ICDL Arabia

الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي - أمن تكنولوجيا المعلومات

منهج إصدار ٢

الغرض

يهدف هذا المستند إلى تقديم التفاصيل حول منهج ECDL / ICDL أمن تكنولوجيا المعلومات. يصف المنهج، من خلال مخرجات التعليم، المعرفة والمهارات التي يجب أن يمتلكها المرشح للحصول على شهادة ECDL/ICDL أمن تكنولوجيا المعلومات. كذلك يقوم المنهج بتقديم أساسا للاختبار النظري والعملي في هذه الوحدة.

إخلاء المسؤولية

بالرغم من أخذ كل عناية من قبل مؤسسة ECDL في إعداد هذا المنشور، لا يتم إعطاء أي ضمان من مؤسسة ECDL، بصفتها الناشر، حول اكتمال المعلومات الواردة فيه، ولن تتحمل مؤسسة ECDL أية مسؤولية عن أية أخطاء، سهو، عدم دقة، خسارة أو ضرر من أي نوع تنشأ بموجب هذه المعلومات أو أية تعليمات واردة في هذا المنشور. يجوز إجراء تغييرات من قبل مؤسسة ECDL حسب تقديرها الخاص وفي أي وقت ودون إشعار مسبق.

الرخصة الأوروبية لقيادة الحاسب الآلي / الرخصة الدولية لقيادة الحاسب الآلي - أمن تكنولوجيا المعلومات

يقدم هذا المقرر المفاهيم والمهارات الأساسية التي يرتكز عليها الاستعمال الآمن لتكنولوجيا المعلومات والاتصالات في الحياة اليومية، واستخدام الأساليب والتطبيقات الملائمة من أجل المحافظة على اتصال شبكي آمن، استخدام الإنترنت بأمان، وإدارة البيانات والمعلومات بشكل ملائم.

أهداف المقرر

سيتمكن المرشحون الناجحون من إظهار المهارات التالية:

