

لائحة تحقّق: أمن المكتب

لا يُراد بلائحة التحقّق هذه أن تكون نموذجاً يُتَّبَع في موقفكم الأمني. إنَّ سياقكم المخصوص هو العامل الأساسي في تحديد ما يتعيّن اتخاذه من إجراءات. يتعيّن أن تأخذوا في الحسبان ما تواجهونه من تهديدات، وما قد يكون لديكم من نقاط الضعف، لتضيفوا على هذه اللائحة ما هو ضروري، وتجعلوها أكثر ملاءمة لوضعكم.

١. الاتصالات التي تُستخدم في حالات الطوارئ:
 - هل هناك قائمة محدّثة و قريبة المتناول تتضمن أرقام الهاتف و عناوين المنظمات المحلية غير الحكومية الأخرى، و المستشفيات، و الشرطة، و جهاز الإطفاء، و خدمات الإسعاف؟
٢. الحواجز التقنية و المادية (الخارجية منها و الداخلية)
 - تحققوا من حالة و أداء البوابات الخارجية / الأسيجة، أبواب المبنى، النوافذ، الجدران، و السطح.
 - تحققوا من حالة و أداء الإنارة الخارجية، و أجهزة الإنذار، و آلات التصوير، و أجهزة التصوير الفيديوي للمدخل.
 - تحققوا من الإجراءات الأساسية، بما في ذلك أن تكون المفاتيح معرّفة على نحو آمن و مرمّز، و إناطة المسؤولية عن الإشراف على المفاتيح و نسخها بشخص معيّن، و أن تكون المفاتيح و نسخها في وضع جيد. تأكّدوا من أن يتم تغيير الأقفال عندما تضيع المفاتيح أو تتعرض إلى السرقة، و أن يتم تسجيل مثل هذه الوقائع في سجل الحوادث.
 - هل لديكم غرفة خاصة آمنة؟
 - هل يمكن أن يتم إنزال اللافتة التي تشير إلى اسم منظمكم في أوقات تزايد التهديدات من أجل الحد من مدى تعرّضكم إلى المخاطر؟

٣. العاملون في المكتب:

- هل تقومون بتوظيف الأشخاص الموثوق بهم حصراً، بما في ذلك الحراس، و تنظرون في رسائل التوصية التي يحملونها؟
- هل يتم تدريب جميع العاملين في المنظمة على الخطط الأمنية ذات الصلة؟
- هل لديكم خطة لاستخدامها في حال عمدت السلطات أو سواها من الجماعات إلى مدهامة المكتب؟
- هل تنفذون سياسة تتعلق بـ ما ينبغي معرفته، بشأن أكثر الأعمال حساسية؟
- هل تقومون بإدانة حوار حسن مع جميع العاملين، و بخاصة إذا علمتم أنهم يعانون مشكلات مالية أو أنهم يتعرضون لضغوط من نوع مختلف؟ (يمكن أن يغدو العاملون المتدمّرون أعداءاً خطرين).
- عندما يترك أحد الموظفين العمل في المنظمة، فهل تقومون بتغيير الإجراءات الأمنية، و كلمات السر، و المفاتيح، على النحو المطلوب؟

٤. إجراءات استقبال الزائرين و نقاط التصفية filters:

- هل يتم تطبيق إجراءات الدخول إلى مقر المنظمة على جميع صفوف الزائرين؟ و هل يدركها جميع العاملين في المنظمة؟
- قوموا بسؤال الموظفين الذين يقومون عادةً بتنفيذ إجراءات الدخول عمّا إذا كانت الإجراءات تعمل كما يجب، و عن التحسينات التي تتطلبها.
- هل يعرف الموظفون ما الذي ينبغي القيام به إذا تلقى المكتب طرداً بريدياً غير متوقع (مثلاً عزله، الامتناع عن فتحه، الاتصال بالسلطات).
- هل تسجّلون أسماء الزائرين (بمن فيهم هؤلاء الذين يحضرون اجتماعات في مكتبكم)؟ إذا كان الأمر كذلك، فهل هذه المعلومات حساسة، و كيف تقومون بحمايتها؟ (بواسطة الرموز و الملفات المحمية بشيفرة خاصة على سبيل المثال).

٥. أمن المعلومات (أنظر أيضاً الملحق الرابع عشر، المتعلق بأمن أجهزة الحاسوب والهاتف):
- هل تقومون على نحو دوري بإعداد نسخ احتياطية من ملفاتكم، و تحتفظون بها في مكان آمن خارج المكتب؟
 - هل يعرف العاملون أهمية ألا يدعوا المعلومات الحساسة متروكة على مكاتبهم؟
 - هل لديكم نظام آمن لتسجيل المعلومات السريّة، كتلك المتعلقة بالموكلين أو الشهود مثلاً؟
 - هل تمنحون لملفاتكم الحساسة (سواءً أكانت ورقية أو إلكترونية) أسماءً آمنة، بحيث يتعدّر التعرّف عليها بسهولة؟

٦. الأمن في حالات الحوادث:
- تحققوا من حالة مطفآت الحريق، وصمامات الغاز و أنابيبه، و صنابير الماء، و مقابس الكهرباء و كابلاتها و مولداتها (إن وُجدت).

٧. المسؤولية و التدريب:
- هل تمّ تقسيم و تحديد المسؤولية عن أمن المكتب و إناطتها بأشخاص معينين؟ و هل كان ذلك الإجراء فعّالاً؟
 - هل ثمة برنامج تدريبي يتعلق بأمن المكتب؟ و هل يغطي جميع الجوانب التي تضمّنتها هذه المراجعة؟ و هل خضع جميع الموظفين الجدد إلى التدريب؟ و هل التدريب فعّال؟

نقلًا عن، أو بتصرّف عن: دليل الحماية للمدافعين عن حقوق الإنسان، الفصل التاسع، إنريكه إيغورين من فرق السلام الدولية، المكتب الأوروبي؛ الصادر عن مؤسسة الخط الأمامي، 2005.