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.
ستُستخدم 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:

١. اسم الشركة:
٢. الشخص المكلف بالتواصل:
٣. رقم هاتف للتواصل:
٤. عنوان البريد الإلكتروني:
٥. موقع الشركة على الإنترنت:
٦. التوقيع :

سياسات وضوابط الأمن السيبراني لتقييم مخاطر:

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

الاستبيان لتقييم مخاطر السيبرانية للأطراف الخارجية:

النطاق	الرقم	الضابط	المعايير	سؤال الضابط	الأدلة المطلوبة	الطرف الخارجي
الحوكمة والالتزام	١-١	ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها وذلك وفقا لمتطلبات الأعمال التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة .	ECC	هل تم تحديد وتوثيق واعتماد سياسات وإجراءات الأمن السيبراني من قبل الإدارة العليا وإبلاغها إلى الأطراف ذات الصلة داخل المنظمة وخارجها؟	عينة من دليل السياسات - سياسة تتضمن تفاصيل المراجعة والموافقة المناسبة	تم ارفاق سياسة incident management policy

	٢-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للموظفين (قبل التوظيف وأثناء التوظيف وبعد إنهاء الخدمة/الانفصال).	ECC	هل لدى المنظمة عملية محددة لضمان تلبية متطلبات الموظفين الكافية مثل اتفاقية عدم الإفصاح، وإزالة الوصول عند إنهاء الخدمة، والتحقق من خلفية الموظفين بعمل مسح أمني؟	نموذج بند اتفاقية عدم الإفصاح (NDA)	نعم - تم ارفاق نموذج اتفاقية 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	وثيقة سياسة الإستخدام المقبول	نعم يوجد تم ارفاق السياسة
	٤-٢	يجب اعتماد سياسة مكتبية واضحة تهدف إلى ضمان خلو المكاتب من الأوراق الحساسة 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 الآمن	وثيقة سياسة المكتب الآمن	نعم Acceptable Use of Information Assets
	٥-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني 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	وثيقة سياسة إدارة الأصول	نعم Asset Discovery and Asset Classification
	٦-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة الهويات الدخول والصلاحيات في الجهة .	ECC	هل لدى المنظمة سياسة محددة لإدارة الوصول؟ ١. منح حق الوصول ٢. مراجعة الأصول	وثيقة سياسة لإدارة اهويات الدخول والصلاحيات	نعم Cybersecurity in Human Resources
	٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة .	ECC	هل لدى المنظمة إجراءات محددة لأمن البريد الإلكتروني وفحصه؟		نعم
	٨-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة أمن الشبكات للجهة	ECC	هل لدى المنظمة سياسة محددة لإدارة الشبكة؟	وثيقة سياسة أمن الشبكة	نعم Network Security
	٩-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين عند ارتباطها بشبكة الجهة .	ECC	هل لدى المنظمة سياسة BYOD محددة؟	BYOD policy	نعم تم ارفاق السياسة

