دليل إدارة المخاطر الأمنية: الخطة الأمنية

مستعد للانطلاق
الدليل المحمول

تعرف على المعلومات الأساسية التي يجب تضمينها في الخطة الأمنية للحفاظ على أمان منظمتك وشركائك وموظفيك ومجتمعاتك.

هيكل الخطة الأمنية

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 الأمني المشترك بين الوكالات **(EISF)** مسؤولية ذلك تحت أي ظرف من الظروف.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

نصائح لإنشاء خطة أمنية فعالة

الخطط الأمنية ليست وثائق استراتيجية، ولذا يجب أن تكون بسيطة وسهلة الاستخدام، وتوفر المعلومات بشكل يمكن للموظفين قراءته وفهمه واستخدامه بسهولة في عملهم اليومي. تعتبر الخطة الأمنية مهمة للغاية لجميع العاملين والمنظمات لأنها تقدم المشورة للعاملين حول كيفية إدارة ومعالجة المخاطر والتهديدات الأمنية المحتملة. اتبع هذه النصائح لإنشاء خطة أمنية فعالة لمنظمتك.

عند وضع الخطة الأمنية، عليك دمج مزيج من العاملين من القطاعات المختلفة (الإدارة العليا، والإدارة، وإدارة البرامج، والعاملين الميدانيين، والسائقين) بالإضافة إلى مختلف الجنسيات والأعراق والأجناس. يتيح ذلك وجود وجهات نظر مختلفة ويخلق شعورًا بملكية الخطة ويحسن من الامتثال لها.

ركّز على الإجراءات الأمنية التفصيلية للعاملين في الميدان لأنهم قد يكونوا أكثر عرضة للخطر. وتجنّب التركيز الزائد عن الحدَ على الأمور الإدارية.

الاهتمام باحتمالية تعرض جميع العاملين للخطر، باختلاف مستوياتهم ومواقعهم، بما في ذلك العاملين الوطنيين الذين ينفذون البرامج. تجنب التركيز المفرط على مجموعة معينة من العاملين، مثل العاملين الدوليين.

حدّد ما إذا كانت هناك نقاط ضعف محددة للعاملين الأقلويين مما قد يعرضهم للخطر في بيئة العمل. قم بوضع تدابير مناسبة لاستخدامها عند الضرورة ورفع مستوى الوعي بين العاملين حول هذه المخاطر.

اتّبع تنسيقًا عامًا وقدم معلومات تهتم بالعوامل الرئيسية المتعلقة بالمنظمة مثل نوع المشاركة وعدد العاملين وحجم الأصول وموقع المشاريع وسياق التشغيل والعوامل المحلية الأخرى.

يجب أن تقتصر الخطة على 20 صفحة أو أقل للحفاظ على قابلية إدارة المعلومات وسهولة قراءتها من قبل العاملين وكذلك سهولة تذكرها واستخدامها.

اشرح بوضوح لجميع العاملين أسباب وضع التدابير المختلفة للعاملين الدوليين والوطنيين والمحليين (إذا كانت تلك التدابير جزءًا من الخطة الأمنية). وإلا فقد يُنظَر إلى المنظمة على أنها ترعى مجموعة معينة من العاملين دون سواهم.

اجعل الخطة الأمنية (أو على الأقل الأجزاء ذات الصلة) متاحة بلغة المستخدمين. إذا كانت الترجمة غير مجدية، يجب اعتبار طرق بديلة لنشر المعلومات الواردة في الخطة الأمنية.

شرح الخطة الأمنية لجميع العاملين باختلاف مستوياتهم، ومن بينهم أولئك العاملين الأقل مشاركة في المنظمة مثل عمال النظافة والحرّاس. يساعد إبلاغ جميع الموظفين بالخطة الأمنية على منع العاملين من مشاركة الأموال أو قبول عروض مالية مقابل الحصول على معلومات سرية قد تؤثر على سلامة وأمن العاملين والمنظمة.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

عناصر الخطة الأمنية

قم بتضمين هذه العناصر الأساسية في خطة الأمان الخاصة بمنظمتك.

نظرة عامة عن الخطة الأمنية

- وضّح الغرض من الخطة وسبب أهميتها لجميع العاملين.
- حدّد المسؤول عن وضع الخطة وتحديثها وتدريب الموظفين.
- حدّد مستويات المخاطر الخاصة بمنظمتك، أي مستوى المخاطر الذي تستطيع المنظمة إدارته وكذلك المستوى المرتفع أو غير المقبول.
- قم بوصف استراتيجيتك الأمنية وطريقة استخدام المنظمة لاستراتيجيات القبول والردع والحماية وكيفية تقييم النتائج.
- قم بتضمين تاريخ كتابة الخطة، ومتى يجب مراجعتها وتحديثها وكم مرة يتعين عليك ذلك.

السياق الحالي (تقييم المخاطر الخاص بك)

- قم بوصف السياق العام بما في ذلك وصف عام للبلد والمنطقة والتحديات الحالية.
- اشرح نظام تقييم المخاطر الخاص بك والذي يتضمن كيفية تحديد التهديدات ونظام التصنيف.
- حدّد التهديدات التي تواجهها في سياقك وفكّر بالتهديدات الداخلية.
- قيّم هذه التهديدات وقدّم تصنيف المخاطر الخاص بهم.

