

متطلبات الأمن السيبراني لتقييم المخاطر السيبرانية للأطراف الخارجية

السلام عليكم ورحمة الله وبركاته،
نشكر لكم اهتمامكم ونأمل التعاون لإستكمال الإستبيان التالي بخصوص ممارسات إدارة مخاطر الأمن السيبراني.
ستستخدم هذه المعلومات لتقييم استعدادكم وتحديد مدى توافق خدماتكم مع متطلبات الأمن السيبراني.

يرجى استكمال الإستبيان وإرجاعه إلينا بنهاية يوم .../.../... هـ.

إذا كنتم بحاجة إلى أي توضيح أو لديكم أي أسئلة، نرجو التواصل مع إدارة الحوكمة والمخاطر والالتزام لأمانة المنطقة الشرقية.

معلومات الشركة:



1. اسم الشركة: تقنيات الجوال
2. الشخص المكلف بالتواصل: أنس حبيب
3. رقم هاتف للتواصل: 126096669 Ext 520 (966)
4. عنوان البريد الإلكتروني: soc@taqnyat.sa
5. موقع الشركة على الإنترنت: <https://taqnyat.sa>
6. التوقيع :

سياسات وضوابط الأمن السيبراني لتقييم مخاطر:

1. يرجى تقديم تفاصيل حول الحوادث الأمنية السابقة وكيف تم التعامل معها.
2. كم عدد سنوات خبرتكم في إدارة مخاطر الأمن السيبراني؟
3. هل تقومون بتقييم شامل لمخاطر الأمن السيبراني؟

الاستبيان لتقييم مخاطر السيبرانية للأطراف الخارجية:

الطرف الخارجي	الادلة المطلوبة	سؤال الضابط	المعايير	الضابط	ترقم	النطاق
تم إرفاق السياسة المطلوبة	عينة من دليل السياسات - سياسة تتضمن تفاصيل المراجعة والموافقة المناسبة	هل تم تحديد وتوثيق واعتماد سياسات وإجراءات الأمن السيبراني من قبل الإدارة العليا وإبلاغها إلى الأطراف ذات الصلة داخل المنظمة وخارجها؟	ECC	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها وذلك وفقاً لمتطلبات الأعمال التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة .	1-1	الحوكمة والالتزام

٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي للموظفين (قبل التوظيف وإنشاء التوظيف وبعد إنهاء الخدمة/الانفصال).	ECC	هل لدى المنظمة عملية محددة لضمان تلبية متطلبات الموظفين للكافة، مثل اتفاقية عدم الإفصاح، وإزالة الوصول عند إنهاء الخدمة، والتحقق من خلفية الموظفين بعمل مسح أملي؟	نعم - تم إرفاق نموذج بند اتفاقية عدم الإفصاح (NDA)
٣-١	يجب تحديد سياسة الاستخدام المقبول لأصول المعلومات والتكنولوجيا، موثقة ومعتمدة	ECC	هل لدى المنظمة سياسة استخدام مقبول محددة تصف الاستخدام المناسب لأصول المنظمة؟ ١. الاستخدام المقبول للبيانات ٢. استخدام محطات العمل للأغراض الرسمية فقط ٣. استخدام رسائل البريد الإلكتروني للتواصل الرسمي فقط	نعم يوجد تم إرفاق السياسة
٤-٢	يجب اعتماد سياسة مكتبية واضحة تهدف إلى ضمان خلو المكتب من الأوراق الصلبة ووسائط التخزين القابلة للإزالة (مثل وحدات USB أو الأقراص الصلبة الخارجية) عند عدم استخدامها أو عند ترك المكتب	ISO	هل لدى المنظمة سياسة واضحة للمكتب الأمن	نعم Acceptable Use of Information Assets
٥-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي لإدارة الأصول المعلوماتية والتقنية للجهة	ECC	هل لدى المنظمة سياسة محددة وموثقة لإدارة الأصول؟ ١. جرد الأصول (البرمجيات، الأجهزة، البيانات) ٢. عملية تدمير الأصول ٣. معايير الاحتفاظ بالأصول	نعم Asset Discovery and Asset Classification
٦-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي لإدارة الهويات النخول والصلاحيات في الجهة.	ECC	هل لدى المنظمة سياسة محددة لإدارة الوصول؟ ١. منح حق الوصول ٢. مراجعة الأصول	نعم Cybersecurity in Human Resources
٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي لحماية البريد الإلكتروني للجهة.	ECC	هل لدى المنظمة إجراءات محددة لأمن البريد الإلكتروني وقمعه؟	نعم
٨-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي لإدارة أمن الشبكات للجهة	ECC	هل لدى المنظمة سياسة محددة لإدارة الشبكة؟	نعم Network Security
٩-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبيريائي للأجهزة الشخصية للعامل بشبكة الجهة.	ECC	هل لدى المنظمة سياسة BYOD محددة؟	نعم تم إرفاق السياسة