- إدراك أهمية تأمين المعلومات والبيانات وتعريف المبادئ العامة لحماية البيانات/الخصوصية والحفظ والتحكم.
- التعرف على تهديدات الأمن الشخصي من سرقة الهوية وتهديدات البيانات المحتملة باستخدام الحوسبة السحابية.
- التمكن من استخدام كلمات المرور والتشفير لتأمين الملفات والبيانات.
- إدراك التهديد الذي تشكله البرامج الضارة والتمكن من حماية الكمبيوتر أو الجهاز أو الشبكة من البرامج الضارة وهجماتها على العناوين.
- التعرف على أنواع الأمن اللاسلكي والشبكي والتمكن من استخدام جدار الحماية الشخصية ونقاط الاتصال الشخصية.
- حماية الكمبيوتر أو الجهاز من الوصول غير المصرح به والتمكن من إدارة كلمات المرور وتحديثها بأمان.
- استخدام إعدادات مناسبة لمتصفح الويب وإدراك كيفية التحقق من صحة المواقع الإلكترونية واستعراض الويب بأمان.
- إدراك مسائل الأمان المتعلقة بالتواصل بما في ذلك البريد الإلكتروني والشبكات الاجتماعية وبروتوكول نقل الصوت عبر الإنترنت والتراسل الفوري والأجهزة المحمولة.
- نسخ البيانات احتياطيًا واستعادتها على مواقع التخزين السحابية والمحلية وحذف البيانات والتخلص من الأجهزة بأمان.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
١. مفاهيم الأمان	١-١ تهديدات البيانات	١-١-١	التفريق بين البيانات والمعلومات
		١-١-٢	فهم مصطلحيّ جرائم الإنترنت والقرصنة وإدراكهما
		١-١-٣	التعرف على البرامج الضارة والتهديدات العرضية التي تتعرض لها البيانات من قبل أفراد أو مقدمي الخدمة أو المنظمات الخارجية.
		١-١-٤	التعرف على التهديدات التي تتعرض لها البيانات نتيجة ظروف استثنائية غير عادية، على سبيل المثال: الحريق والفياضات والحروب والزلازل.
		١-١-٥	التعرف على التهديدات التي تتعرض لها البيانات نتيجة استخدام الحوسبة السحابية، على سبيل المثال: التحكم في البيانات واحتمالية فقدان الخصوصية.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
	١-٢ قيمة البيانات	١-٢-١	إدراك الخصائص الأساسية لأمن المعلومات، على سبيل المثال: السرية والنزاهة والإتاحة.
		٢-٢-١	إدراك أسباب حماية المعلومات الشخصية،على سبيل المثال: تجنب سرقة الهوية والاحتيال والحفاظ على الخصوصية.
		٣-٢-١	إدراك أسباب حماية معلومات العمل المخزنة على أجهزة الكمبيوتر وغيرها من الأجهزة، على سبيل المثال: منع السرقة وعمليات الاحتيال وفقدان البيانات العرضي والأعمال التخريبية.
		٤-٢-١	تعريف المبادئ العامة لحماية البيانات/ الخصوصية والحفظ والتحكم، على سبيل المثال: الشفافية والأغراض الشرعية والتناسب.
		٥-٢-١	إدراك وفهم مصطلحيّ أصحاب البيانات ومراقبي البيانات وكيفية تطبيق مبادئ حماية البيانات/الخصوصية والحفظ والتحكم عليهما.
		٦-٢-١	إدراك أهمية الالتزام باتباع إرشادات استخدام الاتصالات وتكنولوجيا المعلومات (ICT) وسياساته وكيفية الوصول إليهما.
	٣-١ الأمان الشخصي	١-٣-١	إدراك مصطلح الهندسة الاجتماعية والآثار المترتبة عليه، على سبيل المثال: الوصول غير المصرح به لأجهزة الكمبيوتر وغيرها من الأجهزة وجمع المعلومات غير المصرح به والاحتيال.
		٢-٣-١	التعرف على طرق الهندسة الاجتماعية، على سبيل المثال: المكالمات الهاتفية والتصيد (Phishing) والتجول فوق الأكتاف (shoulder surfing).
		٣-٣-١	فهم مصطلح سرقة الهوية والآثار المترتبة عليها وإدراكهما: الشخصية والمالية والقانونية والمتعلقة بالعمل.
		٤-٣-١	تعريف على طرق سرقة الهوية، على سبيل المثال: الغوص في المعلومات والتزوير المالي والتحجج الاحتيالي.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
