استراتيجيات وأنظمة لإدارة المخاطر الأمنية في سياقات جديدة أو في حالات الاستجابة السريعة لحالات الطوارئ.

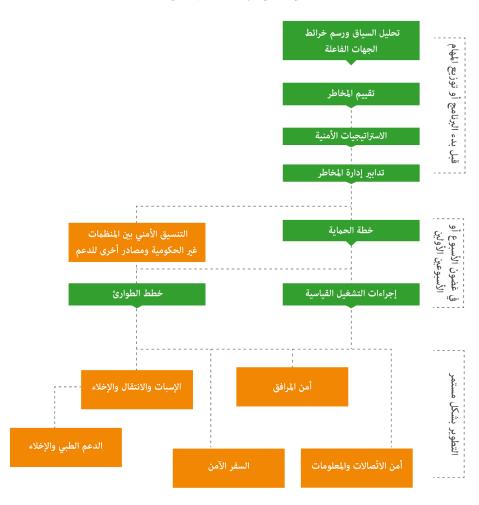


ملاحظة للمبتدئين

المعلومات الواردة في هذا الدليل هي للأغراض التعليمية فقط ولا يجب أن تعد بديلاً عن النصائح الأمنية المهنية أو المتخصصة. وبالتالي فإن التزامك بهذه المعلومات دون سواها يكون على مسؤوليتك الخاصة، ولن يتحمل المنتدى الأوروبي الأمنى المشترك بين الوكالات (EISF) مسؤولية ذلك تحت أى ظرف من الظروف.

عملية تخطيط إدارة المخاطر الأمنية

تخطيط إدارة المخاطر الأمنية أمر بغاية الأهمية في كل مرحلة من مراحل البرنامج. يجب أن يتم التخطيط للبرامج الجديدة قبل مرحلة توزيع الموظفين أو انطلاق البرامج، ويفضل أن يتم التخطيط خلال أول أسبوعين من البرنامج، وأن يتم مراجعة الخطة بانتظام للتكيف والتطوير بشكل مستمر.



عملية تخطيط إدارة المخاطر الأمنية

تحليل السياق ورسم خرائط الجهات الفاعلة

خذ الأسئلة التالية بعين الاعتبار أثناء تحليل السياق ورسم خرائط الجهات الفاعلة:

- ما هو السياق؟ من هي الجهات الفاعلة وما العلاقة بينهم؟
- ما هو تأثير منظمتك وبرامجك على السياق والجهات الفاعلة؟

تقييم المخاطر

أجب على هذه الأسئلة الرئيسية لتساعدك في تقييم المخاطر الأمنية:

- ما هي التهديدات التي تواجهها؟
- ما هي نقاط ضعف منظمتك وموظفيك تجاه هذه التهديدات؟ ما هي المخاطر التي يتعرض لها العاملون من خلفيات أقلويّة؟
 - ما هي احتمالية حدوث المخاطر ومدى تأثيرها؟

الاستراتيجيات الأمنية

- قم بإدراك نهجك التنظيمي إزاء القبول والحماية والردع.
- حدّد الاستراتيجيات الأمنية التي تستخدمها منظمتك، والاستراتيجية الأكثر صلة بهذا السياق على الأخص.

تدابير إدارة المخاطر

بمجرد معرفة الاستراتيجية التي ستستخدمها، يمكنك تطوير إجراءات إدارة المخاطر. قد تشمل تدابير إدارة المخاطر الشائعة ما يلي:

- إجراءات التشغيل القياسية (SOPs)
 - خطط الطوارئ
- تقاسم المخاطر (العمل مع الشركاء المحليين)
 - إعارة الخبراء المتخصصين (SMEs)
 - المناصرة والدفاع

خطة الحماية

الخطة الأمنية هي:

- وثيقة بسيطة تقدم إرشادات للعمل اليومي الآمن.
- خطة شاملة تم إنشاؤها بتمثيل جميع العاملين والأدوار الوظيفية والملفات الشخصية.

التنسيق الأمنى بين المنظمات غير الحكومية ومصادر أخرى للدعم

- تعتمد الإدارة الفعالة للمخاطر الأمنية على معلومات واردة من عدّة مصادر.
 - يزيد التنسيق الأمني من تدفق المعلومات والتحقق.

إجراءات التشغيل القياسية

حدّد كيفية تخفيف العاملين للتهديدات التي تم تحديدها في تقييم المخاطر.

