BLACKBIRD FOR TRAINING

تأمين المنشآت الحيوية والمباني – شهادة IAOSHE

24 October – 4 November 2027

القاهرة (مصر)



تأمين المنشآت الحيوية والمباني – شهادة IAOSHE

المرجع: 326030_3254923 **التاريخ:** 24 October – 4 November 2027 **المكان:** القاهرة (مصر) **الرسوم:** GBP 8800

مقدمة

في عالم يتزايد فيه حجم التهديدات ضد البنية التحتية الحيوية والمرافق الحساسة، أصبحت حماية المنشآت الحيوية أمرًا ضروريًا لضمان استمرارية الأعمال وسلامة المجتمعات. تقدم هذه الدورة الشاملة - تأمين المنشآت الحيوية والمباني - شهادة IAOSHE - المهارات والمعرفة الأساسية لـ مديري الأمن، مسؤولي السلامة، مديري المرافق، وكل من تقع على عاتقه مسؤولية حماية المواقع ذات القيمة العالية أو المخاطر المرتفعة.

تركز الدورة على تقييم التهديدات، تنفيذ التدابير الأمنية المادية والإجرائية، والاستجابة للحوادث بشكل فعّال، وذلك وفقًا لأفضل الممارسات الدولية والمعايير مثل ISO 31000 وASIS. يجمع البرنامج بين الاستراتيجيات العملية ودراسات الحالات الواقعية لتزويدك بخطة أمنية شاملة لحماية المواقع الحيوية.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تحديد وتقييم التهديدات المحتملة التي تستهدف المنشآت الحيوية والبنية التحتية الحساسة.
- تصميم وتنفيذ تدابير الأمن المادي والإجرائي الفعالة والمناسبة للمخاطر الخاصة بكل موقع.
- فهم وتطبيق أحدث التقنيات المستخدمة في كشف التسلل وأنظمة المراقبة.
- التنسيق مع فرق الطوارئ وأصحاب المصلحة الداخليين في حال حدوث أي حادثة.
- إعداد وإدارة خطة شاملة لإدارة الأمن وفقًا للأهداف المؤسسية والمعايير العالمية.



محاور الدورة

اليوم الأول: مقدمة في تأمين البنية التحتية الحيوية

- تعريف المنشآت الحيوية والبنية التحتية الحساسة.
- التهديدات الداخلية مقابل التهديدات الخارجية.
- أهمية إجراء تحليل المخاطر الخاصة بالموقع.
- لمحة عن المعايير التنظيمية مثل ISO 31000 وASIS.
- دور ومسؤوليات مسؤول الأمن في حماية البنية التحتية.

اليوم الثاني: تقييم المخاطر وتحليل نقاط الضعف

- مكونات تقييم التهديدات ونقاط الضعف والتبعات.
- استخدام مصفوفة المخاطر وتقنيات ترتيب الأولويات.
- إجراء عمليات التدقيق الأمني والمسح الميداني للموقع.
- دراسات حالة حول اختراقات أمنية سابقة.
- تطوير ملف التهديدات الخاص بالمنشآت.

اليوم الثالث: تأمين المحيط والتدابير الأمنية المادية

- مبادئ تصميم الأمن المادي.
- الحواجز: الأسوار، البوابات، الحواجز الصلبة.
- أنظمة الدخول والخروج الآمنة وغرف العزل.
- تحسين الإضاءة، اللافتات، ومناطق التحكم في الدخول.
- تقنيات منع المركبات والتسلل.

اليوم الرابع: أنظمة التحكم في الدخول وإدارة الهوية

- أنظمة التحكم في الدخول: بطاقات الوصول، القياسات الحيوية.
- إدارة الزوار والمقاولين بأمان.
- سياسات الوصول حسب الدور وتقسيم المناطق.
- الحواجز المادية مثل البوابات الدوارة وغرف الحجز.
- الأخطاء الشائعة في التحكم بالدخول وطرق معالجتها.



اليوم الخامس: أنظمة المراقبة والرصد

- أفضل ممارسات تخطيط وتركيب أنظمة CCTV.
- أنواع الكاميرات: PTZ، الحرارية، بالأشعة تحت الحمراء، المدعمة بالذكاء الاصطناعي.
- تكامل المراقبة مع أنظمة الإنذار والتحكم بالدخول.
- تصميم غرف التحكم ومراكز المراقبة المركزية.
- استخدام تحليلات الفيديو للكشف الذكي عن التهديدات.