	٢-١٠	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني 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	تم ارفاق السياسة نعم
	٢-١١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير للجهة	ECC	هل لدى المنظمة سياسة تشفير محددة؟	وثيقة سياسة التشفير	تم ارفاق السياسة نعم
	٢-١٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الإحتياطية للجهة .	ECC	هل لدى المنظمة سياسة/إجراء محدد للنسخ الاحتياطي؟	وثيقة سياسة النسخ الاحتياطي/ الإجراء للنسخ الاحتياطي	تم ارفاق السياسة نعم
	٢-١٥	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لإدارة سجلات الأحداث ومراقبة الأمن السيبراني	ECC	هل لدى المنظمة سياسة/عملية محددة لإدارة السجل؟ ١. الاحتفاظ بالسجل ٢. الوصول إلى السجلات	عملية إدارة السجل	تم ارفاق السياسة نعم
	٢-١٦	يجب تحديد وتوثيق واعتماد متطلبات حوادث الأمن السيبراني وإدارة التهديدات	ECC	هل لدى المنظمة عملية محددة وموثقة لإدارة الحوادث والتهديدات؟	سياسة إدارة الحوادث	تم ارفاق السياسة نعم
	٢-١٨	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب	ECC	هل لدى المنظمة سياسة محددة للأمن المادي؟	وثيقة سياسة الأمن المادي	تم ارفاق السياسة نعم
	٢-١٩	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال لدى الجهة .	ECC	هل لدى المنظمة سياسة/خطة محددة لاستمرارية الأعمال؟	وثيقة سياسة / خطة استمرارية الأعمال	تم ارفاق السياسة نعم
	٢-٢٠	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والإستضافة .	ECC	هل لدى المنظمة سياسة محددة لأمن الحوسبة السحابية؟	وثيقة سياسة أمن الحوسبة السحابية	تم ارفاق السياسة نعم
	٢-٢٢	يجب على الجهة الإلتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني	ECC	هل المنظمة تمتثل لقوانين ولوائح الأمن السيبراني الوطنية المعمول بها؟	تقرير الامتثال NCA	كجهة تتبع هيئة الاتصالات والفضاء والتقنية لا يوجد لدينا تقرير عن الإلتزام بمتطلبات NCA
هندسة الأمن Security) (Architecture	٣-١	يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.	ECC	هل لدى المنظمة سياسة محددة لإدارة التغيير؟ هل تضمن السياسة تغطية متطلبات الأمن السيبراني أثناء تنفيذ التغيير كجزء من دورة حياة المشروع؟	سياسة / منهجية إدارة التغيير	تم ارفاق السياسة نعم
	٣-٢	يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى مايلي :إجراء مراجعة الإعدادات والتحصين وحزم	ECC	هل لدى المنظمة سياسة/عملية محددة لإدارة حزم التحديثات والتي توضح متى يلزم تطبيق التحديث كجزء من التغيير؟	وثيقة سياسة/عملية إدارة حزم التحديثات	تم ارفاق السياسة نعم

		التحديثات قبل إطلاق وتدشين المشاريع والتغييرات				
المخاطر	٤-١	يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة وذلك وفقا لاعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية .	ECC	هل لدى المنظمة منهجية وإجراءات لإدارة مخاطر الأمن السيبراني محددة وموثقة ومعتمدة؟	إطار إدارة المخاطر / المنهجية / السياسة	تم ارفاق السياسة
	٤-٢	يجب تطبيق متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى مايلي	ECC	هل المنظمة تفحص وترقب أنظمتها لرئيسية بشكل روتيني بحثًا عن نقاط الضعف؟	تقرير تحليل نقاط الضعف	
	٤-٢-٤	يجب أن تغطي إجراءات إدارة الثغرات بحد أدنى مايلي وعلى سبيل المثال لا الحصر : إجراءات فحص واكتشاف الثغرات دوريا ،آلية تصنيف الثغرات حسب خطورتها ،إجراءات معالجة الثغرات بناء على تصنيفها	ECC			تم ارفاق السياسة نعم
	٤-٤	يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة (SLA) الأطراف الخارجية التي قد تتأثر بإصابتها ببيانات الجهة أو الخدمات المقدمة لها بحد أدنى مايلي : بنود المحافظة على سرية المعلومات والحذف الآمن من قبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة. (Non-Disclosure Clauses)	ECC	هل تضمن المنظمة أن بنود الأمن السيبراني واتفاقية مستوى الخدمة (SLA) تُدرج كجزء من العقود مع الأطراف الثالثة؟ اتفاقية عدم الإفصاح (NDA) مع الموظفين والمقاولين. إزالة البيانات من قبل الطرف الثالث عند إنهاء الخدمة.	نموذج لبنود العقد	
التوعية والتدريب	٥-١	يجب تطوير واعتماد برنامج للتوعية للأمن السيبراني في الجهة من خلال قنوات متعددة دوريا ،وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره ،وبناء ثقافة إيجابية للأمن السيبراني	ECC	هل لدى المنظمة برنامج محدد للتدريب والتوعية بالأمن السيبراني يغطي مايلي؟ ١. التعامل الآمن مع خدمات البريد الإلكتروني، وخاصة رسائل التصيد الاحتيالي. ٢. التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. ٣. التصفح الآمن للإنترنت.	برنامج التوعية بالأمن السيبراني / الجدول الزمني للخطة	تم ارفاق السياسة نعم
	٥-١-١	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها بما في ذلك :التعامل الآمن مع خدمات البريد الإلكتروني وخاصة رسائل التصيد الإلكتروني .	ECC			
	٥-١-٢	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها بما في ذلك :التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.	ECC			
	٥-٢	يجب أن تغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد	ECC			