	١-٤ أمان الملفات	١-٤-١	إدراك تأثيرات تمكين/عدم تمكين الإعدادات الأمنية لملف الماكرو.
		١-٤-٢	إدراك مزايا التشفير وحدود تقييده، وكن على دراية بأهمية وضرورة عدم الإفصاح عن كلمة مرور التشفير أو مفتاحه أو شهادته أو فقدانها.
		١-٤-٣	تشفير ملف أو مجلد أو محرك أقراص
		١-٤-٤	تعيين كلمة مرور للملفات، على سبيل المثال: المستندات وجداول البيانات والملفات المضغوطة.
٢. البرامج الخبيثة	٢-١ الأنواع والطرق	٢-١-١	إدراك مصطلح البرامج الخبيثة وفهمه، إلى جانب التعرف على مختلف الطرق التي يمكن استخدامها كوسيلة لإخفاء البرامج الضارة على أجهزة الكمبيوتر وغيرها من الأجهزة، على سبيل المثال: أحصنة طروادة والجذور الخفية (rootkits) والأبواب الخلفية (backdoors).
		٢-١-٢	التعرف على أنواع البرامج الخبيثة المعدية وإدراك طريقة عملها: الفيروسات والديدان.
		٢-١-٣	التعرف على أنواع البرامج الخبيثة لسرقة البيانات مثل توليد الأرباح/الابتزاز، إلى جانب إدراك طريقة عملها: البرامج الإعلانية وبرامج الفدية وبرامج التجسس وشبكات البوتات وتسجيل ضربات المفاتيح والمسجلات والأجهزة القائمة بعملية الاتصال للربط على شبكة الإنترنت
	٢-٢ الحماية	٢-٢-١	إدراك طريقة عمل البرامج المضادة للفيروسات وحدود تقييدها.
		٢-٢-٢	إدراك ضرورة تثبيت برنامج لمكافحة الفيروسات على أجهزة الكمبيوتر وغيرها من الأجهزة
		٢-٢-٣	إدراك أهمية تحديث البرامج بصورة منتظمة، على سبيل المثال: برامج مكافحة الفيروسات ومتصفح الويب والمكونات الإضافية والتطبيقات ونظام التشغيل.
		٢-٢-٤	مسح محركات أقراص أو مجلدات أو ملفات معينة باستخدام برنامج مضاد للفيروسات، مع الحرص على جدولة عمليات المسح باستخدام برنامج مضاد للفيروسات.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
		٢-٢-٥	إدراك المخاطر الناتجة عن استخدام البرامج القديمة وغير المدعومة، على سبيل المثال: المخاطر المتزايدة للبرامج الضارة وعدم التوافق.
	٢-٣ حل المشكلة والتغلب عليها	٢-٣-١	فهم مصطلح فرض العزل والآثار المترتبة على الملفات الملوثة/المشبوهة
		٢-٣-٢	عزل الملفات الملوثة/المشبوهة وحذفها.
		٢-٣-٣	إدراك إمكانية تشخيص هجمات البرامج الضارة واكتشافها والقضاء عليها باستخدام مصادر إلكترونية، على سبيل المثال: مواقع أنظمة التشغيل وبرامج مكافحة الفيروسات والشركات الموردة لبرامج متصفح الويب ومواقع الأطراف المعنية.
٣. حماية الشبكة	٣-١ الأنواع والطرق	٣-١-١	فهم مصطلح شبكة وإدراك أنواع الشبكات الشائعة مثل: الشبكة المحلية (LAN), الشبكة المحلية الواسعة (WLAN), الشبكات الواسعة (WAN), الشبكة الخاصة الافتراضية (VPN).
		٣-١-٢	فهم كيفية التوصيل بشبكة مؤمنة ضد: البرامج الضارة، الدخول غير المصرح به، الحفاظ على الخصوصية.
		٣-١-٣	فهم دور مسؤول الشبكة في إدارة توثيق دفعات الحماية ذات الصلة وترخيصها وتقديرها ومراقبتها وتثبيتها بجانب تحديث مراقبة شبكة المرور والتعامل مع البرامج الضارة التي توجد داخل الشبكة.
		٣-١-٤	فهم وظيفة جدار الحماية وحدود تقييده في بيئة العمل الشخصية.
		٣-١-٥	تشغيل جدار حماية شخصي وإيقافه، تخصيص جهاز أو خادم/وظيفة ومنع الوصول إليهم من خلال جدار الحماية الشخصي.
	٣-٢ الأمن اللاسلكي	٣-٢-١	إدراك الخيارات المتعددة للأمن اللاسلكي وحدود تقيدها مثل: تكافؤ السرية للشبكة السلكية (WEP), الوصول المحمي اللاسلكي (WPA), الوصول المحمي اللاسلكي (WPA2), التحكم في الوصول إلى الوسائط (MAC), اختفاء معرف ضبط الخادم (SSID).