Taqnyät

JEDDAH: 4030394715
RIVADH: 1010296254
KHOBAR: 2051240697

١٠-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.	ECC	هل لدى المنظمة معيار موثق رسمياً لتصنيف البيانات؟ ١. تصنيف البيانات والمعلومات ٢. ترميز البيانات والمعلومات ٣. متطلبات التشفير	وثيقة سياسة تصنيف البيانات	نعم تم ارفاق السياسة
١١-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني للتشفير للجهة	ECC	هل لدى المنظمة سياسة تشفير محددة؟	وثيقة سياسة التشفير	نعم تم ارفاق السياسة
١٢-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني لإدارة النسخ الاحتياطية للجهة.	ECC	هل لدى المنظمة سياسة لإجراء محدد للنسخ الاحتياطي؟	وثيقة سياسة النسخ الاحتياطي / الإجراء للنسخ الاحتياطي	نعم تم ارفاق السياسة
١٥-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني لإدارة سجلات الأحداث ومراقبة الأمن السبراني	ECC	هل لدى المنظمة سياسة/عملية محددة لإدارة السجل؟ ١. الاحتفاظ بالسجل ٢. الوصول إلى السجلات	عملية إدارة السجل	نعم تم ارفاق السياسة
١٦-٢	يجب تحديد وتوثيق واعتماد متطلبات حوادث الأمن السبراني وإدارة التهديدات	ECC	هل لدى المنظمة عملية محددة وموثقة لإدارة الحوادث والتهديدات؟	سياسة إدارة الحوادث	نعم تم ارفاق السياسة
١٨-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والتلفان والسرقة والتخريب	ECC	هل لدى المنظمة سياسة محددة للأمن المادي؟	وثيقة سياسة الأمن المادي	نعم تم ارفاق السياسة
١٩-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني ضمن إدارة استمرارية الأعمال لدى الجهة.	ECC	هل لدى المنظمة سياسة/خطة محددة لاستمرارية الأعمال؟	وثيقة سياسة / خطة استمرارية الأعمال	نعم تم ارفاق السياسة
٢٠-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السبراني الخاصة باستخدام خدمات الحوسبة السحابية والإستضافة.	ECC	هل لدى المنظمة سياسة محددة لأمن الحوسبة السحابية؟	وثيقة سياسة أمن الحوسبة السحابية	نعم تم ارفاق السياسة
٢٢-٢	يجب على الجهة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السبراني	ECC	هل المنظمة تمتلك لقوانين ولوائح الأمن السبراني الوطنية المعمول بها؟	تقرير الامثال NCA	كجهة تتبع هيئة الاتصالات والفضاء والتقنية لا يوجد لدينا تقرير عن الالتزام بمتطلبات NCA
١-٣	يجب تضمين متطلبات الأمن السبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السبراني جزء أساسي من متطلبات المشاريع التقنية	ECC	هل لدى المنظمة سياسة محددة لإدارة التغيير؟ هل تضمن السياسة تغطية متطلبات الأمن السبراني أثناء تنفيذ التغيير كجزء من دورة حياة المشروع؟	سياسة / منهجية إدارة التغيير	نعم تم ارفاق السياسة
٢-٣	يجب أن تغطي متطلبات الأمن السبراني إدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بشكل أدنى مالي: إجراء مراجعة الإعدادات والتحصين وحزم	ECC	هل لدى المنظمة سياسة/عملية محددة لإدارة حزم التحديثات والتي مطابقة لمتطلبات التحديثات؟	وثيقة سياسة/عملية إدارة حزم التحديثات	نعم تم ارفاق السياسة