إجراءات التشغيل القياسية (SOPs)

حدّد إجراءات التشغيل القياسية (SOPs) لجميع التهديدات والمخاطر المحددة في تقييم المخاطر الأمنية الخاصة بك. قدّم تعليمات بسيطة وواضحة حول كيفية منع العاملون المخاطر (تقليل الاحتمالية) وكيفية التصرف بحال وقوع حادث (تقليل التأثير). استخدام قوائم المراجعة أو الإجراءات أو المبادرات لمعالجة المجالات التالية:

- تحويل الأموال
- استراتيجية التواصل وخطة وسائل التواصل الاجتماعي
- الإبلاغ عن الحوادث والتهديدات الداخلية (المضايقات والتنمر)
- السفر الميداني وسلامة المركبات
- الحرائق (في المكتب أو المجمع)
- القدرة على الوصول إلى المكاتب والمرافق
- السطو والسرقة
- حوادث السيارات
- إجراءات التشغيل القياسية الأخرى

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

الأقسام الرئيسية الأخرى

قم بتقديم معلومات أساسية أخرى ذات صلة بمنظمتك والعاملين فيها وبرامجها، مثل:

- سياسات الصحة والسلامة لحماية العاملين من التهديدات الجسدية والعقلية مثل المرض (الملاريا، فيروس نقص المناعة البشرية) والإصابات والحوادث والإجهاد واضطراب ما بعد الصدمة
- سياسات الموارد البشرية المتعلقة بالتوظيف والتحقق من الخلفية والعقود والسرية
- سياسات التنوع ومكافحة التمييز، بما في ذلك المعلومات حول كيفية استيعاب منظمتك لنقاط الضعف المحددة للعاملين وتدابير التخفيف من التهديدات الداخلية (أنظمة الإبلاغ والكشف عن الفساد)
- سياسات الأمن الإداري والمالي لمنع السرقة والاحتيال والفساد وكذلك التعامل مع النقد والمشتريات
- الأقسام الرئيسية الأخرى

قسم إدارة الأزمات

- قم بوصف الأفراد الذين يعدّون جزءًا من فريق إدارة الأزمات (CMT)، وكذلك التسلسل الإداري الخاص بهم للإبلاغ.
- اشرح كيفية تنشيط فريق إدارة الأزمات في حالة الطوارئ.
- قم بوصف خطط الطوارئ الموضوعة للتعامل مع أي أزمات محتملة مثل الاختطاف أو الكوارث الطبيعية أو عمليات الإخلاء أو النزاع المسلح. على عكس إجراءات التشغيل القياسية، تعد خطط الطوارئ أداة إدارة داخلية ليست للمشاركة أو المعرفة العامة.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

أمن المرافق

تأمين المكاتب والمجمعات والمرافق الأخرى

عند النظر إلى مكتب أو سكن أو مجمع جديد، من الضروري مراجعة تقييم المخاطر الأمنية لمنظمتك في البدء لفهم أنواع التهديدات ومستوى كل تهديد ومستوى الحماية أو الردع الذي ستحتاجه للتخفيف من هذه التهديدات. ينطبق هذا أيضًا عند الانتقال إلى مكتب قائم مع منظمة شريكة.

عليك الاهتمام ببناء استراتيجية قبول لجميع الممتلكات المؤسساتية والمكاتب والمساكن والمستودعات والعيادات والمدارس في مواقع العمليات. يمكن أن يكون هذا أكثر صعوبة في المواقع الحضرية الكبيرة بينما يكون سهل إدارته في المناطق الريفية. ومع ذلك فمن المستحسن دائمًا أن يكون هناك تفاهم متبادل مع جيرانك. إذا كانت استراتيجية القبول ممكنة، فمن المهم الاتفاق على ماهية المسؤول عن إدارة الإجراءات الأمنية المختلفة مثل أمن المنطقة المحيطة وخدمات الحراسة واستراتيجية القبول المحلية وغيرها من الإجراءات.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

تأمين الجوار

الجوار هو المنطقة المحيطة بالمكتب أو المجمع أو المنشأة أو السكن. يمكن أن يكون للناس في هذه المنطقة تأثيرًا على سلامة العاملين. يجب أن يحدد تقييم المخاطر الذي وضعته العناصر الرئيسية لتأمين الجوار المحيط بمكان عملك.

حدّد الجهات المعنية الموجودة في الجوار والذين سينفذون استراتيجية القبول الخاصة بك. من الضروري تطوير التفاهم بينك وبين جيرانك في جميع البيئات سواء الريفية أو الحضرية.

حدّد نوع الطريق الذي يؤدي إلى المكتب وكيف سيسافر العاملون بأمان إلى المواقع الأخرى. قد يكون الطريق المسدود أمرًا سيئًا ولكنه سيحدّ من خيارات السفر ومسارات النجاة.

حدّد المخاطر الطبيعية مثل الأنهار (الفيضانات) أو التلال (الانهيارات الطينية/الانهيارات الجليدية) أو المستنقعات (الملاريا/حمى الضنك) أو الغابات (الحرائق/الحياة البرية).

حدّد موقع السفارات المجاورة أو مراكز الجيش أو الشرطة أو البنوك أو المكاتب الحكومية أو المنظمات غير الحكومية الأخرى أو الجامعات.

احسب المسافة إلى المطارات والفنادق والمواقع الرئيسية في حالات الطوارئ.

حدّد الهياكل المعرقلة والخصائص الطبيعية التي من شأنها تعطيل اتصالات الأقمار الصناعية في حالات الطوارئ.

راجع سجل المالك وسمعته.

حدّد مصادر موثوقة تتيح لك الحصول على مياه نظيفة.