خطط الطوارئ

حدّد كيفية استجابة الإدارة والموظفين للمواقف المتوقعة.

أمن المرافق

حدّد التهديدات ونقاط الضعف والمخاطر التي تتعرض لها جميع الممتلكات، بما في ذلك المكاتب والمجمعات والمرافق التي تستخدمها منظمتك، وقم بإجراءات التخفيف الملائمة.

أمن الاتصالات والمعلومات

- إن أنظمة الاتصالات ضرورية للحفاظ على سلامة الموظفين والمستفيدين.
- اضمن أمن المعلومات التنظيمية بما في ذلك التخزين الآمن لجميع البيانات والمستندات وحمايتها.

السفر الآمن

قم بوضع إجراءات لإدارة السفر الآمن في المطارات وعند استخدام المركبات أو وسائل النقل داخل وبين البلدان.

الإسبات والانتقال والإخلاء

حدّه الوقت الذي تكون فيه إجراءات الإسبات أو الانتقال أو الإخلاء هي الإجراءات الأنسب في الحالات الخطرة أمنيا.

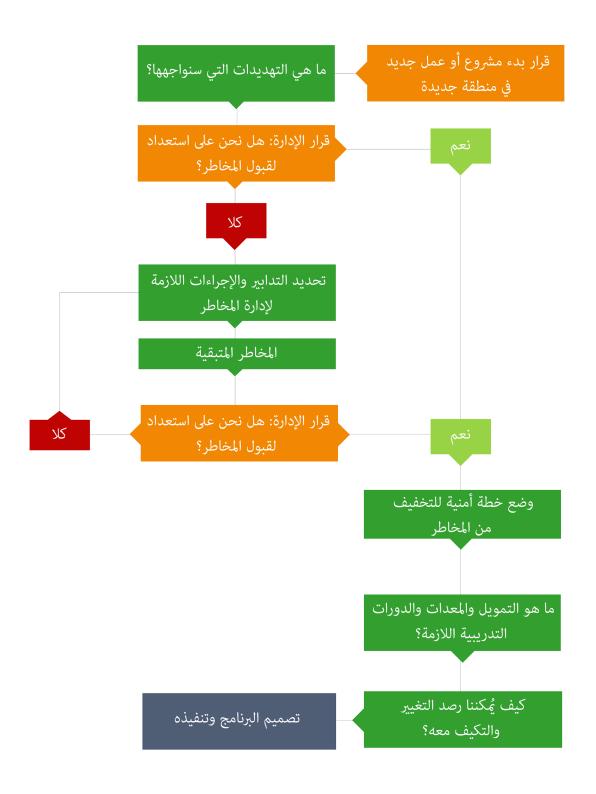
- الإسبات: بقاء العاملين في المنزل (أو المكتب) ويكون هناك تعليق مؤقت للبرامج أثناء الأزمات.
- الانتقال: نقل المكاتب أو العاملين أو الأنشطة أو كل ذلك إلى موقع أكثر أمانًا داخل نفس البلد، وعادةً يكون ذلك بشكل مؤقت.
- الإخلاء: نقل العاملين الدوليين إلى دولة أو منطقة أخرى، ومساعدة نقل العاملين الوطنيين إلى مناطق أكثر أمانًا، مع تعليق البرامج أو استمرارها مع الإدارة عن بُعد.

الدعم الطبى والإخلاء

قم بوضع خطط استجابة للطوارئ الطبية تشمل العاملين والمجتمعات.

تقييم المخاطر الأمنية

تعد أول خطوة لجميع تدابير السلامة والأمن هي استكمال تقييم المخاطر. يمكن للكوارث الطبيعية والمجاعات وتفشي الأمراض وحتى الانتخابات الوطنية أن تشكّل ذات عدد المخاطر التي يمكن أن يشكّلها الصراع أو الإرهاب أو أنواع أخرى من العنف. لا تتعلق إدارة المخاطر الأمنية الجيدة بتجنّب المخاطر فحسب، بل بالتعرف على المخاطر ووضع تدابير مناسبة لإدارة المخاطر لتمكين تسليم البرامج بأمان. إذا كانت الإجراءات الأمنية تمنع تنفيذ البرامج، فيجب على منظمتك التفكير فيما إذا كانت مجهزة للعمل في تلك البيئات.