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
		٣-٢-٢	إدراك خطورة استخدام شبكة لاسلكية غير مؤمنة حيث يمكن أن تؤدي إلى: اختراق الشبكة من قبل المتجسسون.
		٣-٢-٣	فهم مصطلح نقاط الاتصال الشخصية.
		٣-٢-٤	تمكين وتعطيل نقاط اتصال شخصية مؤمنة وتوصيل الأجهزة وفصلها بشكل آمن.
٤. التحكم في الوصول	٤-١ الوسائل	٤-١-١	تعريف إجراءات منع الوصول غير المصرح به إلى البيانات مثل: اسم المستخدم، كلمة المرور، رمز PIN، برامج التشفير، المصادقة المتعددة.
		٤-١-٢	فهم مصطلح كلمة المرور لمرة واحدة واستخدامها بشكل نموذجي.
		٤-١-٣	إدراك الغرض من إنشاء حساب على الشبكة.
		٤-١-٤	إدراك أهمية الوصول إلى الحساب على الشبكة من خلال إدخال اسم المستخدم وكلمة المرور وضرورة قفل الحساب أو الخروج منه عند عدم الاستخدام.
		٤-١-٥	تعريف تقنيات مقاييس الحماية الحيوية المستخدمة في التحكم بالوصول مثل: بصمة الإصبع، المسح الضوئي ببصمة العين، التعرف على الوجه، هندسة اليد.
	٤-٢ إدارة كلمة المرور	٤-٢-١	إدراك سياسات كلمة المرور الجيدة، مثل: ملائمة طول كلمة المرور، ملائمة الحروف، المزيج الملائم من الحروف الخاصة والأرقام والأحرف الأبجدية، عدم مشاركة كلمات المرور، تغيير كلمة المرور بشكل منتظم،استخدام كلمات مرور مختلفة للخدمات المختلفة.
		٤-٢-٢	إدراك وظيفة وحدود تقييد برامج إدارة كلمة المرور.
٥. الإستخدام الآمن لشبكة الإنترنت	٥-١ إعدادات المتصفح	٥-١-١	اختر إعدادات مناسبة لتمكين وعدم تمكين خاصية الإكمال التلقائي وعدم الحفظ عند إكمال نموذج.
		٥-١-٢	حذف بيانات شخصية من المتصفح مثل: سجل المتصفح، السجلات المحملة، ملفات الإنترنت المخزنة، كلمات المرور، ملفات التعريف، البيانات التي تم إكمالها بشكل تلقائي.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
	٥-٢ تأمين التصفح	٥-٢-١	الانتباه إلى أهمية إجراء أي نشاط محدد عبر الإنترنت (الشراء، المعاملات المالية) من خلال صفحات إنترنت آمنة باستخدام اتصال إنترنت آمن.
		٥-٢-٢	تعريف طرق متعددة لتأكيد صحة موقع الإنترنت مثل: المحتويات عالية الجودة، العملات الأجنبية، عنوان URL الساري، المعلومات الخاصة بالشركة أو المالك، معلومات الاتصال، شهادة الأمان، التحقق من مجال المالك.
		٥-٢-٣	فهم مصطلح عمليات الاحتيال.
		٥-٢-٤	إدراك وظيفة برامج التحكم في المحتوى وأنواعها مثل: برامج الترشيح على الإنترنت، برامج المراقبة الأبوية.
٦. الاتصالات	٦-١ البريد الإلكتروني	٦-١-١	إدراك الهدف من تشفير البريد الإلكتروني فك تشفيره
		٦-١-٢	فهم مصطلح التوقيع الرقمي
		٦-١-٣	التعرف على رسائل البريد الإلكتروني الاحتيالية وغير المرغوب فيها.
		٦-١-٤	التعرف على الخصائص الشائعة للتصيد الإلكتروني (phishing) مثل: استخدام أسماء المنظمات القانونية والأشخاص وروابط الويب المزيفة والشعارات والعلامات التجارية وتشجيع الكشف عن المعلومات الشخصية.
		٦-١-٥	الدراية بإمكانية الإبلاغ عن محاولات التصيد الإلكتروني للمنظمات القانونية والأطراف المعنية.
		٦-١-٦	إدراك خطر إصابة الكمبيوتر أو الجهاز بالبرامج الضارة عن طريق فتح مرفق البريد الالكتروني الذي يحتوي على ملف ماكرو أو ملف قابل للتنفيذ.
	٦-٢ الشبكات الاجتماعية	٦-٢-١	إدراك أهمية تجنب الكشف عن المعلومات السرية أو الشخصية على الشبكات الاجتماعية .
		٦-٢-٢	الدراية بضرورة ضبط إعدادات حساب موقع التواصل الاجتماعي ومراجعته بانتظام مثل: خصوصية الحساب والموقع.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
		٦-٢-٣	ضبط إعدادات حساب موقع التواصل الاجتماعي: خصوصية الحساب والموقع.
		٦-٢-٤	إدراك المخاطر المحتملة لاستخدام مواقع التواصل الاجتماعي مثل: التسلط عبر الإنترنت والاستمالة والكشف عن المحتويات الشخصية والهويات الزائفة الارتباطات والرسائل الاحتيالية أو الخبيثة.
		٦-٢-٥	إدراك إمكانية إبلاغ مزود الخدمة والأطراف المعنية عن الاستخدام أو السلوك غير الصحيح لمواقع التواصل الاجتماعي.
	٦-٣ بروتوكول نقل الصوت عبر الإنترنت والتراسل الفوري	٦-٣-١	إدراك نقاط الضعف الكامنة في أمان التراسل الفوري وبروتوكول نقل الصوت عبر الإنترنت مثل: البرامج الخبيثة والوصول المستتر والوصول إلى الملفات والتنصت.
		٦-٣-٢	التعرف على طرق ضمان السرية عند استخدام بروتوكول نقل الصوت عبر الإنترنت والتراسل الفوري مثل: التشفير وعدم الكشف عن المعلومات الهامة وحظر مشاركة الملفات.
	٦-٤ الهواتف المحمولة	٦-٤-١	إدراك الآثار المحتملة لاستخدام تطبيقات من متاجر التطبيقات غير الرسمية مثل: البرامج الضارة للهواتف المحمولة والاستخدام غير الضروري للمصادر والوصول إلى البيانات الشخصية ورداءة الجودة والتكاليف الضمنية.
		٦-٤-٢	فهم مصطلح صلاحيات التطبيقات.
		٦-٤-٣	إدراك إمكانية استخلاص المعلومات الخاصة من تطبيقات الهواتف المحمولة مثل: تفاصيل الاتصال وسجل الموقع والصور.
		٦-٤-٤	الدراية بالإجراءات الاحتياطية وإجراءات الطوارئ التي يجب اتخاذها في حالة فقدان الهاتف مثل: التعطيل عن بعد والمسح عن بعد وتحديد موقع الهاتف.
٧. تأمين إدارة البيانات	٧-١ تأمين البيانات ونسخها احتياطيًا	٧-١-١	التعرف على طرق ضمان الأمن المادي لأجهزة الكمبيوتر والأجهزة الأخرى مثل: تجنب ترك مواقع وتفاصيل معدات تسجيل الدخول دون مراقبة، واحرص على استخدام أقفال الكبلات والتحكم في الوصول.