حدّد إمكانية الوصول الموثوق إلى خط هاتف وشبكة إنترنت وشبكات جوال.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

تأمين الممتلكات

الممتلكات هي المناطق الأولى التي تقع تحت سيطرة المنظمة. يجب أن يحدد تقييمك للمخاطر الأمنية ما يلي:

- استراتيجيتك للحماية وطرق تأمين المنطقة باستخدام جدار محيط أو حاجز أو سياج.
- إذا كنت تشعر بالحاجة إلى إنشاء مخبأ للبقاء آمنًا، فربما يجب ألا يكون مقرّك في هذه المنطقة.

تخطيط المنطقة المحيطة

خذ ما يلي بعين الاعتبار عند تخطيط محيط ممتلكات منظمتك:

- كيف سيؤثر وجودك على جيرانك وعلى صورة منظمتك وعلى الرسالة التي تهدف إلى نشرها؟
- هل تحتاج إلى مولد كهربي؟ إذا كنت بحاجة إليه، فهل يمكن وضعه بعيدًا عن الممتلكات الأخرى أو هل هناك مساحة لعزل الصوت أو هل يتوافر كلا الخيارين؟
- هل توجد مواقف كافية للسيارات داخل المجمع أو في المنطقة دون أن يتسبب ذلك في إزعاج الآخرين؟
- هل يخلق وجودك مخاطر أمنية على جيرانك؟
- إذا كنت توظف حراسًا، فأين سيكون موقعهم؟

تدابير حماية المباني

من الممكن وضع تدابير حماية لا تغير مظهر المجمّع على نحوٍ سلبي. على سبيل المثال، استخدام الأسلاك الشائكة أسفل الجزء العلوي من الجدار أو استخدام أحواض الزهور أو الأواني لإخفاء الحواجز الإسمنتية. خذ بعين الاعتبار المشاكل المحتملة التالية التي قد تواجه ممتلكاتك الخاصة:

- كيف يمكن للعاملين أو الزوار أو الموردين أو أعضاء المجتمع الوصول إلى ممتلكاتك؟
- كيف ستتم إدارة بوابات عبور المركبات أو الأفراد، وفحوصات الهوية، والأماكن الآمنة لوقوف السيارات، وبطاقات الهوية، وأماكن الانتظار، والسيطرة على التجمعات (إن وجدت)؟ ما مدى سهولة دخول الأشخاص إلى الموقع؟
- إذا كنت توظف حراسًا، فأين سيكون موقعهم؟
- هل هناك مساحات مفتوحة أو حدود مشتركة مع الجيران؟
- هل هناك أشجار متدلية وما هو مدى قرب المباني من الجدران الحدودية؟
- ما هي مخاطر الحرائق المحتملة (تخزين الوقود والمواد القابلة للاحتراق، وخطوط الطاقة الكهربائية، والمناطق المخصصة للتدخين)؟
- كيف يتم جمع القمامة والتعامل معها بطريقة آمنة ومناسبة بيئياً؟
- كيف ستدير مخارج الطوارئ؟
  - ✓ إذا كان المجمّع الخاص بك يحتوي على جدار وبوابة رئيسية تواجه الشارع، فكيف سيتم إخلاء العاملين دون مراقبة إذا كان هناك خطر أمام المنشأة؟
  - ✓ كيف يخرج العاملون من ذوي الإعاقة الحركية بأمان؟
  - ✓ إلى أين سيذهب العاملون بمجرد خروجهم من العقار؟
  - ✓ هل يوجد مجمّع مجاور أو مرفق تابع للأمم المتحدة أو أي منظمة غير حكومية أخرى أو مساكن يمكن للعاملين الوصول إليها؟

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

تأمين المبنى

يعد تأمين مباني منظمتك، سواء كانت مكاتب أو مجمّعات أو مخازن أو مساكن، أمرًا أساسيًا حيث أنها تحتفظ بأكثر العناصر قيمة بالنسبة لك بما في ذلك الأشخاص والمعدات والأملاك والنقد والسجلات ومواد المساعدة أو الإمدادات. يجب أن يكون تصميم المبنى مناسبًا أيضًا للمخاطر الطبيعية (مقاوم للزلازل، ومعزول ضد الحرارة أو البرودة). من المهم أيضًا أن يشعر العاملون بالأمان في مكاتبهم وأماكن إقامتهم. يجب أن يحدد تقييم المخاطر الذي وضعته هذه العناصر الرئيسية لتأمين مباني المنظمة.

قم بتأمين الأبواب والنوافذ حيث تمنع الوصول غير المصرح به ولكن لا تحتجز العاملين بحال نشوب حريق أو إخلاء.

قم بتأمين الأسطح (غالبًا ما تكون نقطة دخول مفضلة لعمليات السطو).

قم بإعداد منطقة استقبال تتحكم في الوصول إلى المناطق الضعيفة الأخرى.

قم بوضع إجراءات التحكم في الوصول وتنفيذها حتى لا يتمكن الزوار من التجول حول المبنى بدون إشراف.

قم بجدولة فحوصات كهربائية منتظمة لتقليل مخاطر الحريق ووضع سياسات صارمة لمنع التحميل الزائد على المآخذ الكهربائية.

قم بضمان التخزين الآمن للمستندات يتضمن ذلك توفير الخزائن المقاومة للحريق المثبتة على الحوائط أو الأرضيات.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

قم تحديد وتصنيف طرق الإخلاء في حالات الطوارئ. درّب العاملين على إجراءات الإخلاء وقم بتجريب إجراءات الإخلاء. احرص من أن التدريب يشمل كيفية المساعدة في إخلاء العاملين الذين يعانون من إعاقات حركية (باستخدام كراسي الإخلاء).