		منها بما في ذلك : التعامل الآمن مع خدمات تصفح الإنترنت.				
	٢-٦	يجب تطبيق سياسة الإستخدام المقبول للأصول المعلوماتية والتقنية للجهة.	ECC	هل تضمن المنظمة تنفيذ سياسة الاستخدام المقبول مع فرض قيود مناسبة على استخدام الأصول؟	سياسة الاستخدام المقبول	تم ارفاق السياسة نعم
حماية البيانات والخصوصية	١-٧	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة.	ECC	هل تمتلك المنظمة أدوات كافية لتمكين تصنيف البيانات عبر جميع أقسامها؟ هل تم تحديد، توثيق، والموافقة على متطلبات الأمن السيبراني لحماية البيانات والمعلومات ومعالجتها وفقًا للقوانين واللوائح ذات الصلة؟ ملكية البيانات والمعلومات. آليات تصنيف البيانات والمعلومات ووضع العلامات عليها. خصوصية البيانات والمعلومات	لقطات شاشة من الأدوات المنفذة للتأكد من تصنيف البيانات وتصنيفها	تم ارفاق اللقطات
	١-١-٧	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى مايلي ملكية البيانات والمعلومات	ECC			
	٢-١-٧	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى مايلي تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms)	ECC			
	٣-١-٧	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى مايلي: خصوصية البيانات والمعلومات	ECC			
إدارة الهويات وصلاحيات الدخول	١-٨	يجب تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجهة .	ECC	هل لدى المنظمة عملية وإطار لإدارة الهويات وبيانات الاعتماد والوصول بشكل آمن؟		نعم
	٢-٨	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى مايلي : التحقق من هوية المستخدم (User Authentication) بناء على إدارة تسجيل المستخدم بإدارة كلمة المرور	ECC	هل تمتلك المنظمة عملية مصادقة للمستخدم تعتمد على اسم المستخدم وكلمة المرور؟	لقطات شاشة من الأداة لضمان تنفيذ آلية كلمة المرور المعقدة	تم إرفاق الأدلة
	٣-٨	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى مايلي :التحقق من الهوية متعددة العناصر (Multi-factor Authentication) لعمليات الدخول عن بعد.	ECC	هل تضمن المنظمة أن جميع المستخدمين ملزمون بتسجيل الدخول باستخدام المصادقة متعددة العوامل (MFA)؟	لقطة شاشة للتأكد من تنفيذ MFA للتطبيقات الخارجية	تم إرفاق الأدلة

	٥-٨	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى مايلي :إدارة الصلاحوات الهامة والحساسة (Privileged Access Management)	ECC	هل يتم التحكم في جميع أدوات الوصول لجميع الأنظمة والأجهزة الرئيسية من خلال مبادئ الامتيازات الأقل والفصل بين المهام؟		نعم
	٦-٨	يجب أن تكون أنظمة إدارة الكلمات السرية تفاعلية وأن تضمن كلمات مرور قوية وآمنة	ISO	هل لدى المنظمة سياسة لكلمات المرور؟ الطول المناسب وتحديد كلمة المرور.	لقطة شاشة من الأداة لضمان تطبيق آلية كلمة المرور المعقدة	تم الإرفاق
	٨-٨	يجب تنفيذ عملية رسمية لإدارة الوصول للمستخدمين لتعيين أو إلغاء حقوق الوصول لجميع أنواع المستخدمين إلى جميع الأنظمة والخدمات.	ISO	هل لدى المنظمة عملية تعرف إدارة الوصول للمستخدمين؟	سياسة إدارة الهويات وصلاحيات الدخول	تم إرفاق السياسة
	١-٩	يجب تطبيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة.	ECC	هل قامت المنظمة بتطبيق جدار حماية لتطبيقات الويب (WAF) للتطبيقات الويب الموجهة للجهات الخارجية؟	يتم تنفيذ لقطات الشاشة من أداة التحقق من صحة WAF	WAF يتم تطبيق ال من خلال Mod security
أمن التطبيقات	٢-٩	يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى مايلي: إستخدام جدار الحماية لتطبيقات الويب (application web firewall)	ECC	هل تم تكوين جدران الحماية؟ ١. مراجعة قواعد جدار الحماية ٢. إدارة التغيير	يتم تنفيذ لقطات الشاشة من أداة التحقق من صحة WAF	WAF يتم تطبيق ال من خلال Mod security
	٥-٩	يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى مايلي: التحقق من الهوية متعدد العناصر (Multi-factor Authentication) لعمليات دخول المستخدمين .	ECC	هل تمتلك المنظمة تحكمًا مناسبًا وآمنًا في الوصول أثناء استخدام تطبيقات الويب الخارجية؟	لقطة شاشة من الأداة MFA لضمان تنفيذ للتطبيقات الخارجية	تم الإرفاق
	٢-١٠	يجب تطبيق متطلبات الأمن السيبراني لإدارة أمن الشبكات في الجهة	ECC	هل قامت المنظمة بتطبيق سياسة أمن الشبكة؟ ١. الفصل المنطقي أو المادي وتجزئة أجزاء الشبكة باستخدام جدران الحماية ومبادئ الدفاع المتعمق ؟ ٢. التصفح الآمن والاتصال بالإنترنت بما في ذلك القيود المفروضة على	لقطة شاشة من الأدوات مثل جدار الحماية، IPS، مخطط تقسيم الشبكة	تم الإرفاق
أمن الشبكة	١-٢-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى مايلي : العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن واللازم لسيطرة على مخاطر الأمن السيبراني ذات العلاقة باستخدام جدار الحماية (Firewall)ومبدأ الدفاع الأمني	ECC			