الفئة	مجموعة المهارات	المرجع	موضوع المهمة
		٢-١-٧	التعرف على أهمية نسخ البيانات احتياطيًا في حالة فقدانها من أجهزة الكمبيوتر أو الأجهزة الأخرى.
		٣-١-٧	التعرف على مميزات النسخ الاحتياطي مثل: الانتظام/التكرار والجدول وموقع التخزين وضغط البيانات.
		٤-١-٧	نسخ البيانات احتياطيًا إلى موقع ما مثل: برنامج التشغيل المحلي أو الوسائط/برنامج التشغيل الخارجي أو الخدمة السحابية.
		٥-١-٧	استعادة البيانات من موقع النسخ الاحتياطي مثل: برنامج التشغيل المحلي أو الوسائط/ برنامج التشغيل الخارجي أو الخدمة السحابية.
	٢-٧ الإتلاف والحذف الآمن	١-٢-٧	التفرقة بين حذف البيانات وبين تدميرها بشكل دائم.
		٢-٢-٧	إدراك أسباب الحذف الدائم للبيانات من محركات الأقراص أو الأجهزة.
		٣-٢-٧	الدراية بتعذر تدمير البيانات بشكل دائم للمحتويات من الخدمات مثل: مواقع التواصل الاجتماعي والمدونات ومنتديات الإنترنت والخدمات السحابية.
		٤-٢-٧	التعرف على الطرق الشائعة تدمير البيانات بشكل دائم مثل : التمزيق أو تدمير محرك الأقراص/الوسائط أو إزالة المغنطة أو استعمال أدوات تدمير البيانات .