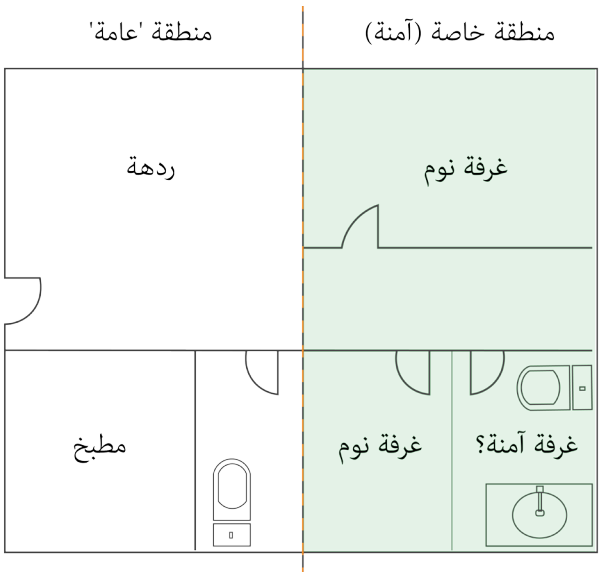
إذا لزم الأمر، قم بتجهيز مساحة آمنة تتناسب مع جميع الموظفين في المبنى على أن تكون مزودة بمستلزمات الطوارئ (مجموعة الإسعافات الأولية والمصابيح والأغطية والأغذية وطفاية الحريق وأجهزة الاتصال التي يتم شحنها أو تشغيلها). تحقق من أن معدات اتصالات الطوارئ تعمل في الغرفة الآمنة. تتطلب هواتف الأقمار الصناعية عادةً خط رؤية، لذا قد تكون هناك حاجة إلى هوائيات خارجية.

إعداد وحدات تزويد الطاقة دون انقطاع (UPS) لحماية أجهزة الكمبيوتر والأجهزة الكهربية الأخرى عندما يكون مصدر الطاقة غير موثوق به أو عرضة لارتفاع التيار الكهربي أو انقطاعه.

قم بتثبيت أجهزة إنذار واختبارها. أبلغ العاملين بخطوات العمل التي يجب اتباعها عند سماع هذه الإنذارات وتدرّب على اتخاذ تدابير الإخلاء في حالات الطوارئ. تأكد من أن العاملين ذوي الإعاقة السمعية أو البصرية يمكنهم التعرّف على نظام الإنذار.

تأمين مساكن العاملين

يمكن التعامل مع تأمين مساكن العاملين بطريقة مماثلة للعقارات الأخرى ولكن مع بعض الاحتياطات الإضافية لضمان السلامة. في حين يحتاج السكن بأكمله إلى التأمين الكافي، فإن الأشياء الثمينة (مثل أجهزة التلفاز وأجهزة الكمبيوتر والأجهزة المنزلية) يتم الاحتفاظ بها عادةً في المناطق "العامة" في المنزل حيث يتمكن الضيوف أو الأصدقاء من التسلية، ومن المحتمل أن تكون هذه العناصر مصدر رئيسي لإغراء اللصوص. يجب أن تكون المناطق الخاصة في السكن التي تحتوي على مناطق للنوم أكثر أمانًا من المناطق العامة.



قم بتثبيت باب صلب قابل للقفل بين المناطق العامة والمناطق الخاصة في السكن.

قم بتأمين النوافذ والأسقف في المناطق الخاصة. يجب أن تكون النوافذ قابلة للقفل من الداخل بشرط ألا تشكل عقبة للإخلاء بحال نشوب حريق.

تجهيز المساحة الآمنة بأدوات الإسعافات الأولية والأغطية ومصباح يدوي وطفاية حريق وجهاز اتصالات يتم شحنه واختباره بانتظام.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

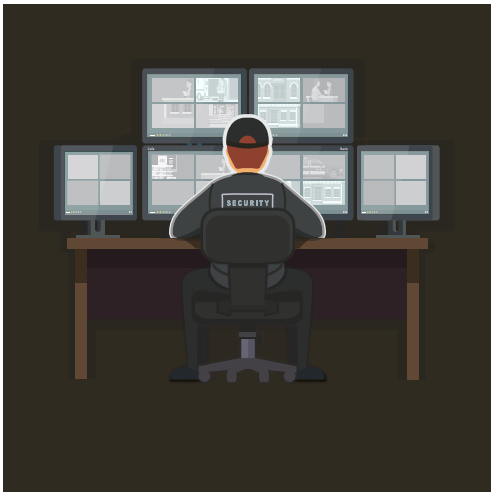
تثبيت ستائر النوافذ لمنع البعوض (للوقاية من الأمراض).

الاحتفاظ بالمفاتيح وأي نسخ منها في مكان آمن للغاية.

تركيب الأضواء الخارجية خاصة حول المداخل.

خذ الثقافة المحلية بعين الاعتبار. في البيئات المحافظة، قد تحتاج إلى وحدات سكنية منفصلة للذكور والإناث. قد تحتاج أيضًا إلى النظر في الفصل بين العاملين الوطنيين (مثل الحراس والسائقين) والعاملين الدوليين. قد يكون هذا الفصل ضروريًا لطمئنة العاملين الدوليين بشأن احتمالية الإساءة إليهم من قبل أحد العاملين الآخرين أو أخذ الانطباع الخاطئ عنهم بسبب تناول المشروبات الكحولية أو الرقص أو ارتداء ملابس معينة غير مقبولة في الثقافة المحلية.