التحديثات قبل إطلاق المشاريع والتغييرات				
المخاطر	١-٤	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة وذلك وفقاً لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.	ECC	هل لدى المنظمة منهجية وإجراءات لإدارة مخاطر الأمن السيبراني محددة وموثقة ومعتمدة؟
	٢-٤	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات بعد أدنى مائلي	ECC	هل المنظمة تلخص وتراقب أنشطتها لرتبسية بشكل روتيني بحثاً عن نقاط الضعف؟
	٤-٢-٤	يجب أن تغطي إجراءات إدارة الثغرات بعد أدنى مائلي وعلى سبيل المثال لا الحصر : إجراءات فحص واكتشاف الثغرات دورياً ،آلية تصنيف الثغرات حسب خطورتها ،إجراءات معالجة الثغرات بناء على تصنيفها	ECC	تقرير تحليل نقاط الضعف
	٤-٤	يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) الأطراف الخارجية التي قد تتكرر باسمايتها ببيانات الجهة أو الخدمات المقدمة لها بعد أدنى مائلي : بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الأمن من قبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.	ECC	نموذج لنموذج العقد
النوعية والتدريب	١-٥	يجب تطوير واعتماد برنامج للتوعية للأمن السيبراني في الجهة من خلال قنوات متعددة دورياً وذلك لتعزيز الوعي بالأمن السيبراني وتبنيته ومخاطره ،وبناء ثقافة إيجابية للأمن السيبراني	ECC	هل لدى المنظمة برنامج محدد للتدريب والتوعية بالأمن السيبراني يغطي مائلي؟
	١-١-٥	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتحديات السيبرانية وما يستجد منها بما في ذلك التعامل الأمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني.	ECC	١. التعامل الأمن مع خدمات البريد الإلكتروني، وخاصة رسائل التصيد الاحتمالي
	٢-١-٥	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتحديات السيبرانية وما يستجد منها بما في ذلك التعامل الأمن مع الأجهزة المحمولة ووسائل التخزين.	ECC	٢. التعامل الأمن مع الأجهزة المحمولة ووسائل التخزين.
	٢-٥	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتحديات السيبرانية وما يستجد	ECC	٣. التصديق الأمن للإتقنات.