		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 بحد أدنى مايلي :أمن التصفح والاتصال بالإنترنت ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة ومواقع مشاركة وتخزين الملفات ومواقع الدخول عن بعد	ECC		
	٣-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى مايلي : أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems)	ECC	هل لدى المنظمة نظام (IPS) يتم تنفيذه للمراقبة المستمرة للأنشطة الضارة ومنعها؟	لقطة شاشة من الأداة للتأكد من تنفيذ IPS. يمكن أن يكون IPS جزءا من Next Gen Firewall	تم ارفاق الدليل
	٤-١٠	يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى مايلي :أمن نظام أسماء النطاقات (DNS)	ECC	هل لدى المنظمة خدمة اسم المجال (DNS) التي تم تكوينها بشكل أمن؟	لقطة شاشة من الأداة للتأكد من تنفيذ DNS	تم ارفاق الدليل
	٦-١٠	يجب تطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة	ECC	هل لدى المنظمة عملية للنسخ الاحتياطي وأرشفة رسائل البريد الإلكتروني؟ هل تم تطبيق معايير أمان البريد الإلكتروني؟ (مثل DMARC و DKIM و SPF) 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).	لقطة شاشة لتكامل MFA مع البريد الإلكتروني	تم ارفاق الدليل
	١-٦-١٠	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى مايلي:تحليل وتصفية (Filtering) رسائل البريد الإلكتروني (وخصوصا رسائل التصيد الإلكتروني << Phishing Email>> والرسائل الاقتحامية <<Spam Email>>) باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني .	ECC			
أمن البريد الإلكتروني	2-6-10	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى مايلي:التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail)	ECC			
	5-6-10	يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجهة بحد أدنى مايلي: توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية مثل طريقة إطار سياسة المرسل (Sender Policy Framework)	ECC			

	7-10	يجب تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة .	ECC	هل قامت المنظمة بتطبيق تقنية النسخ الاحتياطي؟ اختبارات دورية لفعالية استعادة النسخ الاحتياطية.	لقطة شاشة من الأداة للتأكد من تنفيذ تقنية النسخ الاحتياطي	تم ارفاق الدليل
	1-11	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى مايلي :الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على المستخدمين والخوادم باستخدام تقنيات وآليات 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 ارفاق الدليل
امن نهاية النقاط Endpoint) (Security	2-11	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى مايلي:التقييد الحازم 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 مقيد للاستخدام	تم ارفاق الدليل
	٥-١١	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى مايلي: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
تطوير وصيانة النظام	١-١٢	يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد 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 ارفاق الدليل
Defense & Security Analysis تحليل الدفاع (والأمن)	١-١٣	يجب تطبيق متطلبات الأمن السيبراني لسجلات الأحداث ومراقبة الأمن السيبراني للجهة.	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 ارفاق الدليل
	١-١-١٣	يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بحد أدنى ما يلي:المراقبة المستمرة لسجلات	ECC			

