المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

أمن المعلومات الإلكترونية في شبكة الجمارك

فكرة الدورة

أصبحت شبكات المعلومات في المؤسسات الجمركية عنصرًا أساسيًا في إنجاز المعاملات، وتبادل البيانات، ودعم القرارات التشغيلية والرقابية. ومع تزايد الاعتماد على الأنظمة الإلكترونية، تبرز الحاجة إلى رفع مستوى الوعي بأمن المعلومات، وحماية البيانات من الاستخدام غير المصرح به، وتقليل المخاطر المرتبطة بالأخطاء البشرية أو التهديدات التقنية.

يركز هذا البرنامج التدريبي من AINFCT على المفاهيم الأساسية لأمن المعلومات الإلكترونية في بيئة العمل الجمركي، مع توضيح مسؤوليات المستخدمين، وضوابط الوصول، وحماية كلمات المرور، والتعامل الآمن مع البريد الإلكتروني والملفات والأنظمة الداخلية. كما يتناول البرنامج مبادئ السرية والسلامة والتوافر، وربطها بسلوكيات عملية داخل بيئة الشبكة المؤسسية.

يمنح البرنامج المشاركين أساسًا مهنيًا واضحًا للتعامل الآمن مع المعلومات، بما يدعم استمرارية العمل ويعزز الثقة في الخدمات الإلكترونية الجمركية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- فهم مبادئ أمن المعلومات الإلكترونية.
- تمييز التهديدات الشائعة داخل الشبكات.
- تطبيق ممارسات الاستخدام الآمن للأنظمة.
- حماية البيانات الجمركية الحساسة.
- التعامل السليم مع الحوادث الإلكترونية.
- تعزيز الالتزام بسياسات أمن المعلومات.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة من بيئات العمل.
- تمارين عملية على مواقف إلكترونية شائعة.
- تحليل سيناريوهات لحوادث أمن معلومات.
- نقاشات جماعية حول السلوكيات الآمنة.
- قوائم تحقق قابلة للاستخدام بعد التدريب.

أثر الدورة على المنظمة

يمكن تعزيز جودة الأداء المؤسسي في هذا المجال من خلال:

- تقليل مخاطر تسرب البيانات المؤسسية.
- رفع جاهزية المستخدمين ضد التهديدات الإلكترونية.
- تعزيز موثوقية الأنظمة والخدمات الرقمية.
- دعم الالتزام بضوابط أمن المعلومات.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على تطوير قدراتهم العملية من خلال:

- استخدام الشبكات المؤسسية بوعي أمني.
- اكتشاف مؤشرات الخطر الإلكتروني مبكرًا.
- تطبيق ضوابط حماية الحسابات والملفات.
- الإبلاغ عن الحوادث بطريقة صحيحة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج الموظفين الذين يستخدمون الأنظمة والشبكات الإلكترونية في إنجاز الأعمال الجمركية اليومية. كما يفيد المشرفين الراغبين في رفع مستوى الوعي الأمني داخل فرق العمل.

- موظفو الإدارات الجمركية والتشغيلية.
- مستخدمو الأنظمة والشبكات المؤسسية.
- مشرفو الوحدات الإدارية والرقابية.
- موظفو الدعم الفني وخدمات المستخدمين.
- العاملون في إدارات الوثائق والمعلومات.

موضوعات الدورة

اليوم الأول: مدخل إلى أمن المعلومات في البيئة الجمركية

- مفهوم أمن المعلومات وأبعاده الأساسية.
- أهمية حماية البيانات في العمل الجمركي.
- مبادئ السرية والسلامة والتوافر.
- أنواع المعلومات الحساسة داخل الشبكات.
- مسؤوليات المستخدمين في حماية الأنظمة.
- الأخطاء الشائعة في التعامل مع المعلومات.

اليوم الثاني: المخاطر والتهديدات الإلكترونية الشائعة

- البرمجيات الخبيثة ورسائل التصيد الإلكتروني.
- مخاطر الروابط والمرفقات غير الموثوقة.
- الهندسة الاجتماعية وأساليب الخداع الرقمي.
- مخاطر استخدام الأجهزة والوسائط الخارجية.
- المؤشرات المبكرة للحوادث الإلكترونية.
- تقييم السلوكيات اليومية عالية الخطورة.

اليوم الثالث: الاستخدام الآمن للأنظمة والشبكات

- إدارة كلمات المرور وحسابات المستخدمين.
- ضوابط الدخول والصلاحيات داخل الشبكة.
- حماية البريد الإلكتروني والمراسلات الرسمية.
- التعامل الآمن مع الملفات والمجلدات المشتركة.
- الاستخدام المهني للإنترنت داخل العمل.
- مبادئ النسخ الاحتياطي وحفظ البيانات.

اليوم الرابع: سياسات أمن المعلومات والاستجابة للحوادث

- أهمية السياسات والإجراءات الأمنية الداخلية.
- تصنيف البيانات وتحديد مستويات السرية.
- خطوات الإبلاغ عن الحوادث الإلكترونية.
- حفظ الأدلة الأولية عند وقوع الحوادث.
- التنسيق مع فرق تقنية المعلومات.
- مواءمة الممارسات مع مبادئ ISO/IEC 27001.

اليوم الخامس: التطبيق العملي وتعزيز الثقافة الأمنية

- تمارين على كشف رسائل التصيد الإلكتروني.
- تحليل سيناريوهات اختراق أو تسرب بيانات.
- إعداد قائمة تحقق للاستخدام الآمن.
- مراجعة السلوكيات الفردية داخل الشبكة.
- بناء خطة تحسين شخصية للوعي الأمني.
- قياس جاهزية المشاركين للتطبيق العملي.

course_daily_schedule

يمتد البرنامج على خمسة أيام تدريبية، بواقع أربع ساعات يوميًا. يبدأ كل يوم بعرض المفاهيم الأساسية، ثم ينتقل إلى التمارين التطبيقية ودراسة الحالات. ويُختتم اليوم التدريبي بمراجعة مركزة تربط المفاهيم بممارسات العمل اليومية داخل الشبكة المؤسسية.

course_assessment

يعتمد تقييم المشاركين على التفاعل أثناء الجلسات، والمشاركة في التمارين العملية، وتحليل السيناريوهات التدريبية، إضافة إلى إعداد قائمة تحقق للاستخدام الآمن للمعلومات. يحصل المشاركون الذين يستكملون متطلبات الحضور والمشاركة على

شهادة إتمام أو حضور صادرة من AINFCT.

course_key_competencies

- الوعي بأمن المعلومات.
- حماية البيانات الحساسة.
- الاستخدام الآمن للشبكات.
- إدارة مخاطر المستخدم.
- الاستجابة الأولية للحوادث.
- الالتزام بالسياسات الأمنية.

مكتب القاهرة الرئيسي

القاهرة، جمهورية مصر العربية

7 شارع وهران، الطيران، مدينة نصر

+201152466358

info@ainfct.com

ainfct.com

رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد

training@ainfct.com

ainfct.com