شركة سبائك الدوال المعلوماتية المحدودة

Taqnyät

JEDDAH 4030394715
RIYADH 1010296254
KHOBAR 2051240697

			منها بما في ذلك : التعامل الآمن مع خدمات تصفح الإنترنت.		
نعم	سياسة الاستخدام المقبول	هل تضمن المنظمة تنفيذ سياسة الاستخدام المقبول مع فرض قيود مناسبة على استخدام الأصول؟	ECC	يجب تطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.	٢-٦
نعم	لقطات شاشة من الأنوار المنفذة للتأكد من تصنيف البيانات وتصنيفها	هل تمتلك المنظمة أدوات كافية لضمان تصنيف البيانات عبر جميع أقسامها؟ هل تم تحديث، توثيق، والموافقة على متطلبات الأمن السبيري للبيانات لحماية البيانات والمعلومات بعد أدنى مالي ملكية البيانات والمعلومات؟ هل تم تحديث، توثيق، والموافقة على متطلبات الأمن السبيري للبيانات لحماية البيانات والمعلومات بعد أدنى مالي تصنيف البيانات والمعلومات وألية ترميزها (Classification and Labeling Mechanisms)؟ هل تم تحديث، توثيق، والموافقة على متطلبات الأمن السبيري للبيانات لحماية البيانات والمعلومات بعد أدنى مالي: خصوصية البيانات والمعلومات	ECC	يجب تطبيق متطلبات الأمن السبيري لحماية البيانات ومعلومات الجهة.	١-٧
			ECC	يجب أن تغطي متطلبات الأمن السبيري لحماية البيانات والمعلومات بعد أدنى مالي ملكية البيانات والمعلومات	١-١-٧
			ECC	يجب أن تغطي متطلبات الأمن السبيري لحماية البيانات والمعلومات بعد أدنى مالي تصنيف البيانات والمعلومات وألية ترميزها (Classification and Labeling Mechanisms)	٢-١-٧
			ECC	يجب أن تغطي متطلبات الأمن السبيري لحماية البيانات والمعلومات بعد أدنى مالي: خصوصية البيانات والمعلومات	٣-١-٧
نعم		هل لدى المنظمة عملية وإطار لإدارة الهويات وبيانات الاعتماد والوصول بشكل آمن؟	ECC	يجب تطبيق متطلبات الأمن السبيري لإدارة هويات الدخول والصلاحيات في الجهة .	١-٨
نعم	لقطات شاشة من الأدلة لضمان تنفيذ آلية كلمة المرور المعقدة	هل تمتلك المنظمة عملية مساعدة للمستخدم تعتمد على اسم المستخدم وكلمة المرور؟	ECC	يجب أن تغطي متطلبات الأمن السبيري المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بعد أدنى مالي : التحقق من هوية المستخدم (User Authentication) بناء على إدارة تسجيل المستخدم ،إدارة كلمة المرور	٢-٨
نعم	لقطات شاشة من الأدلة لضمان تنفيذ آلية كلمة المرور المعقدة	هل تضمن المنظمة أن جميع المستخدمين ملزمون بتسجيل الدخول باستخدام المصادقة متعددة العوامل (MFA)؟	ECC	يجب أن تغطي متطلبات الأمن السبيري المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بعد أدنى مالي : التحقق من الهوية متعددة العناصر (Multi-factor Authentication) لعناصر الدخول عن بعد.	٣-٨

(MFA) ثبات الدوال المعلوماتية المحدودة

Taqnyat

JEDDAH : 4030394715
RIVADH : 1010296254
KHOBAR : 2091240597

نعم		هل يتم التحكم في جميع أدوات الوصول لجميع الأنظمة والأجهزة الرئيسية من خلال مبادئ الإمتيازات الأقل وتفصل بين المهام؟	ECC	يجب أن تغطي متطلبات الأمن السيرباني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بعد أدنى مابلي :إدارة الصلاحيات الهامة والحساسة (Privileged Access Management)	٥-٨
تم الإفراق	لغة شائعة من الأداة لضمان تطبيق الية كلمة المرور المعقدة	هل لدى المنظمة سياسة لكلمات المرور؟ الطول المناسب وتعقيد كلمة المرور.	ISO	يجب أن تكون أنظمة إدارة الكلمات السرية تقاعية وأن تضمن كلمات مرور قوية وأمنة	٦-٨
تم إفراق السياسة	سياسة إدارة الهويات وصلاحيات الدخول	هل لدى المنظمة عملية تعرف إدارة الوصول للمستخدمين؟	ISO	يجب تنفيذ عملية رسمية لإدارة الوصول للمستخدمين تعيين أو إلغاء حقوق الوصول لجميع أنواع المستخدمين إلى جميع الأنظمة والخدمات.	٨-٨
WAF يتم تطبيق ال Mod security من خلال	يتم تنفيذ لقطات الشاشة من أداة التحقق من صحة WAF	هل قامت المنظمة بتطبيق جدار حماية لتطبيقات الويب (WAF) للتطبيقات الويب الموجهة للجهات الخارجية؟	ECC	يجب تطبيق متطلبات الأمن السيرباني لحماية تطبيقات الويب الخارجية للجهة.	١-٩
WAF يتم تطبيق ال Mod security من خلال	يتم تنفيذ لقطات الشاشة من أداة التحقق من صحة WAF	هل تم تكوين جدران الحماية؟ ١. مراجعة قواعد جدار الحماية ٢. إدارة التغيير	ECC	يجب أن تغطي متطلبات الأمن السيرباني لحماية تطبيقات الويب الخارجية للجهة بعد أدنى مابلي : استخدام جدار حماية لتطبيقات الويب (application web firewall)	٢-٩
تم الإفراق	لغة شائعة من الأداة لضمان تنفيذ MFA للتطبيقات الخارجية	هل تملك المنظمة تحكماً مناسباً وأدنى في الوصول أثناء استخدام تطبيقات الويب الخارجية؟	ECC	يجب أن تغطي متطلبات الأمن السيرباني لحماية تطبيقات الويب الخارجية للجهة بعد أدنى مابلي : التحقق من الهوية متعدد العناصر (Multi-factor Authentication) لعمليات دخول المستخدمين .	٥-٩
تم الإفراق	لغة شائعة من الأدوات مثل جدار الحماية، IPS، مخطط تقسيم الشبكة	هل قامت المنظمة بتطبيق سياسة أمن الشبكة؟ ١. الفصل المنطقي أو المادي وتجزئة أجزاء الشبكة باستخدام جدران الحماية ومبادئ الدفاع المتمسق ؟ ٢. التصفح الأمن والاتصال بالإنترنت بما في ذلك القيد المفروضة علي	ECC ECC	يجب تطبيق متطلبات الأمن السيرباني لإدارة أمن الشبكات في الجهة يجب أن تغطي متطلبات الأمن السيرباني لإدارة أمن شبكات الجهة بعد أدنى مابلي : العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل أمن واللازم لسيطرة على مخاطر الأمن السيرباني ذات العلاقة باستخدام جدار الحماية (Firewall) ومبدأ النطاق الأمني	٢-١٠ ١٠-٢-١٠