العناصر المهمة لتقييم المخاطر الأمنية

عند الاستجابة لحالة طوارئ جديدة أو عند بدء عمليات في منطقة جديدة، من الضروري دمج تقييم المخاطر الأمنية في عملية تقييم الاحتياجات. من خلال القيام بذلك، يمكن دمج أي تكاليف لإدارة المخاطر الأمنية في تصميم البرنامج منذ البداية بدلاً من وضع التعديل عليه في النهاية. هناك العديد من العناصر شديدة الأهمية التي يجب على منظمتك أخذها بعين الاعتبار عند التخطيط والإعداد لتقييم المخاطر الأمنية.

واجب الرعاية

- واجب الرعاية هو الالتزام القانوني والأخلاقي لمنظمة ما باتخاذ جميع التدابير الممكنة للحد من خطر إلحاق الضرر بمن يعملون لصالح المنظمة أو من يعملون نيابة عنها.
- ينطبق واجب الرعاية على جميع المنظمات التي توظف عاملين في بيئات صعبة. يشمل ذلك الموظفين والمتطوعين والمتدربين والمتعاقدين (مثل الحراس أو السائقين) والمنظمات الشريكة (على الرغم من أن مستوى واجب الرعاية المطلوب قد يكون مختلفًا).
 - و يكن مقاضاة المنظمات بسبب الإهمال في واجب الرعاية، ما في ذلك كبار المدراء على مستوى فردى.

تكاليف إدارة المخاطر الأمنية

إدارة المخاطر الأمنية الجيدة لا تحتاج بالضرورة إلى تكاليف مالية عالية. في كثير من الحالات يتعلق الأمر أكثر بما يلي:

- بناء قدرات العاملين
- وضع سياسات جيدة تتكيف مع الملفات الشخصية المتنوعة للعاملين
 - مراقبة بيئة التهديد باستمرار
 - الحفاظ على خريطة الحوادث
 - وضع سياسة لتسجيل الوصول
 - تطبیق حدود سرعة السیارة
 - · توفير مستلزمات الطوارئ
- المشاركة في منتديات المنظمات غير الحكومية الأخرى لضمان سلامة وأمن العاملين بالمنظمة والأملاك
 - التأكد من أن المانحين على دراية بتكاليف إدارة مخاطر الأمن والسلامة

إذا كان تقييم المخاطر الأمنية يبرر النفقات، فيمكن دمج التكاليف المباشرة في ميزانية تنفيذ البرنامج. ومع ذلك، يمكن أن يكون التحدي الرئيسي هو تحديد العاملين المسؤولين وإعطاء أولوية للقيام بهذه الأنشطة.

التكاليف المتعلقة بالأمن

غالبًا ما يكون المانحون على استعداد لتمويل بنود الميزانية الأمنية إذا كان هناك ما يبررها من قبل تقييم المخاطر. تأكد من تضمين ما يلي في مقترحات وميزانيات مشروعك:

- المعدات (أجهزة الراديو والهواتف الفضائية ومجموعات الإسعافات الأولية ومعدات وإمدادات الطوارئ وأموال الطوارئ وتحسين المرافق والتأمين)
 - · الوقت (تنفيذ استراتيجية قبول استباقية، والتفاوض من أجل الوصول المستدام)
 - بناء القدرات (التدريب والكتيبات وورش العمل)

السياسات والإجراءات الأمنية

تحديث السياسات والإجراءات الأمنية بانتظام للتكيف مع التهديدات المتغيرة في بيئة العمليات. أجب عن الأسئلة التالية:

- من المسؤول عن مراجعة وتحديث تقييم المخاطر والخطط الأمنية؟
 - كم مرة يجب القيام بذلك (سنويًا، ربع سنويًا، شهريًا)؟
- ما هي مؤشرات التغيير التي ستؤدي إلى مراجعة مخصصة لتقييم المخاطر والخطط الأمنية؟
 - كيف سيتم إبلاغ العاملين عن التغييرات في السياسات والإجراءات وتدريبهم عليها؟
- هل يدرك العاملون على نحو كافي المخاطر الفردية وكذلك المخاطر التي تؤثر على عمال الإغاثة الآخرين؟

رسم خرائط الحوادث

عامل مهم في مراقبة الطبيعة المتغيرة للتهديدات في بيئة العمليات هو تحديد مؤشرات التغيير. واحدة من أبسط الطرق وأفضلها لمراقبة التغيير هي رسم خرائط للحوادث. قد يشمل ذلك:

- تحديد التطورات السياقية التي يمكن مراقبتها والتي ينبغي مراقبتها لإعطاء تحذير مبكر من التغييرات التي يمكن أن يكون لها تأثير على المخاطر التى تواجهها المنظمة.
- و تضمين "الحوادث القريبة من الأخطاء" والحوادث التي حدثت في بيئة التشغيل الخاصة بك ولكنها لم تؤثر بشكل خاص على منظمتك.
 - · تطوير آليات قوية للإبلاغ حيث يسهل الوصول إليها لرصد التهديدات الداخلية وتسهيل الإبلاغ عن المخاوف والحوادث.
 - تتبّع أوقات وأماكن الحوادث، بما في ذلك الوقت التفصيلي والأفراد المستهدفين والعواقب، لتحديد تحسن أو تدهور الوضع وكذلك أوقات التحسن والتدهور. على سبيل المثال، يمكنك استخدام خريطة بدبابيس مختلفة الألوان لتمثيل كل نوع من أنواع الحوادث والمتضررين (منظمتك، منظمة غير حكومية أخرى، الأمم المتحدة، منظمة شريكة، منظمة غير حكومية محلية).



الاستراتيجيات الأمنية

هناك ثلاث استراتيجيات أمنية رئيسية تستخدمها منظمات المساعدة الإنسانية في جميع السياقات: القبول والحماية والردع. غالباً ما تعطي منظمات المساعدة الدولية والوطنية أولوية لاستراتيجية القبول باعتبارها النهج المفضل. ومع ذلك، يستغرق هذا وقتًا للتطوير ولا ينبغي للمنظمات التي تنتشر في مناطق جديدة أن تفترض قبول المجتمع لها منذ البداية. في هذه الحالة، قد تركز المنظمات في البداية على تدابير الحماية والردع حتى يتم تطوير القبول، مع الأخذ بعين الاعتبار أن جميع سلوكيات الموظفين وإجراءاتهم ستؤثر على جهود بناء القبول.



القبول

الحد من المخاطر عبر تغيير التهديد.

مثال: بناء بيئة عمل آمنة من خلال الموافقة والقبول والتعاون من جميع الجهات المعنية المحلية، بما في ذلك الأفراد والمجتمعات والسلطات المحلية.

الحماية

الحد من المخاطر وليس التهديد. سيؤدى ذلك إلى تقليل تعرض المنظمة لهذا التهديد.

مثال: الأسوار والحراس والإجراءات.

الردع

تقليل المخاطر من خلال احتواء التهديد بتهديد مضاد.

مثال: الحماية المسلحة، النفوذ الدبلوماسي أو السياسي، التعليق المؤقت.

نصائح لبناء القبول

بعد حدوث حالة طوارئ بشكل سريع، يصعب على الحكومات والمجتمعات المضيفة التمييز بين المنظمات المختلفة عند وصول مجموعة جديدة من المنظمات غير الحكومية الدولية والوطنية الجديدة ووكالات الأمم المتحدة إلى المنطقة. يمكن أن يكون هذا معقدًا بسبب التغيير السريع للعاملين في الأسابيع القليلة الأولى حيث يقوم المستجيبون الأوائل بتسليم مهام العمل إلى العاملين الباقون على المدى البعيد. في هذا النوع من الحالات يجب على المنظمات الحصول على المعلومات من جميع الموظفين المحليين والمنتشرين، بما في ذلك المدراء ومُحركي المجتمع والسائقين، حول كيفية توظيفهم للاستراتيجيات الأمنية الثلاث، وكيف سيتم بناء القبول مع جميع الجهات المعنية. اتبع هذه الإرشادات حول بناء القبول.

يجب أن تدرك بأنّ التقبّل المجتمعي يكتسب ويمكنك فقدانه بسهولة بالغة. قد يؤثر سلوك مستجيب واحد على المجتمع بأكمله.

يجب اكتساب القبول ليس فقط داخل المجتمعات التي تعمل فيها منظمتك، ولكن مع جميع الجهات المعنية.

اتّبع نهج فعّال للتقبّل المجتمعي. وتأكّد من مشاركة الجهات المعنية الرئيسية قبل البدء في أي عمل.

قم بإنشاء خريطة فاعلين لتحديد الجهات المعنية التي قد تتأثر من برامج منظمتك، ولتحديد الحلفاء في تطوير القبول مع الجهات المعنية الأخرى.