المراقبون وحراس الأمن



قررت العديد من المنظمات العمل مع المراقبين المحليين وحراس الأمن، أو كليهما معًا، كخطوة أولى لتطوير أنظمتها التأمينية للمنشآت. غالبًا ما تستخدم المنظمات مصطلح "المراقبين" بدلاً من "الحراس" لاستنتاج أنه لا يُتوقع من العاملين المخاطرة بسلامتهم لحماية المجمّع والأصول. غالبًا ما يكون الحرّاس نقطة الاتصال الأولى بين المجتمع المضيف والمنظمة. غالبًا ما ينعكس سلوك الحرّاس وأسلوبهم ومهنيتهم على أرباب عملهم. اتبع هذه الإرشادات عند العمل مع الحراس أو المراقبين.

- ✓ قم بإبلاغ الحراس بتفويض منظمتك وقواعدها السلوكية.
- ✓ قم بإبلاغ الحراس بتعليمات واضحة حول واجباتهم وكيف سيتم الإشراف عليهم.
- ✓ زوّد الحراس بقائمة توضح الإجراءات المتعلقة بكيفية إدارة الزائرين أو الأنشطة المشبوهة أو السرقة أو السطو أو الحريق أو الإصابات أو الحوادث الأخرى المحتمل حدوثها والتي تم تحديدها في تقييمك للمخاطر الأمنية.
- ✓ تأكد من أن العاملين يتعاملون مع الحراس باحترام ومن أنهم يفهمون واجباتهم لضمان الامتثال.
- ✓ امنح الحراس قائمة تضم جهات الاتصال في حالات الطوارئ وحدد وسيلة للاتصال في حالة وقوع حادث.
- ✓ غالبا ما يكون الحراس الذين يعملون لدى المنظمات غير الحكومية غير مسلحين. ومع ذلك، فإن بعض المنظمات قد يكون لديها استجابة مسلحة في حالة الطوارئ في البيئات عالية المخاطر، ويتم تنشيط هذه الاستجابة بواسطة أزرار الذعر أو الحراس الموجودين. إذا كان هذا هو الحال بالنسبة لمنظمتك، فاحصل على معلومات حول من يقدم الخدمة المسلحة (سواء كانت شركة خاصة أو شرطة أو جيش) وأهدافهم (حماية موظفي المنظمة وأملاكها أم القبض على المهاجمين) ومستوى تدريبهم ومسؤولية منظمتك إذا تم إطلاق النار على أحد الأشخاص (موظف، حارس، أحد المارة) أثناء الاستجابة المسلحة.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

خدمات الحراسة التجارية

يتم توفير خدمات الحراسة التجارية من قبل شركة خدمات حراسة متعاقدة. قد يتناوب موظفو شركة الحراسة على أوقات العمل مما يصعّب من خلق مستوى من الثقة بين الحارس والعاملين بالمنظمة. من المهم، خاصة بالنسبة للمباني السكنية، أن يعرف العاملون الحارس المسؤول عن موقع العمل ويثقون به، وإلا فقد يكون الحارس سببًا في شعور السكّان بعدم الأمان بدلاً من الاطمئنان. فيما يلي بعض مزايا وعيوب العمل مع خدمات الحراسة التجارية.

المزايا

- يمكن أن تقدم شركة خدمات الحراسة خدمات إضافية مثل فريق الاستجابة السريعة (كن واضحًا بشأن ما ينطوي عليه ذلك)، وأجهزة الإنذار وشبكات الراديو ودوريات المركبات والمشرفين الليليين.
- تتولى شركة خدمات الحراسة مسؤولية إدارة التوظيف والتدريب والرواتب والموارد البشرية والإدارة والجدولة.

العيوب

- تكاد تكون سيطرة المنظمة على تعليمات الحراسة ومعايير الواجب منعدمة.
- تهتم شركات خدمات الحراسة في الغالب بتحقيق الربح من الاحتياجات الأمنية للمنظمة.
- قد لا يتقاضى الحرّاس أجرًا عادلًا في أغلب الأحيان وقد لا يتم تحفيزهم على نحوٍ ملائم.

حراس متعاقدون

يتم توظيف الحراس المتعاقدين مباشرة من قبل المنظمة. فيما يلي بعض مزايا وعيوب العمل مع الحراس المتعاقدين.

المزايا

- غالباً ما يتقاضى الحراس أجورًا أعلى لأن أموال منظمة المساعدة ليست للربح التجاري.
- يزاد ولاء الحراس باعتبارهم أعضاء في هيئة العاملين، وتتوطد معرفتهم بمعايير المنظمة وسياساتها وقواعدها السلوكية.

العيوب

- تتحمل المنظمة المسؤولية الكاملة عن توظيف الحراس المتعاقدين وتدريبهم وتوفير الزي الرسمي والمعدات والإدارة والإشراف عليهم.
- لا يوجد دعم إضافي متاح للمساعدة في إدارة الحارس المتعاقد.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

المتطوعون المجتمعيون

المتطوعون المجتمعيون هم عادة الحراس الذين يوفرهم المجتمع المضيف في المناطق المعنية بالبرنامج. غالبًا ما يكونوا الخيار الأوحد في المناطق النائية. عادة ما تغطي المنظمة تكلفة الرواتب والتدريب والحد الأدنى من المعدات. فيما يلي بعض مزايا وعيوب العمل مع المتطوعين المجتمعيين.