		الأحداث الخاصة بالأمن السيبراني		(يجب أن تكون ١٢ شهرًا على الأقل).		
	٢-١٣	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة .	ECC	هل لدى المنظمة سياسة لإدارة الحوادث؟ خطط الاستجابة لحوادث الأمن السيبراني وإجراءات التصعيد؟	وثيقة التعامل مع الحوادث / عملية التصعيد	تم ارفاق السياسة
	1-2-13	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى مايلي :وضع خطط الإستجابة للحوادث الأمنية وآليات التصعيد.	ECC			
استمرارية الاعمال	1-14	يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال الجهة .	ECC	هل قامت المنظمة بتنفيذ خطة استمرارية الأعمال؟خطط التعافي من الكوارث.	خطة استمرارية الأعمال خطة التعافي من الكوارث	تم ارفاق الخطة
	2-1-14	يجب أن تتضمن متطلبات الأمن السيبراني لإدارة استمرارية الأعمال بحد أدنى مايلي :وضع خطط التعافي من الكوارث(Disaster Recovery Plan)	ECC			
الامن السحابي	1-15	يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة .	ECC	هل لدى المنظمة سياسة حوسبة سحابية مطبقة؟ ١. الفصل المنطقي للبيانات في التخزين السحابي. ٢. مشاركة السجل من مزود الخدمة السحابية. ٣. إدارة مفاتيح التشفير	سياسة أمن الحوسبة السحابية	تم ارفاق السياسة
الموارد البشرية	1-16	يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة.	ECC	هل قامت المنظمة بتنفيذ متطلبات كافية للأمن السيبراني للأفراد وفقًا للمعايير ،هل تقوم المنظمة بإجراء مسح أمني للموظفين والمقاولين قبل البدء بالعمل ؟ .	سياسة أمن الموارد البشرية عملية تخليص الموظف	تم ارفاق السياسة
	1-1-16	أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى ما يلي: تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية	ECC			
	2-1-16	يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.	ECC			

الأمن المادي	1-17	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدن والسرقة والتخريب للجهة بحد 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)	ECC	هل لدى المنظمة ضوابط كافية للأمن المادي في الأماكن التي يتم فيها تخزين أو معالجة بيانات العملاء؟ ١. الوصول المصرح به إلى المناطق الحساسة داخل المنظمة (مثل مركز البيانات، مركز التعافي من الكوارث، مرافق معالجة المعلومات الحساسة، مركز مراقبة الأمن، خزائن الشبكة). ٢. حماية سجلات الدخول والخروج إلى المنشآت وسجلات المراقبة. ٣. أجهزة إنذار الحرائق وأنظمة إطفاء الحرائق. ٤. عملية الموافقة على الزوار.	لقطة شاشة من الأداة لضمان تنفيذ الأمان المادي	يتم استضافة تجهيزات الشركة لدى مزود خدمة مثل نورنت وصحارى
	2-17	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدن والسرقة والتخريب للجهة بحد أدنى ما يلي :سجلات الدخول والمراقبة .(CCTV)	ECC	هل قامت المنظمة بتفعيل نظام مراقبة بالكاميرات (CCTV) في المواقع التي يتم فيها تخزين ومعالجة بيانات الموظفين والعملاء ؟	لقطة شاشة من الأداة لضمان تنفيذ الأمان المادي	يتم استضافة تجهيزات الشركة لدى مزود خدمة مثل نورنت وصحارى
	3-17	يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدن والسرقة والتخريب للجهة بحد أدنى ما يلي :حماية معلومات سجلات الدخول والمراقبة.	ECC	هل لدى المنظمة سياسة واضحة للزوار؟ ١. سجل الزوار. ٢. بطاقات تعريف الزوار. ٣. الموافقة على دخول الزوار. ٤. مرافقة الزوار داخل المنشأة.		نعم

شكرًا لكم على وقتكم المخصص لاستكمال هذا الإستبيان.
نحن نقدر تعاونكم، وسيتم مراجعة الإجابات وان تكون لقطة شاشة 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 و المخاطر والالتزام

اعتماد المدير العام للأمن السيبراني

المهندس / محمد الشاطري