مراجعة تقنيات الدوال المعلوماتية المحدودة

Taqnyat

JEDDAH: 4030394715

RIYADH: 1010296254

KHOBAR: 2051240697

Defense-in-Depth	متعدد المراحل (Defense-in-Depth)	استخدام تخزين/مشاركة الملفات والوصول إلى مواقع الويب عن بعد، والحماية من مواقع الويب المشبوهة؟	٣-٢-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بعد أدنى مائي: أمن التصفح والاتصال بالإنترنت ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة ومواقع مشاركة وتخزين الملفات ومواقع الدخول عن بعد
٣-١٠	ECC	هل لدى المنظمة نظام (IPS) يتم تنفيذه المراقبة المستمرة للأنشطة الضارة ومعتمتها؟	٣-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بعد أدنى مائي: أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems)
٤-١٠	ECC	هل لدى المنظمة خدمة اسم المجال (DNS) التي تم تكوينها بشكل آمن؟	٤-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بعد أدنى مائي: أمن نظام أسماء النطاقات (DNS)
٦-١٠	ECC	هل لدى المنظمة عملية للتسرخ الاحتمالي وأرشفة رسائل البريد الإلكتروني؟ هل تم تطبيق معايير أمن البريد الإلكتروني؟ (مثل DKIM و DMARC و SPF)	٦-١٠	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة
١٠-٦-١٠	ECC	١. المصادقة متعددة العوامل للوصول إلى البريد الإلكتروني عبر الإنترنت والوصول عن بُعد. ٢. التحقق من نطاقات خدمة البريد الإلكتروني للمنظمة (مثل استخدام إطار سياسة المرسل (SPF).	١٠-٦-١٠	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بعد أدنى مائي: تحليل وتصفية (Filtering) رسائل البريد الإلكتروني (وخصوصاً رسائل التصيد الإلكتروني >> Phishing <<Email و الرسائل الاحتمالية <<Spam Email>>) باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني.
2-6-10	ECC	١. المصادقة متعددة العوامل للوصول إلى البريد الإلكتروني عبر الإنترنت والوصول عن بُعد. ٢. التحقق من نطاقات خدمة البريد الإلكتروني للمنظمة (مثل استخدام إطار سياسة المرسل (SPF).	2-6-10	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بعد أدنى مائي: التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة مواقع البريد الإلكتروني (Webmail)
5-6-10	ECC	١. المصادقة متعددة العوامل للوصول إلى البريد الإلكتروني عبر الإنترنت والوصول عن بُعد. ٢. التحقق من نطاقات خدمة البريد الإلكتروني للمنظمة (مثل استخدام إطار سياسة المرسل (SPF).	5-6-10	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بعد أدنى مائي: توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية مثل طريقة إطار سياسة المرسل (Sender Policy Framework)