تذكّر بأن الجهات المعنية تحصل على معلومات من مصادر أخرى، ليس فقط من منظمتك والعاملين المحليين.

كن واضحا بشأن مهمة منظمتك وخلفيتها وأولوياتها ومصادر تمويلها وكيفية تطوير البرامج.

جعل الرسائل التي توجهها للمجتمعات والسلطات المحلية متسقة مع المعلومات الموجودة على موقع منظمتك وقنوات التواصل الاجتماعي الخاصة بك.

قم بإدراك كيف يرى الآخرون منظمتك والعاملين بها. افهم الشركاء الذين تعمل معهم، والنظرة العامة تجاههم، وما تأثير العلاقة بينكم على قبولك وقبولهم. إذا كنت تمثل منظمة دينية أو علمانية، فكن واضحًا بشأن كيفية تأثير ذلك أو عدم تأثيره على عملك، خاصة في البيئات الدينية القوية.

يجب أن يكون لديك نظام شكاوى صارم وعملية واضحة للمتابعة واتخاذ إجراءات بشأن المخاوف.

لا تعزل موظفيك عن المجتمع المحيط. عزز تواجدك وكن متاحًا للوصول.

نصائح لتعزيز الحماية

يجب تطوير تدابير الحماية بما يتماشى مع تقييم المخاطر لدى منظمتك، ويجب تطبيقها بالتساوي على الموظفين على اختلاف المستويات (المتطوعين والعاملين والدوليين والإدارة العليا). اتبع هذه الإرشادات حول تعزيز الحماية.

قم بتوفير التدريب والتحديثات المنتظمة بشأن التدابير الأمنية للعاملين، عما في ذلك "السبب" و"الماهية".

تأكِّد من أن إجراءات الحماية مناسبة للسياق. يمكن أن تكون التدابير الصارمة غير فعالة كتلك التي تكون متساهلة للغاية.

قم بتحديد نقاط الضعف المختلفة للموظفين والتأكد من أن التدابير تعكس احتياجات أنواع الملفات الشخصية الفردية، ما في ذلك الخصائص المخفية وكذلك المرئية.

قدّم إحاطات عن التدابير الأمنية باعتبارها جزء من التوجيه لجميع الموظفين الجدد، سواء المحليين أو الدوليين.

متابعة التنسيق مع الهيئات والمنتديات الأمنية الأخرى.

تأكّد من أن المجمّعات والمكاتب أو أماكن العمل الأخرى تندمج مع المباني المجاورة. يجب ألا تكون الحماية المادية للمباني أو المجمعات أو مواقع التوزيع تبدو كما لو أن المنظمة تقوم ببناء مخبأ أو حصن.

استخدم أفضل الأنظمة المتاحة للاتصالات وبأسعار معقولة تناسب منظمتك (راديو، إنترنت، هاتف محمول، خط أرضي، قمر صناعي، فاكس، بريد سريع غير رسمي). لا تعتمد بشكل مطلق على طريقة اتصال واحدة.

قم بوضع سياسات لأنظمة الاتصالات تمكن الموظفين من الإبلاغ (بانتظام أو حسب جدول زمني) لضمان السلامة.

نصائح لاستخدام الردع

عادة ما يكون الردع هو الحل الأخير. يتم استخدامه عندما لا تنجح إجراءات القبول والحماية أو عندما يثبت أنهما غير ملائمين. في بعض السياقات، قد تكون تدابير الردع مطلوبة من قبل الحكومات المضيفة. اتبع هذه الإرشادات حول استخدام الردع.

اعتبر تمامًا عواقب التهديد بوقف الخدمات كإجراء للردع. لا تقم بتوجيه تهديدات فارغة.

كن حذر عند سحب الخدمات من منطقة غير آمنة. يجب أن تضمن منظمتك أولاً عدم تعرض الحكومات المحلية واتفاقيات المانحين للخطر.

تجنّب الحراس المسلحين أو الجيش أو مرافقة الشرطة حيثما أمكن ذلك. فهم غالبًا ما يجعلون القبول مستحيلًا أو صعبًا للغاية، حتى فيما بعد. وقد تزيد أيضًا من مخاطر الابتزاز أو المضايقة أو الإصابات الناجمة عن تبادل إطلاق النار.

