الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني للأنظمة الحساسة

Guide to Critical Systems Cybersecurity Controls Implementation

(GCSCC– 1 : 2023)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

إخلاء مسؤولية: طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة، كما تخلي الهيئة الوطنية مسؤوليتها من الاعتماد على هذه الوثيقة فقط؛ والأخذ بعين الاعتبار المتطلبات الخاصة بالجهة وبيئتها؛ وتؤكد الهيئة الوطنية للأمن السيبراني بأن هذه الوثيقة ماهي إلا دليل إرشادي يمكن استخدامه كمثال ولا تعني بالضرورة أن تكون الطريقة الوحيدة لتطبيق الضوابط على ألا تتعارض الطرق الأخرى مع متطلبات الهيئة الوطنية للأمن السيبراني. تحتوي هذه الوثيقة على بعض الأمثلة للمخرجات ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقيم أو المدقق لضمان التأكد من تطبيق جميع الضوابط.

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للإستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

قائمة الأشكال

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني المنصوص عليها في ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC - 1: 2019) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني للأنظمة الحساسة. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

الأهداف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني للأنظمة الحساسة في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني التي تنشأ من التهديدات السيبرانية الداخلية والخارجية.

نطاق العمل وقابلية التطبيق

نطاق العمل لهذا الدليل كما هو مذكور في ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019):

- الجهات العامة المالكة أو المشغلة للأنظمة الحساسة سواء كانت جهات حكومية داخل المملكة العربية السعودية أو خارجها (مثل الوزارات والهيئات والمؤسسات والسفارات وغيرها) والجهات والشركات التابعة لها وجهات القطاع الخاص، (ويشار لها جميعاً في هذا الوثيقة بـ "الجهة").

- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).

١	حوكمة الأمن السيبراني Cybersecurity Governance	١-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
		١-٣	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects	١-٤	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit
		١-٥	الأمن السيبراني المتعلقة بالموارد البشرية Cybersecurity in Human Resources		
٢	تعزيز الأمن السيبراني Cybersecurity Defense	٢-١	إدارة الأصول Asset Management	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
		٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢-٤	إدارة أمن الشبكات Networks Security Management
		٢-٥	أمن الأجهزة المحمولة Mobile Devices Security	٢-٦	حماية البيانات والمعلومات Data and Information Protection
		٢-٧	التشفير Cryptography	٢-٨	إدارة النسخ الاحتياطية Backup and Recovery Management
		٢-٩	إدارة الثغرات Vulnerabilities Management	٢-١٠	اختبار الاختراق Penetration Testing
		٢-١١	ادارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	حماية تطبيقات الويب Web Application Security
		٢-١٣	حماية التطبيقات Application Security		
٣	صمود الأمن السيبراني Cybersecurity Resilience	٣-١	صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience of Business Continuity Management (BCM)		
٤	الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity

شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة

هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي لضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).

	اسم المكون الأساسي
الرقم المرجعي للمكون الأساسي	
الرقم المرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
الرقم المرجعي للضابط	بنود الضابط
إرشادات تطبيق الضوابط:	
المخرجات المتوقعة:	

شكل ٢: هيكلية الدليل الارشادي لضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019)