امن البريد الإلكتروني

شركة تقنيات الجوال للمعلوماتية المحدودة

Taqnyät

J U D A H : 4 0 3 0 3 9 4 7 1 5
R I Y A D H : 1 0 1 0 2 9 6 2 5 4
K H O B A R : 2 0 8 1 2 4 0 6 9 7

7-10	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة .	ECC	هل قامت المنظمة بتطبيق تقنية النسخ الاحتياطي؟ اختبارات دورية لعملية استعادة النسخ الاحتياطية.	لقطة شاشة من الأداة للتأكد من تنفيذ تقنية النسخ الاحتياطي	تم إرفاق الدليل
1-11	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بعد أدنى مالي: الحماية من الفيروسات والبرامج والأشعة المشبوهة والبرمجيات الضارة على المستخدمين (Malware) والخوادم باستخدام تقنيات وأليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.	ECC	هل لدى المنظمة برنامج مكافحة الفيروسات مثبت على جميع محطات العمل والخوادم؟	لقطة شاشة من الأداة للتأكد من تثبيت AV	تم إرفاق الدليل
2-11	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بعد أدنى مالي: التقيد بالحزم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها.	ECC	هل تقوم المنظمة بتقييد استخدام الوسائط القابلة للإزالة؟ عملية استخدام الوسائط القابلة للإزالة تشفير البيانات على الأجهزة القابلة للإزالة	لقطة شاشة من الأداة للتأكد من أن USB مفيد للاستخدام	تم إرفاق الدليل
5-11	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بعد أدنى مالي: الاستخدام المحدد والمقيد بناء على ما تتطلبه مصلحة أعمال الجهة.	ECC	هل لدى المنظمة عملية لضمان تقييد استخدام الأجهزة المحمولة (الشخصية) لأغراض محدودة فقط؟		نعم
1-12	يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بعد أدنى ما يلي: استخدام معايير (Coding Secure Standards)	ECC	هل تستخدم المنظمة معايير تشفير آمنة أثناء تطوير التطبيقات؟	وثيقة معايير تطوير البرمجيات الآمنة (SDLC)	تم إرفاق الدليل
1-13	يجب تطبيق متطلبات الأمن السيبراني لسجلات الأحداث ومراقبة الأمن السيبراني للجهة. يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بعد أدنى ما يلي: المراقبة المستمرة لسجلات	ECC	هل يتم تسجيل الأحداث ومراقبتها بشكل مستمر؟ المراقبة المستمرة لأحداث الأمن السيبراني فترة الاحتفاظ بسجلات أحداث الأمن السيبراني	لقطة شاشة من الأداة للتأكد من تسجيل الأحداث	تم إرفاق الدليل
1-1-13		ECC		شركة تقيت الدوال المعلوماتية المحدودة	

امن نهاية النقاط
(Endpoint)
(Security)

تطوير وصيانة
النظام

Defense &
Security
Analysis
(تحليل الدفاع
(والأمن)