يجب الإدراك بأنّ جميع المنظمات مختلفة، ليس فقط في مهمتها وبرامجها، ولكن أيضًا في نقاط ضعفها وقدرتها على الاستجابة للحوادث. لا يعني تنفيذ استراتيجية منظمة أخرى أنها ستعمل لصالح منظمتك، حتى إذا كنت تعمل في نفس السياق.



الحكومية ومصادر الدعم الأخرى

المنتديات الأمنية ومصادر معلومات السلامة

عندما تتجمع منظمات المساعدة استجابةً لأزمة طارئة أو أزمة مستمرة، ستتطور أيضًا منتديات ومجموعات تنسيق مختلفة في ذلك البلد أو ذلك الموقع. في المناطق التي عِثل فيها انعدام الأمن مشكلة، قد تتكون أيضًا منتديات تابعة للمنظمات غير الحكومية. قد تكون جزءًا من هيئة تنسيق أوسع للمنظمات غير الحكومية، أو هيئة قائمة بحد ذاتها، أو مجموعة غير رسمية لتبادل المعلومات والتنسيق.

كبف تعمل المنتديات الأمنية

المنتديات الأمنية:

- عادة ما ترأسها منظمة واحدة وتحضرها نقاط اتصال أمنية للمنظمات الأعضاء.
 - تتشارك تقييمات السياق وتحليله.
 - تتشارك التقارير حول الحوادث وتتحقق من صحة المعلومات.
 - تتقاسم تكاليف تنظيم تدريب العاملين.
 - تقدم المشورة بشأن توصيات السفارات أو الحكومات المضيفة.
- يمكن أن تعمل كنقطة تنسيق مركزية مع الجهات الفاعلة الأخرى، مثل إدارة الأمم المتحدة للسلامة والأمن (UNDSS).

المشاركة في أحد المنتديات الأمنية

- مَكِّن المنتديات الأمنية المنظمات من جمع معلومات السياق وتحديد أفضل الممارسات لبلد أو موقع معين.
- لا تعد المنتديات الأمنية بديلاً عن قيام إحدى المنظمات بإجراء تقييم مخاطر خاص بها وتطوير علاقات عمل مع الجهات الفاعلة الرئيسية، مثل إدارة الأمم المتحدة للسلامة والأمن أو وكالات أخرى.
 - عند تعيين أحد العاملين لحضور اجتماعات التنسيق الأمنى، تأكد من أن الشخص:
 - ° مكنه المشاركة بنشاط في التحليل والتفاعل والإبلاغ عن الحوادث التي تؤثر على المنظمة.
 - و مكنه أن يكرس وقته ويعتبر هذا نشاطًا ذا أولوية.
 - ويتم إحاطته تمامًا بكل قواعد المشاركة.
 - يعلم كيفية إدارة أي معلومات مشتركة.
 - ° يتم دعمه في مشاركة المخرجات داخل المنظمة، بما في ذلك فرق البرنامج واللوجستيات، لتعزيز فوائد التعامل مع هيئة التنسيق.

مصادر أخرى لمعلومات السلامة والأمن

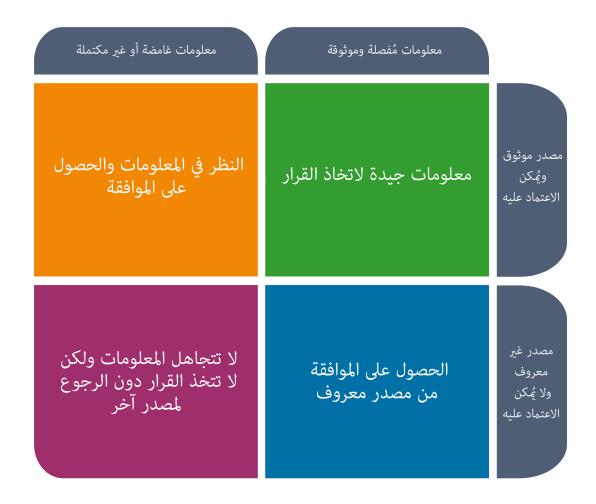
هناك عدد من المصادر التي يمكن أن توفر معلومات أمنية إضافية لمساعدة المنظمات على تحسين تدفق المعلومات حول الحوادث، والحصول على المشورة حول كيفية التخفيف من المخاطر الناجمة عن التهديدات المختلفة وتحسين القدرة الأمنية. وقد تتضمن ما يلى:

- ، إطار "إنقاذ الحياة معا" (SLT) للتعاون الأمنى بين المنظمات غير الحكومية والأمم المتحدة
 - الحكومات الوطنية وسفارات العاملين المنتشرين والحكومات المانحة
 - · الإدارات الحكومية المضيفة
- دائرة المساعدات الإنسانية والحماية المدنية التابعة للمفوضية الأوروبية (ECHO) (تنتج مواد أمنية لمنظمات المساعدة في بعض السياقات)
 - مقدمو التأمين (غالبًا ما يقدمون خدمات استشارية بشأن التهديدات مرتبطة بمختلف البلدان أو المناطق)
 - مستشارو أمن المنظمات غير الحكومية
 - مزودو الأمن المحليين لأغراض تجارية (شركات الحراسة)
 - وسائل الإعلام الدولية والوطنية
 - المنظمات غير الحكومية الأخرى والمنظمات الشريكة لها
 - المجتمعات المضيفة والمستفيدة
 - العاملون الوطنيون والمحليون
 - إدراك انعدام الأمن
 - واعدة بيانات أمن عمال المساعدة
 - المنظمة الدولية لسلامة المنظمات غير الحكومية (INSO) (في بعض البلدان)
 - منتدى الأمن الأوروبي المشترك بين الوكالات (EISF)

تقييم مصادر المعلومات

يتطلب اتخاذ قرارات جيدة لإدارة المخاطر الأمنية معلومات موثوقة ودقيقة. يجب النظر إلى جميع المعلومات حسب موثوقية المصدر، وعدد الأفراد أو المنظمات المنفصلة التي تبلغ عن نفس المعلومات، وأي تحيز محلي. من الضروري جدًا تجنب التصرف بناءً على معلومات أو شائعات دون التأكد من مصدر موثوق.

في حالة الطوارئ أو الأزمات، تعتمد سلامة العاملين التنظيميين والمجتمعات المستفيدة على قدرتك على اتخاذ القرارات وتفعيل خطط الطوارئ. استخدم هذه الشبكة البسيطة لتقييم صحة المعلومات (ومصدرها) التي قد تتلقاها منظمتك.



أداة المعلومات وتقييم المصدر

يكن لمنظمتك استخدام هذه الأداة لتقييم المعلومات ومصدرها. أولاً، قم بتقييم موثوقية المصدر الذي قدم المعلومات باستخدام مقياس تصنيف من 1-6 في العمود الأيمن حيث يشير "1" إلى أن المصدر موثوق للغاية، ويشير "6" إلى أن المصدر قد لا يكون موثوقًا بالمطلق. بعد ذلك، قيّم صحة المعلومات باستخدام مقياس تصنيف من F-A حيث تشير "A" إلى تأكيد المعلومات بينها يشير "F" إلى أنه لا يمكن تحديد صحة المعلومات. ستساعدك النتيجة المجمعة في تحديد الوقت الذي قد تحتاج فيه إلى اتخاذ إجراءات إضافية للتحقق من المصدر أو المعلومات التي تحصل عليها.

المعلومات		المصدر	
 مؤكدة منطقية متسقة مع المعلومات الأخرى ذات الصلة 	A	 موثوق به تمامًا عدم وجود شكوك في صحة المصدر أو مصداقيته أو كفاءته تاريخ حافل بالموثوقية الكاملة 	1
 صحيحة غالبًا منطقية متسقة مع المعلومات الأخرى ذات الصلة 	В	 موثوق عادة به شكوك ثانوية تاريخ حافل بالمعلومات الصالحة في الغالب 	2
 صحیحة علی الأرجح منطقیة علی نحو معقول متسقة مع بعض المعلومات الأخری ذات الصلة 	С	 موثوق به إلى حد ما به شكوك قدم معلومات صالحة فيما مضى 	3
 مشكوك في صحتها ليست منطقية ولكنها محتملة لا توجد معلومات أخرى حول الموضوع 	D	 غیر موثوق به عادة به شکوك كبیرة قدم معلومات غیر صالحة فیما مضی 	4
 غير محتملة ليست منطقية متعارضة مع المعلومات الأخرى ذات الصلة 	E	 غير موثوق به يفتقر إلى المصداقية والثقة والكفاءة تاريخ حافل بالمعلومات غير الصالحة 	5
 لا يُحكن الحكم على مدى صدقها لا يُحكن تحديد مدى صحتها 	F	 لا يُحكن الحكم على مدى موثوقيته معلومات غير كافية لتقييم صحة المصدر 	6