الأمن الرقمي (الجيش والشرطة)

هذا المقرر سيساعد المرشحين على فهم المفاهيم الأساسية لحماية المعلومات والبنية التحتية الحساسة من الهجمات الإلكترونية.

عند الانتهاء من هذا المقرر، سيتمكن المرشح من:

- فهم الاختلافات الرئيسية بين الأمن الإلكتروني على المستوى العسكري والأمن الرقمي المدني
- معرفة أساسيات الدفاع الرقمي، الأمن الفيدرالي والإرهاب الرقمي
- التوعية بمخاطر الاحتمالات مثل الحرب الإلكترونية ومعرفة لماذا تجعل مهنتهم من معلوماتهم الشخصية أمراً شديد الحساسية
- فهم المخاطر عبر الإنترنت ومفاهيم الأمان الأساسية، بما في ذلك تهديدات البيانات وقيمة المعلومات والأمان الشخصي وأمان الملفات
- معرفة ما هي الفيروسات وبرامج التجسس وفيروسات الفدية والإنترنت المظلم؛ تعرف على كيفية الحفاظ على الحماية ضد الجهات الفاعلة في التهديد عبر الإنترنت.
- التعرف على تكنولوجيات الأمن الرقمي الرائدة عالمياً التي طورها الأمن الداخلي والعسكري
- فهم أساسيات أمان الشبكة، بما في ذلك الشبكات والاتصالات، وأمان الشبكات اللاسلكية
- إجراء التحكم في الوصول إلى المعلومات من خلال أساليب مختلفة، وإدارة كلمات المرور بشكل فعال
- استخدم الويب بشكل آمن من خلال إعدادات المتصفح، واعتمد أفضل ممارسات التصفح
- قنوات اتصال آمنة مثل البريد الإلكتروني والشبكات الاجتماعية و تقنية الاتصال الصوتي عبر الإنترنت VoIP والرسائل الفورية والمحمول
- تنفيذ ممارسات إدارة البيانات الآمنة، بما في ذلك تأمين البيانات ونسخها احتياطيًا، وحذف البيانات / إتلافها بشكل آمن
- فهم التهديدات الشائعة لأمن المواطنين، بما في ذلك إدمان استخدام الإنترنت، والتطرف عبر الإنترنت
- فهم مدى أهمية آلية الاستجابة للحوادث ضد الهجمات الإلكترونية
- التعرف على المكونات الحيوية لسياسة الأمن الرقمي، وفهم أهمية تدقيق الالتزام بالسياسة الأمنية على الإنترنت

ما هي فوائد هذا المقرر؟

- يغطي المعلومات الأساسية والمهارات اللازمة لحماية المعلومات والبنية التحتية الحساسة من الهجمات الإلكترونية
- يمكن تطبيقه على سيناريوهات متنوعة للتهديدات عندما يكون الأمن الرقمي للموارد العسكرية والشرطية على حافة الخطر
- شهادة أفضل الممارسات في مجال الأمن الرقمي (الجيش والشرطة)
- تم تطويره من خلال مدخلات من مستخدمي الكمبيوتر والخبراء المتخصصين والمحترفين من جميع أنحاء العالم. تضمن هذه العملية مدى ملاءمة محتوى ونطاق المقرر.

مخرجات المقرر

الموضوع	المهارات
مقدمة	• الأمن الرقمي العسكري مقابل الأمن الرقمي المدني • الدفاع الإلكتروني • الأمن الفيدرالي • الإرهاب الإلكتروني
الحماية	• تحديد المخاطر • حماية المعلومات الشخصية • البصمة الرقمية • مصادقة المستخدم • مكافحة الفيروسات وبرامج التجسس وفيروسات الفدية والإنترنت المظلم
الأمان	• العمليات الإلكترونية العسكرية • تأمين البريد الإلكتروني والاتصالات اللاسلكية ووسائل التواصل الاجتماعي • التشفير • تدمير المعلومات الحساسة • إنترنت الأشياء في الجيش والشرطة
التطبيق	• حماية التواجد على الإنترنت • البرامج والتطبيقات • اجراءات لإرضاء المتطلبات • النسخ الاحتياطي
الدعم	• سياسة الأمن الرقمي • الطوارئ والاستمرارية • الاستجابة للحادث • ثقافة الأمن الرقمي

HOW DO I GET STARTED?

To find out more about this certification, please visit www.icdlarabia.org/certifications

To locate your nearest accredited test centre, please visit www.icdlarabia.org/find-test-centre