المزايا

توظيف حراس محليين يدعم نهج "استراتيجية القبول" من خلال دمج المجتمع مع إدارة المخاطر الأمنية.

العيوب

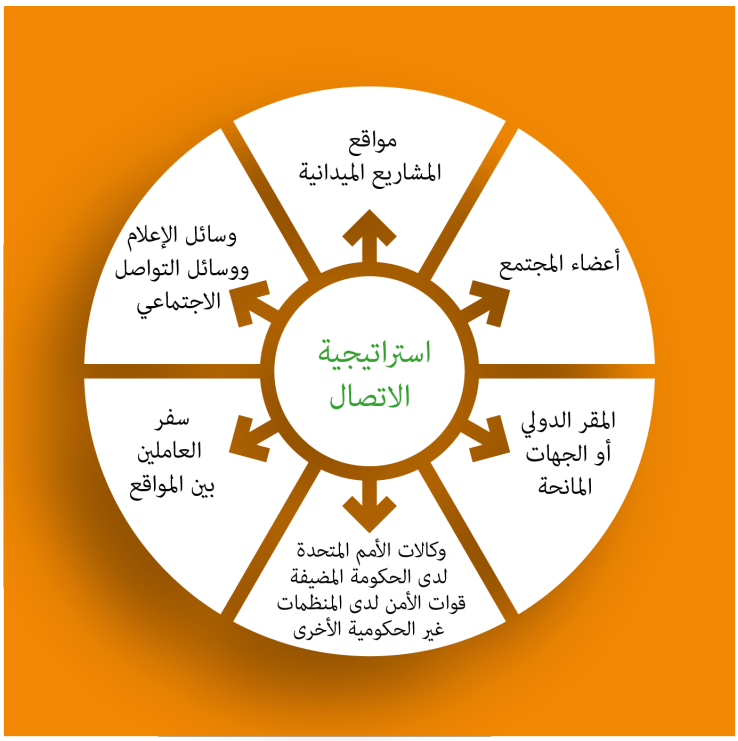
- لا توجد معايير محددة للواجبات.
- انعدام المحاسبة.
- معرّض لإساءة استخدام السلطة وسوء السلوك.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

أمن الاتصالات والمعلومات

تخطيط استراتيجية الاتصال الخاصة بك

عند إعداد أي نشر أو برنامج جديد، من المهم تحديد أنواع الاتصالات التي ستكون متاحة (مثل الخط الأرضي، شبكات الهاتف المحمول، الهواتف الفضائية (المتصلة بالأقمار الصناعية)، الإنترنت، البريد السطحي، البريد السريع) ومدى موثوقيتها في بيئة التشغيل الخاصة بك. في العالم الحديث، يُعتبر التواصل حاجة أساسية للنجاة مثل الطعام والماء والمأوى. اعتبر ما ستحتاجه للتواصل بفعالية مع مختلف العاملين والشركاء والجهات المعنية الرئيسية كجزء من تخطيط استراتيجية الاتصال لديك.



حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

أعضاء المجتمع

- المشاركة
- بناء القبول
- التخطيط
- الاستشارة

مواقع المشاريع الميدانية

- إدارة البرنامج
- تقارير السلامة
- تقارير سير العمل
- التنسيق
- المتابعة والتقييم
- صحة العاملين ورفاهيتهم

وسائل الإعلام ووسائل التواصل الاجتماعي

- نشر القصص
- معلومات حول جمع التبرعات
- إدارة التوقعات
- التحكم في الرسائل
- مخاطر السمعة

سفر العاملين بين المواقع

- الإبلاغ عن التأخير ومشكلات المركبات
- السلامة والأمن أثناء السفر
- الأعطال والحوادث
- تأخيرات السفر
- قضايا السلامة على الطريق

وكالات الأمم المتحدة لدى الحكومة المضيفة

- التنسيق
- رسائل الطوارئ
- الإبلاغ عن الحوادث

قوات الأمن لدى المنظمات غير الحكومية الأخرى

- التفاوض على الوصول
- طلب الدعم

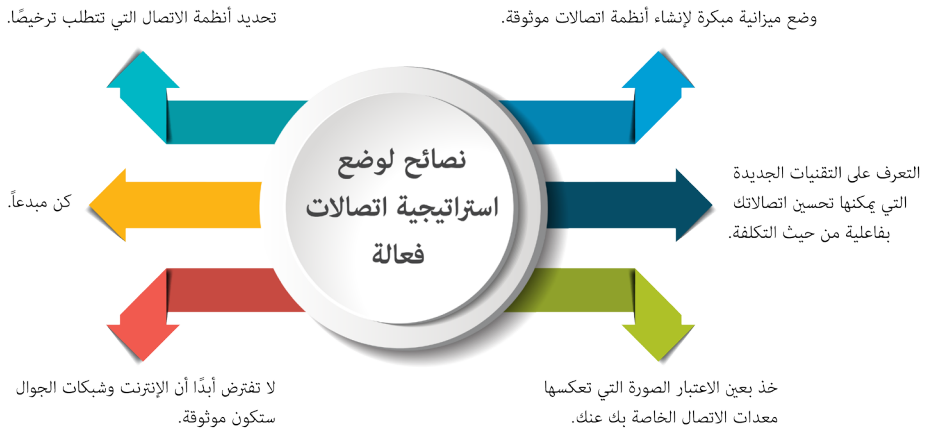
المقر الدولي أو الجهات المانحة

- تقديم التقارير
- إدارة الأزمة
- متطلبات المانحين
- مقترحات التمويل
- تقييمات البرنامج

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

نصائح لوضع استراتيجية اتصالات فعالة

اتبع هذه النصائح لوضع استراتيجية اتصال فعالة لمنظمتك والشركاء والعاملين.