Taqnyat

JEDDAH: 4030394715
RIYADH: 1010296254
KHOBAR: 2051240697

الأحداث الخاصة بالأمن السيراني	(يجب أن تكون ١٢ شهراً على الأقل).			
٢-١٣	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيراني في الجهة .	ECC	هل لدى المنظمة سياسة لإدارة الحوادث؟ خطط الاستجابة لحوادث الأمن السيراني وإجراءات التصعيد؟	تم ارفاق السياسة وثيقة التعامل مع الحوادث / معالجة التصعيد
1-2-13	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيراني بعد أدنى مالي: بوضع خطط الاستجابة للحوادث والأمنية واليات التصعيد.	ECC		
1-14	يجب تطبيق متطلبات الأمن السيراني ضمن إدارة استمرارية الأعمال .	ECC	هل قامت المنظمة بتنفيذ خطة استمرارية الأعمال؟ خطط التعافي من الكوارث.	تم ارفاق الخطة خطة استمرارية الأعمال خطة التعافي من الكوارث
2-1-14	يجب أن تتضمن متطلبات الأمن السيراني لإدارة استمرارية الأعمال بعد أدنى مالي: بوضع خطط التعافي من الكوارث (Disaster Recovery Plan)	ECC		
1-15	يجب تطبيق متطلبات الأمن السيراني الخاصة بخدمات الحوسبة السحابية والإستضافة للجهة .	ECC	١. الفصل المنطقي للبيانات في التخزين السحابي. ٢. مشاركة السجل من مزود الخدمة السحابية. ٣. إدارة مفاتيح التشفير	تم ارفاق السياسة سياسة أمن الحوسبة السحابية
1-16	يجب تطبيق متطلبات الأمن السيراني المتعلقة بالمعاملين في الجهة .	ECC		
1-1-16	أن تغطي متطلبات الأمن السيراني قبل بدء علاقة المعاملين المهاية بالجهة بعد أدنى ما يلي: لضمان مسؤوليات الأمن السيراني وبنود المحافظة على سرية المعلومات (Non-Disclosure في عقود المعاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية	ECC	هل قامت المنظمة بتنفيذ متطلبات كافية للأمن السيراني للأفراد وفقاً للمعايير ،هل تقوم المنظمة بإجراء مسح أمني للموظفين والمقاولين قبل البدء بالعمل ؟	تم ارفاق السياسة سياسة أمن الموارد البشرية معالجة تخفيض الموظف
2-1-16	يجب مراجعة وإلغاء الصلاحيات للمعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهاية لهم بالجهة.	ECC		

شركة نقيات الدوال المعلوماتية المحدودة

Taqnyat

JEDDAH: 4030394715

RIYADH: 1010296254

KHOBAR: 2051240697

يتم استضافة تجهيزات الشركة لدى مزود خدمة مثل نورت وصحاري	لفئة شائعة من الأداة لضمان تنفيذ الأمان المادي	هل لدى المنظمة ضوابط كافية للأمن المادي في الأماكن التي يتم فيها تخزين أو معالجة بيانات العملاء؟ - الوصول المصرح به إلى المناطق الحساسة داخل المنظمة (مثل مركز البيانات، مركز التعافي من الكوارث، مراكز معالجة المعلومات الحساسة، مركز مراقبة الأمن، خزانة الشبكة). - حماية سجلات الدخول والخروج إلى المنشآت وسجلات المراقبة. - أجهزة إنذار الحرائق وأنظمة إطفاء الحرائق. - صلابة الموافقة على الزوار.	ECC	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والتفطن والسرقة والتخريب للجهة بعد أدنى ما يلي: الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها)	الأمن المادي
يتم استضافة تجهيزات الشركة لدى مزود خدمة مثل نورت وصحاري	لفئة شائعة من الأداة لضمان تنفيذ الأمان المادي	هل قامت المنظمة بتفعيل نظام مراقبة بالكاميرات (CCTV) في المواقع التي يتم فيها تخزين ومعالجة بيانات الموظفين والعملاء؟	ECC	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والتفطن والسرقة والتخريب للجهة بعد أدنى ما يلي: سجلات الدخول والمراقبة (CCTV).	
نعم		هل لدى المنظمة سياسة واضحة للزوار؟ - سجل الزوار. - بطاقات تعريف الزوار. - الموافقة على دخول الزوار. - موافقة الزوار داخل المنشأة.	ECC	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والتفطن والسرقة والتخريب للجهة بعد أدنى ما يلي: حماية مخومات سجلات الدخول والمراقبة.	

شركة نقيات الجوال المعلوماتية المحدودة

Taqnyät

JEDDAH: 4030394715
RIVADH: 1010296254
KHOBAR: 2051240697

اعتماد المدير العام للأمن السيبراني


المهندس / محمد الشاطري

شكراً لكم على وقتكم المخصص لاستكمال هذا الإستبيان.
نحن نقدر تعاونكم، وسيتم مراجعة الإجابات وإن تكون نقطة شائعة أو رابط للتوثيق أو وثيقة لاتخاذ القرار.
يرجى إعادة الاستبيان المكتمل على النحو التالي:
عنوان البريد الإلكتروني: alalmuqrin@eamana.gov.sa
خلال ثلاث أيام عمل من استلام الإستبيان: .../.../... هـ.

مع أطيب التحيات،
الإدارة العامة للأمن السيبراني
إدارة الحوكمة والمخاطر والائترام