مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

أمن المعلومات وحماية البيانات في المؤسسات الحكومية

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 08 – 12 / 06 / 2025.

مقدمة :

تُشكل المعلومات و البيانات أصولًا حيوية لِلمؤسسات الحكومية، حيث تُستخدم في جميع العمليات و الخدمات و تُساهم في اتخاذ القرارات و تطوير السياسات .و تتطلب حماية هذه الأصول من الضياع أو السرقة أو التلف بناء نُظم فعّالة لِأمن المعلومات و تطبيق أفضل الممارسات في هذا المجال.

يهدف هذا البرنامج التدريبي إلى تزويد المشاركين بالمعرفة و المهارات اللازمة لِحماية المعلومات و البيانات في المؤسسات الحكومية بِكفاءة و فعالية .سيركز البرنامج على استعراض مجموعة واسعة من المواضيع، مثل مبادئ أمن المعلومات و أنواع التهديدات)بما فيها الهجمات السيبرانية و الأخطاء البشرية(، و تقنيات الحماية و الوقاية)مثل التشفير و جدران الحماية(، و إدارة الأزمات و الاستجابة للحوادث، و التعاون و تبادل المعلومات بين المؤسسات الحكومية .كما سيتناول البرنامج أفضل الممارسات في مجال حوكمة أمن المعلومات و إدارة المخاطر، و كيفية بناء فرق استجابة للحوادث فعّالة، و تطوير الكوادر الوطنية في هذا المجال .و سيُقدم البرنامج أيضًا تمارين محاكاة و دراسات حالة واقعية لتعزيز فهم المشاركين و تطبيق المعارف المكتسبة في بيئات عمل مُحاكية.

أهداف الورشة:

- فهم مبادئ أمن المعلومات و أهميته في حماية المؤسسات الحكومية .
- التعرف على مختلف أنواع التهديدات و المخاطر التي تُهدد المعلومات و البيانات .
- إتقان مهارات الحماية و الوقاية من التهديدات و تطبيق أفضل الممارسات الأمنية .
- إدارة الأزمات و الاستجابة للحوادث الأمنية بِكفاءة و فعالية لِتقليل الضرر .
- تطبيق أفضل الممارسات في مجال حوكمة أمن المعلومات و إدارة المخاطر .
- بناء فرق استجابة للحوادث فعّالة و قادرة على التعامل مع التهديدات بِسرعة .
- تعزيز التعاون و تبادل المعلومات بين المؤسسات الحكومية لِمواجهة التهديدات بِشكل مُشترك.

محتويات الورشة:

اليوم الأول:

مُقدمة في أمن المعلومات و حماية البيانات

- مبادئ أمن المعلومات و أهميته في العصر الرقمي و علاقته بِالأمن الوطني.
- مفهوم حماية البيانات و أهم التشريعات و القوانين ذات الصلة)مثل قوانين الخصوصية.(
- أنواع التهديدات و المخاطر)الهجمات السيبرانية، الأخطاء البشرية، الكوارث الطبيعية.(
- ورشة عمل :تحديد الأصول و البيانات الحرجة في مؤسسة حكومية و تقييم مستوى حمايتها.

اليوم الثاني:

التهديدات السيبرانية و أساليب الهجوم

- أنواع الهجمات السيبرانية)البرمجيات الخبيثة، هجمات الحرمان من الخدمة، التصيد الاحتيالي.(
- أساليب الهجوم السيبراني و تقنيات الاختراق)الهندسة الاجتماعية، ثغرات الأمن السيبراني.(
- أمثلة على هجمات سيبرانية على مؤسسات حكومية و دراسة أسباب نجاحها و نتائجها.
- تمرين محاكاة :تحليل هجوم سيبراني و تحديد أساليب الهجوم المُستخدمة و كيفية اختراق الأنظمة.

اليوم الثالث:

الحماية و الوقاية من التهديدات

- تقنيات و أدوات الحماية من التهديدات)التشفير، جدران الحماية، أنظمة كشف التسلل.(
- أمن الشبكات و الخوادم و قواعد البيانات و التطبيقات و الأجهزة المُتصلة.
- أمن البيانات و تشفيرها و إدارة الهويات و التحكم في الوصول و النسخ الاحتياطي.
- ورشة عمل :تطبيق تقنيات الحماية و الوقاية على نظام مُحاكى لِمنع هجمات سيبرانية مُختلفة.

اليوم الرابع:

إدارة الأزمات و الاستجابة للحوادث

- مراحل إدارة الأزمات و خطوات الاستجابة)الكشف، الاحتواء، التحقيق، المعالجة، التعافي.(
- خطط الاستجابة للحوادث الأمنية و إجراءات التعامل مع الاختراقات و إدارة الأدلة الرقمية.
- التحقيق في الهجمات السيبرانية و جمع الأدلة الرقمية و التعاون مع الجهات الأمنية.
- تمرين محاكاة :التعامل مع حادث أمني و تطبيق خطة الاستجابة لِاحتواء الضرر و استعادة البيانات.

اليوم الخامس:

حوكمة أمن المعلومات و التعاون

- مبادئ حوكمة أمن المعلومات و أفضل الممارسات)مثل معيار .(ISO 27001
- إدارة مخاطر أمن المعلومات و وضع السياسات و الإجراءات الأمنية و التدقيق الأمني.
- التعاون و تبادل المعلومات بين المؤسسات الحكومية و الجهات الأمنية لِمواجهة التهديدات بِشكل مُشترك.
- جلسة نقاش :

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.