Ref.No.....

التـاريخ:.....

" ورقة عمل دورة تدريبية "

الاستراتيجيات المتقدمة لأمن الشبكات وأمن المعلومات السلكية واللاسلكية

أولاً: معلومات الدورة:

عنوان الدورة: الاستراتيجيات المتقدمة لأمن الشبكات وأمن المعلومات السلكية واللاسلكية.

- **الجهة المقدمة: نادي الفجيرة العلمي**
- **مدة الدورة 3: أيام**
- **نمط التنفيذ: حضوري / عملي تفاعلي**

ثانياً: الهدف من الدورة:

تهدف هذه الدورة إلى تزويد المشاركين بالمعارف والمهارات المتقدمة في مجال أمن المعلومات وأمن الشبكات السلكية واللاسلكية، وتمكينهم من فهم أحدث التهديدات السيبرانية وأساليب الهجوم الحديثة، والتعرف على أفضل الممارسات والاستراتيجيات العالمية لحماية البنية التحتية الرقمية. كما تهدف إلى تطوير قدراتهم في تأمين الشبكات، وتحليل الثغرات الأمنية، وإدارة المخاطر، واستخدام الأدوات والتقنيات الحديثة لمراقبة الشبكات واكتشاف التهديدات والاستجابة لها، بما يسهم في تعزيز الأمن السيبراني ورفع مستوى الجاهزية الأمنية داخل المؤسسات والبيئات الرقمية.

ثالثاً: محاور الدورة:

- مقدمة في أمن المعلومات والأمن السيبراني.
- مبادئ أمن الشبكات السلكية واللاسلكية.
- مفاهيم السرية والسلامة والتوافر.(CIA Triad)
- التهديدات والهجمات السيبرانية الحديثة وأساليب مواجهتها.
- تأمين البنية التحتية للشبكات.(Routers, Switches, Firewalls)
- أمن الشبكات اللاسلكية (Wi-Fi Security) وآليات الحماية باستخدام بروتوكولات.WPA2/WPA3
- أساليب التشفير وحماية البيانات أثناء النقل والتخزين.
- إدارة الهوية والصلاحيات والتحكم في الوصول.(Identity & Access Management)
- تقسيم الشبكات (Network Segmentation) باستخدام VLANs لتعزيز الحماية.
- أنظمة كشف ومنع الاختراق (IDS/IPS) ومراقبة حركة الشبكة.
- تحليل الثغرات الأمنية (Vulnerability Assessment) وأفضل ممارسات المعالجة.
- مقدمة في اختبار الاختراق (Penetration Testing) وأخلاقيات الاختبار.
- أمن إنترنت الأشياء (IoT Security) والتحديات الأمنية في البيئات الذكية.
- مراقبة وتحليل سجلات الأحداث الأمنية باستخدام منصات.SIEM
- استراتيجيات الاستجابة للحوادث الأمنية والتعافي من الهجمات السيبرانية.
- أفضل الممارسات والمعايير العالمية في أمن المعلومات، مثل ISO/IEC 27001 و.NIST Cybersecurity Framework

التـاريخ:.....

Ref.No.....

رابعاً: الفئة المستهدفة :

- العاملون في مجال تقنية المعلومات وأمن المعلومات.
- مهندسو ومسؤولو الشبكات والبنية التحتية.
- طلاب ومهتمو الأمن السيبراني والشبكات.
- المختصون الراغبون في تطوير مهاراتهم في حماية الشبكات والأنظمة الرقمية.

خامساً: مخرجات التعلم : بنهاية الدورة، سيكون المشارك قادراً على:

- بنهاية الدورة، سيكون المشارك قادراً على:
- فهم مفاهيم أمن المعلومات وأمن الشبكات السلكية واللاسلكية.
- التعرف على أبرز التهديدات والهجمات السيبرانية وأساليب الحماية منها.
- تحليل الثغرات الأمنية وتطبيق أفضل ممارسات تأمين الشبكات.
- استخدام أدوات مراقبة وتحليل الشبكات واكتشاف المخاطر الأمنية.
- تطبيق استراتيجيات حماية الأنظمة والبيانات ورفع مستوى الجاهزية الأمنية.

سادساً: آلية التنفيذ : تعتمد الدورة على أسلوب تدريبي تفاعلي يجمع بين:

- الشرح النظري للمفاهيم الأساسية والمتقدمة في أمن المعلومات والشبكات.
- التطبيقات العملية والمختبرات التدريبية.
- تحليل سيناريوهات واقعية للهجمات السيبرانية وأساليب الحماية.
- التدريب على أدوات تحليل وتأمين الشبكات.
- ورش عمل وتمارين تطبيقية لتعزيز المهارات العملية.

سابعاً: التقييم والأنشطة الختامية :

- تنفيذ تطبيقات عملية واختبارات تقييمية لقياس مستوى الاستيعاب والمهارات المكتسبة.
- تحليل سيناريوهات أمنية واقعية وتقديم الحلول المناسبة.
- تنفيذ نشاط أو مشروع تطبيقي في مجال حماية الشبكات وأمن المعلومات.
- تقييم قدرة المشاركين على اكتشاف التهديدات وتطبيق أساليب الحماية المناسبة.

ثامناً: متطلبات الدورة (إن وجدت) :

مشرف القسم

مهندس / مصطفي علي عبد العزيز