€TRAINING

الاستراتيجيات الإدارية في أمن المعلومات

الاستراتيجيات الإدارية في أمن المعلومات

مقدمة عن البرنامج التدريبي:

نظام إدارة أمن المعلومات "ISMS" هو مجموعة من السياسات المعنية بإدارة أمن المعلومات أو أنها ذات صلة بالمخاطر المتعلقة بالمعلومات، والمبدأ الذي يحكم نظام إدارة أمن المعلومات هو أن المنظمة ينبغي عليها تصميم وتنفيذ والحفاظ على مجموعة مترابطة من السياسات والعمليات ونظم إدارة المخاطر لأصولها في مجال المعلومات الخاصة بها، وبالتالي ضمان مستويات مقبولة من مخاطر أمن المعلومات. ترفد هذه الدورة المشاركين بالمعرفة المتعمقة والمهارات العملية اللازمة للتخطيط والتقديم ومراقبة تكنولوجيا وأمن المعلومات للعملاء الداخليين والخارجيين لتشمل مجموعة كاملة وشاملة للتخصصات في مجالات سياسات تكنولوجيا المعلومات وكتاب إدارة الأمن التشغيلي واختبار الأمن / الاختراق والقرصنة الأخلاقية وقراصنة القبعة السوداء. تغطي أيضاً هذه الدورة أمن الـ" WIFI" وأمن الموقع الالكترونية والعوامل البشرية والأمن الجنائي وإدارة الفرق الأمنية ومركز العمليات الآمنة "SOC" وفرق الاستجابة لحوادث أمن الحاسب الآلي "CSIRT" وتتضمن الدورة جلسات عملية وأشرطة الفيديو وأمثلة عن الفيروسات وأدوات القرصنة البيضاء والسوداء. كما يتم تزويد جميع المشاركين بأحدث الأبحاث والمقالات. وكجزء من الدورة، يقوم المشاركون بإجراء تقييم المخاطر لمنشورين مختلفين استنادا إلى الأيزو "27001" الذي يحدد أي تهديدات مباشر أو غير مباشر والتعرضات الأمنية أو احتمال وجود نقاط ضعف، ويقوم المشاركون بالتعامل مع مثال في الأمن والتعرف على أفضل الممارسات التي يمكن تطبيقها لتأمين مؤسساتهم والأصول المرتبطة بها.

أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

- تطبيق معايير أمن المعلومات لمنظمتهم وأصولها الحرجة.
- التعرف على التهديدات التي تسببها الفيروسات والبرمجيات الخبيثة والرموز النشطة والتهديدات المستمرة النشطة " APT" والنظر في مختلف الخيارات المقللة.
- صياغة وإدارة فرق الأمن الالكترونية الفعالة وتطبيق إطار فريق الاستجابة لحوادث أمن الحاسوب "CSIRT" والأدوات والقدرات اللازمة لتحقيق الفعالية من حيث التكلفة وحلول قوية لحماية المنظمة.
- استخدام البرمجة اللغوية العصبية "NLP" لتسليم رسائل من شأنها أن تغير طريقة عمل الموظفين والتفكير الآمن.
- فحص مجالات بروتوكولات أمن الشبكات اللاسلكية وخصائصها الأمنية وانعدام الأمن المحتملة داخل المنظمة وفي الأماكن العامة.
- معرفة كيفية اختبار الاختراق والقرصنة الأخلاقية لتعزيز الأمن التنظيمي.
- تقييم الأمن الحديث: المصادر المفتوحة الذكية "OSINT" و طفرات الذكاء الصناعي.

الفئات المستهدفة:

- المختصون في تكنولوجيا المعلومات ومجال الأمن والتدقيق.
- المسؤولون عن المواقع والإدارة العامة.
- أي شخص مكلف بإدارة وحماية سلامة البنية التحتية للشبكات الالكترونية.
- كل من هو على دراية بتكنولوجيا المعلومات/ الإنترنت/ الأمن الرقمي.

محاورالبرنامج التدريبي:

الوحدة الأولى:

info@euro-training.net
+447447999485 - +447492882996

عصر تكنولوجيا المعلومات:

- خصائص وعناصر وتوجهات الإدارة الإلكترونية.
- الأنظمة الإلكترونية اللازمة للإدارة الإلكترونية.
- سمات الإدارة الإلكترونية وعناصرها وتوجهاتها.
- خصائص الإدارة الإلكترونية وإمكانية تنفيذ المعاملات إلكترونياً.

الوحدة الثانية:

عناصر الإدارة الإلكترونية:

- إدارة بدون ورق.
- إدارة بلا تنظيمات جامدة.
- إدارة بلا مكان.
- إدارة بلا زمان.
- ما هي مواصفات مدير المكتب والسكرتير الإلكتروني؟

الوحدة الثالثة:

أمن الوثائق والمستندات:

- التطور التاريخي لعلم أمن المعلومات.
- سياسات أمن المعلومات.
- وضع وتطوير استراتيجية أمن المعلومات في مواجهة الأخطار المحتملة.
- المفاهيم الأساسية في إدارة أمن المعلومات.
- المراحل الأمنية لأمن الوثائق والمستندات.
- مرحلة إنشاء الورقة الرسمية.
- مرحلة حفظها وتأمينها.
- مرحلة التداول والاطلاع.
- مرحلة إعدام الورقة الرسمية.
- بعض أساليب حماية البيانات.

الوحدة الرابعة:

تكنولوجيا توثيق المعلومات:

- الأرشفة الإلكترونية
- مفهوم نظام معالجة الوثائق الآلية
- طرق حفظ الملفات
- تصنيف وفهرسة الملفات
- الأهداف الاستراتيجية للأرشفة الإلكترونية
- أهداف الأرشفة الإلكترونية داخل المنظمة
- إيجابيات وسلبيات الحفظ الإلكتروني للمعلومات .
- كيف يعمل نظام معالجة الوثائق والملفات
- مميزات نظام معالجة الوثائق والملفات الآلي.

الوحدة الخامسة:

تحويل أرشيف ورقي إلى أرشيف الكتروني:

- حالة عملية في مجال التوثيق والأرشفة الإلكترونية.
- الاشتراطات الأمنية للعاملين.
- تطبيقات الحاسب الآلي وسرية المعلومات.

- تطبيقات أمن الوثائق والمستندات.
- حماية البيانات من خلال مجموعة البرامج المكتبية.
- أساليب الحفظ الاحتياطي.
- تشفير البيانات.
- حماية البريد الإلكتروني.
- الفيروسات والقرصنة الإلكترونية ونظم وبرامج الحماية.
- أوجه القصور الأمني في مجال الوثائق والمستندات.