اليوم السادس: الاستجابة للطوارئ وإدارة الحوادث

- تطوير خطط الاستجابة للطوارئ والتنسيق مع الأطراف المعنية.
- بروتوكولات الاستجابة للحرائق، التهديدات بالمتفجرات، والتخريب.
- إجراءات الإبلاغ عن الحوادث وطرق التصعيد.
- أدوار الأمن الخاص، الشرطة، والدفاع المدني.
- محاكاة السيناريوهات وخطط الاتصال.

اليوم السابع: الأمن السيبراني للبنية التحتية المادية

- التقاطع بين الأمن السيبراني والأمن المادي.
- الثغرات الشائعة في أنظمة أتمتة المباني.
- تأمين شبكات SCADA وأنظمة التحكم في الدخول.
- تدريب الموظفين والمقاولين على الوعي الأمني.
- التعاون مع فرق تكنولوجيا المعلومات والأمن السيبراني.

اليوم الثامن: العامل البشري وتقليل التهديدات الداخلية

- أساليب التحقق الأمني وفحص الخلفيات.
- مراقبة سلوك الموظفين والإبلاغ عن الأنشطة المريبة.
- الأخلاقيات، قنوات الإبلاغ الداخلية، والشفافية.
- برامج تدريب وتوعية الموظفين بالأمن.
- أمثلة حقيقية على خروقات أمنية داخلية.



اليوم التاسع: تخطيط الأمن والتوثيق

- تطوير خطة أمنية خاصة بالموقع.
- صياغة السياسات، الإجراءات التشغيلية الموحدة SOPs، وخطط الطوارئ.
- دمج خطط الأمن مع متطلبات الصحة والسلامة ومكافحة الحرائق.
- تحديد أدوار ومسؤوليات أفراد الأمن.
- التعاون مع مديري المرافق وإدارة المخاطر.

اليوم العاشر: دراسات حالة وتدريبات عملية وختام

- مراجعة حوادث عالمية في المنشآت الحيوية.
- مشروع جماعي: تصميم خطة أمنية لمنشأة حساسة.
- إجراء تدريبات عملية ومحاكاة للحوادث.
- مناقشة مفتوحة: التحديات وأفضل الممارسات.
- تقديم الشهادات وختام الدورة.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات

- اكتساب معرفة عملية قابلة للتطبيق: تعلم كيفية تحديد، تقييم، وتقليل التهديدات على المنشآت الحيوية.
- تعزيز المهارات الأمنية: تدريبات عملية لتطبيق أفضل ممارسات الأمن المادي والتحكم في الدخول.
- الاستفادة من أحدث التقنيات: التعرف على أحدث أدوات كشف التسلل والمراقبة.
- تنسيق فعّال للاستجابة: إتقان إدارة الحوادث بالتعاون مع فرق الطوارئ والأطراف الداخلية.
- تطوير خطة أمنية شاملة: تصميم خطة متكاملة متوافقة مع المعايير الدولية مثل ISO 31000.
- التعلم من دراسات حالة حقيقية: تطبيق الخبرات المكتسبة على سيناريوهات حقيقية.
- تعزيز مكانتك المهنية: الحصول على شهادة معترف بها من IAOSHE لتعزيز مسارك المهني.
- استعداد لمواجهة التهديدات المستقبلية: تجهيز نفسك لمواجهة التحديات المتغيرة في أمن البنية التحتية الحيوية.

الخاتمة

إن حماية المنشآت الحيوية والمرافق الحساسة ضروري لضمان استمرارية العمل وسلامة المجتمع. تقدم لك هذه الدورة المعتمدة من IAOSHE المهارات والخبرات العملية لتصميم وتنفيذ وإدارة خطة أمنية شاملة ومتكاملة.

سواء كنت مدير أمن، قائد فريق سلامة، أو مسؤول عن حماية المواقع الحساسة، تمنحك هذه الدورة الأدوات والثقة لتكون جاهزًا لمواجهة التهديدات الحالية والتحديات المستقبلية. ابدأ رحلتك اليوم نحو بناء مؤسسة أكثر أمانًا واستدامة!