وضع ميزانية مبكرة لإنشاء أنظمة اتصالات موثوقة. يجب أن يكون لديك أنظمة احتياطية وأنظمة بديلة لاستبدال المعدات التالفة أو المفقودة أو المسروقة.

التعرف على التقنيات الجديدة التي يمكنها تحسين اتصالاتك بفاعلية من حيث التكلفة. قد يشمل ذلك "حزم" الأقمار الصناعية للهواتف الذكية أو أنظمة المراسلة عبر الأقمار الصناعية بدلاً من الهواتف الصوتية التقليدية. قم بشراء الأفضل قدر استطاعتك.

خذ بعين الاعتبار الصورة التي تعكسها معدات الاتصال الخاصة بك عنك. إذا كان وجود ملف تعريف منخفض جزءًا من استراتيجيتك الأمنية، فإن إضافة أجهزة لاسلكية وهوائيات عالية التردد (HF) إلى المركبات سيجعلك أهلًا لتمثيل المنظمة.

لا تفترض أبدًا أن الإنترنت وشبكات الجوال ستكون موثوقة. أثناء حالات الطوارئ الأمنية أو الصراعات أو الاضطرابات المدنية أو بعد الكوارث الطبيعية، غالبًا ما تتحكم الحكومات في الشبكات أو تغلقها في الوقت الذي تكون أنت في أمس الحاجة إليها. لذلك لا تعتمد فقط على نظام واحد سواء كان خط أرضي أو شبكات جوال أو هواتف متصلة بالأقمار الصناعية أو الإنترنت أو أي من الأنظمة الأخرى.

كن مبدعاً. في حالات الطوارئ تحتاج المنظمات إلى طرق بديلة للتواصل مع العاملين البعيدين والمجتمعات البعيدة إذا تعطلت الهواتف أو الإنترنت. تتضمن بعض الطرق الإبداعية استخدام سائقي سيارات الأجرة وحتى راكبي الجمال لتوصيل الرسائل إلى الآخرين.

تحديد أنظمة الاتصال التي تتطلب ترخيصًا. قد تتطلب أنظمة الراديو أو الأقمار الصناعية ترخيصًا للعمل. وقد تكون الأمم المتحدة قادرة على تقديم الدعم للحصول على هذه التراخيص. يجب أن تضع منظمتك ميزانية لوقت البث أو الحصول على الترخيص، أو كليهما معًا، عند الضرورة.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

نصائح لأمن الاتصالات وإجراءاتها

اتبع هذه النصائح حول كيفية إنشاء شبكة اتصالات واسعة النطاق وصيانتها لضمان سلامة وأمن ونجاح العمليات.

درّب العاملين على كيفية استخدام الشبكات اللاسلكية أو الهواتف الفضائية (إذا كانت متوفرة) كجزء من استقراءهم. قم باطلاعهم على أماكن استخدام المعدات في بيئة عملهم (الداخلية والخارجية) ومعالجة أي تحديات (أماكن مبهمة).

تأكد من قدرة العاملين على التواصل مع العائلة والأصدقاء أثناء عمليات الانتشار، خاصة في حالات الطوارئ.

استخدم التطبيقات الاجتماعية لمشاركة المعلومات في الوقت الفعلي مباشرة بين الموظفين (مثل واتساب وتلجرام). قم بوضع إرشادات واضحة بشأن المعلومات التي يمكن أو لا يمكن مشاركتها في هذه التطبيقات، والإجراءات التي يجب اتباعها للتصرف بناءً على المعلومات الواردة.

أبلغ الموظفين بجميع إجراءات الاتصال والقواعد الإرشادية. قم بإتاحة الإجراءات المكتوبة ومعلومات الاتصال الأساسية في حالات الطوارئ، بما في ذلك أرقام الهواتف والترددات وإشارات الاتصال، في المكتب لكل مركبة وعلى بطاقة يحملها كل موظف.

قم باختبار أنظمة ومعدات الاتصالات بانتظام واحصل على إمدادات طاقة احتياطية لشحن الراديو والهاتف المحمول أو الهاتف الفضائي (الذي يعمل على القمر الصناعي).

قم بتوجيه الموظفين لضرورة عدم إرسال معلومات حساسة بلغة واضحة عبر شبكات الراديو أو الهاتف (مثل تحويل الأموال أو خطط السفر).

احصل على موافقة من حكومة الدولة المضيفة والترخيص قبل استخدام معدات الاتصالات، والتي من بينها أجهزة الراديو والهواتف الخلوية وهواتف الأقمار الصناعية.

الحصول على ترددات VHF و HF متعددة لأجهزة الراديو لكل مكتب إذا أمكن. التنسيق مع منظمات أخرى مثل الأمم المتحدة لاستخدام شبكات الراديو الخاصة بهم.

القيام بإجراء فحوصات روتينية للرسائل القصيرة أو المكالمات الهاتفية عبر الأقمار الصناعية أو الراديو مع المكاتب البعيدة والمسافرين في المنطقة (حسب الاقتضاء).

تطبيق سياسة محددة عندما يفشل أحد العاملين أو إحدى الفرق في تسجيل الوصول وكان من الصعب الاتصال به. تأكد من أن جميع الموظفين على دراية بهذه السياسة ونفّذها.

إنشاء كلمات أو عبارات تحمل رمزًا للضغط يستخدم عند الطوارئ الشائعة (مثل الاختطاف أو التطفل) وأبلغ الموظفين بهذه الرموز.

مراقبة أجهزة الراديو وهواتف الطوارئ على مدار الساعة (حسب الاقتضاء).

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

نصائح لأمن المعلومات

لا تعتبر منظمات العون والتنمية الدولية كيانات محايدة ومستقلة دائمًا. إنهم يتدخلون ويحاسبون ويدافعون، وغالبًا ما يمارسون الأنشطة المرتبطة عادةً بالحكومات مثل الرعاية الصحية والمياه والصرف الصحي والإغاثة في حالات الطوارئ. وفي كثير من الظروف يمارسون بهذه الأنشطة بينما يتم تمويلهم من قبل الحكومات "الغربية" بأجنداتها السياسية الخاصة. مما يجعل عمل المنظمات الإنسانية يبدو مريباً بنظر البعض.

اتبع هذه النصائح للمساعدة في تقليل تعرض منظمتك لمخاطر أمن المعلومات.

احذر من أي شيء تكتبه أنت أو زملائك في بريد إلكتروني، قد يقرأه المجرمين أو الوكلاء الحكوميون. تستطيع الحكومات مراقبة المكالمات الهاتفية للمنظمات الأخرى، وكذلك نشاط الإنترنت ووسائل التواصل الاجتماعي، وقد تكون لديها القدرة على اختراق محركات الأقراص الصلبة لأجهزة الحاسب الآلي.

كن على دراية بأن المنظمات الإجرامية قد تعتبر منظمتك "هدفًا رائعًا" بناءً على استخدامك للمركبات وأجهزة الكمبيوتر المحمولة والهواتف التي تعمل عبر الأقمار الصناعية، فضلاً عن مستويات التمويل المعلنة من الجهات المانحة.

امنع العاملين من حفظ المعلومات الشخصية والحساسة على مساحة القرص المشترك الخاص بمنظمتك. يمكن أن تتضمن بياناتهم الصور غير اللائقة والمعلومات الشخصية وتحليل السياق، وقد يساء فهم تلك البيانات أو اعتبارها مهينة من قبل العاملين الآخرين.

حدّد نوع المعلومات التجارية والشخصية الآمنة وغير الآمنة لتميز المعلومات التي يمكن الاحتفاظ بها على الأجهزة المحمولة مثل الهواتف الذكية والتي يمكن فقدانها أو سرقتها بسهولة.

قم بتقييم معلومات التأثير إذا كانت تصل إلى الأشخاص غير المرغوب فيهم، مثل مضايقة العاملين أو نشر الصور غير اللائقة أو الوصول إلى رسائل البريد الإلكتروني أو VPN/خادم المكتب.

احتفظ بنسخة احتياطية من جميع الملفات بانتظام والاحتفاظ بنسخ احتياطية لجميع المستندات والسجلات الرئيسية (الاتفاقيات الحكومية والمستندات القانونية والسجلات المصرفية وسجلات الموارد البشرية) خارج الموقع تحسبًا لحالات الطوارئ مثل نشوب الحرائق أو الفيضانات أو السرقة أو غيرها من الحوادت التي يمكن أن تدمر النسخ الأصلية.

استخدم أجهزة تمزيق الملفات لأي ملفات لا يتم تخزينها في مكان آمن.

لا تترك المستندات الورقية في صناديق القمامة أو على المكاتب. قد يسمح ذلك بتسرب المعلومات إذا تم تركها لعمال النظافة وغيرهم من العاملين أو الزوار الذين قد يتمكنوا من رؤيتها أو نسخها أو إزالتها.

حافظ على أنظمة جدار الحماية الأمنية الجيدة على أي خادم.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation

قلّل من قدرة وصول العاملين إلى الشبكات التي تحتوي على أجهزة كمبيوتر أو أجهزة لوحية أو هواتف غير تابعة للمنظمة لمنع انتشار الفيروسات في الأجهزة.

قم بإعداد عمليات التحقق من المعلومات التي يتم إرسالها عبر واتساب والتطبيقات الاجتماعية الأخرى التي تسهّل مشاركة المعلومات بشكل مباشر بين الموظفين. يجب أن توجد إرشادات واضحة حول ما يجب وما لا يجب مشاركته.

تذكر أن برنامج المراسلة مثل سكايب ليس آمنًا من القرصنة.

قم بوضع سياسة للتحكم في وسائل التواصل الاجتماعي توضح للموظفين ما يمكنهم وما لا يمكنهم نشره على مواقع التواصل الاجتماعي.

تجنب الاتصالات التي قد تجعلك تبدو وكأنك تقوم بجمع "معلومات استخبارية" أو تمرير أي معلومات عسكرية أو أمنية إلى حكومات أجنبية أو مانحين أو مقر منظمتك غير الحكومية.

تجنب تشفير المعلومات كلما أمكن ذلك حيث قد يفهم العاملون والشركاء ذلك على نحوٍ خاطئ، خاصة إذا ادعت منظمتك غير الحكومية أنها مفتوحة وخاضعة للمساءلة. قد يتم استجوابك حول حاجتك إلى تشفير الوثائق.

تجنب أجهزة الكمبيوتر المكتبية كلما أمكن. على الرغم من أن سرقة أجهزة الكمبيوتر المحمولة أسهل، إلا أنها أسهل في النقل إذا احتاج المكتب أو المشروع إلى الانتقال.

حقوق النشر 2020 © مؤسسة Cornerstone OnDemand Foundation