إرشادات عامة لتطبيق ضوابط الأمن السيبراني للأنظمة الحساسة

إرشادات عامة
• حصر الأنظمة الحساسة على المستوى الوطني باستخدام أداة حصر الأنظمة الحساسة الصادرة عن الهيئة الوطنية للأمن السيبراني, ومراجعة تقييم حساسية الأنظمة بشكل دوري. • حصر جميع الأنظمة الحساسة ومكوناتها التقنية ومراجعتها سنوياً على الأقل، أو عند حدوث تغييرات تستلزم ذلك. • حصر حسابات المستخدمين ذوي الصلاحيات الهامة والحساسة (Privileged Accounts) والذين لديهم القدرة على الوصول إلى الأنظمة الحساسة أو إدارتها، ومراجعتها بشكل دوري. • تحديد وتوثيق متطلبات الأمن السيبراني للأنظمة الحساسة للجهة والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري. • مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني للأنظمة الحساسة. • وضع خطة لتطبيق ضوابط الأمن السيبراني للأنظمة الحساسة، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	استراتيجية الأمن السيبراني (Cybersecurity Strategy)
الهدف	ضمان احتواء خطط العمل والأهداف والمبادرات والمشاريع داخل الجهة للأمن السيبراني وإسهامها في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	بالإضافة للضوابط ضمن المكون الفرعي ١ - ١ في الضوابط الأساسية للأمن السيبراني، يجب أن تضع إستراتيجية الأمن السيبراني للجهة أولـويـة لدعم حماية الأنظمة الحساسة الخاصة بالجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج استراتيجية الأمن السيبراني. **إرشادات تطبيق الضوابط:** • العمل على تضمين حماية الأنظمة الحساسة الخاصة بالجهة ضمن الأهداف الاستراتيجية للأمن السيبراني ومواءمتها مع الأهداف الإستراتيجية للجهة. • عقد ورش عمل مع أصحاب المصلحة والمعنيين في الجهة لتوضيح أهمية إعطاء أولـويـة لدعم حماية الأنظمة الحساسة الخاصة بالجهة. • إعطاء الأولوية في التنفيذ للمشاريع المتعلقة بالأنظمة الحساسة الخاصة بالجهة عن غيرها من المشاريع. • إعطاء أولوية لتأمين وحماية الأنظمة الحساسة في مشاريع ومبادرات الأمن السيبراني وتوثيق ذلك في خارطة تنفيذ إستراتيجية الأمن السيبراني.
	المخرجات المتوقعة: • وثيقة إستراتيجية الأمن السيبراني المعتمدة من قبل صاحب الصلاحية في الجهة (نسخة إلكترونية أو نسخة ورقية رسمية) لإعطاء أولوية لدعم حماية الأنظمة الحساسة الخاصة بالجهة. • العرض التقديمي لورشة العمل التي تم عقدها مع أصحاب المصلحة والمعنيين في الجهة. • وثيقة خارطة طريق تنفيذ إستراتيجية الأمن السيبراني موضحًا فيها مستوى الإنجاز في تنفيذ المشاريع والمبادرات المتعلّقة بالأنظمة الحساسة الخاصة بالجهة. • جدول مراجعة جرد وتحديث دوري لقائمة الأنظمة الحساسة.
١-٢	إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الضوابط	
١-٢-١	بالإضافة للضوابط ضمن المكون الفرعي ١ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يأتي:
١-٢-١-١	تنفيذ اجراء تقييم مخاطر الأمن السيبراني على الأنظمة الحساسة مرة واحدة سنوياً على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة إدارة مخاطر الأمن السيبراني ● نموذج إجراء إدارة مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** ● العمل على إجراء تقييم مخاطر الأمن السيبراني على الأنظمة الحساسة (التي تم حصرها ضمن مخرجات ضابط رقم ١-١-١-٢) وذلك لتحديد جميع التهديدات المحتملة والتي من الممكن أن تؤثر على سلامة تلك الأنظمة أو تعرض المعلومات التي تعالجها لأي مخاطر سيبرانية أو ثغرات محتملة، مع الأخذ بالاعتبار طبيعة تلك الأنظمة. ● العمل على تقييم مخاطر الأمن السيبراني لكل نظام حساس دوريًا، بحيث يتم مرة واحدة سنوياً على الأقل. ● العمل على إنشاء تقارير بعمليات تقييم مخاطر الأمن السيبراني لكل نظام حساس، على ان يتم توثيق بها ما يلي: ○ المخاطر السيبرانية والثغرات المحتملة. ○ احتمالية حدوث الخطر. ○ نسبة التأثير. ○ مستوى الخطر. ○ المسؤول عن الخطر المحتمل. ○ وصف خطة المعالجة للخطر. ○ الأصول المتأثرة. ● العمل على تطوير خطة معالجة لقائمة مخاطر الأمن السيبراني لكل نظام حساس، واعطاء الأولوية في التنفيذ لخطة معالجة المخاطر المتعلقة بالأنظمة الحساسة عن غيرها من المخاطر.
	المخرجات المتوقعة: ● تقارير تقييم مخاطر الأمن السيبراني الدورية على نطاق الأنظمة الحساسة في الجهة. ● خطط المعالجة لمخاطر الأمن السيبراني لكل نظام حساس. ● تقارير او اثبات يوضح متابعة خطط المعالجة والتحقق من تنفيذها.
١-٢-١-٢	انشاء سجل مخاطر الأمن السيبراني الخاص بالأنظمة الحساسة ومتابعته مرة شهرياً على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سجل مخاطر الأمن السيبراني ● نموذج سياسة إدارة مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:**

	• العمل على إنشاء سجل مخاطر الأمن السيبراني خاص للأنظمة الحساسة أو تضمين المخاطر المتعلقة بالأنظمة الحساسة بشكل واضح ضمن سجل مخاطر الأمن السيبراني العام بالجهةً، بحيث يحتوي على التالي: ○ المخاطر السيبرانية والثغرات المحتملة. ○ احتمالية حدوث الخطر. ○ نسبة التأثير. ○ مستوى الخطر. ○ المسؤول عن الخطر المحتمل. ○ وصف خطة المعالجة للخطر. ○ الأصول المتأثرة. • العمل على تضمين مخاطر الأمن السيبراني الخاصة بالأنظمة الحساسة التي تم تحديدها وتقييمها خلال عملية التقييم، وإسنادها لأصحاب المصلحة. • متابعة سجل مخاطر الأمن السيبراني الخاص بالأنظمة الحساسة دورياً، مرة واحدة شهرياً على الأقل، بحيث يتم متابعة خطط المعالجة والتحقق من تنفيذها وإضافة أي مخاطر جديدة وتوثيق التغييرات في السجل.
	المخرجات المتوقعة: • سجل مخاطر الأمن السيبراني الخاص بالأنظمة الحساسة. • سجل التغييرات الخاصة بسجل مخاطر الأمن السيبراني الخاصة بالأنظمة الحساسة. • تقارير او اثبات يوضح متابعة خطط المعالجة والتحقق من تنفيذها.
١-٣	**الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Project)**
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات ادارة مشاريع الجهة؛ لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة، ودقتها وتوافرها؛ وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-٦-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للأنظمة الحساسة في الجهة، بحد أدنى ما يلي:
١-٣-١-١	إجراء اختبار التحمل للمكونات التقنية للأنظمة الحساسة (Stress Testing) للتأكد من سعة المكونات المختلفة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير **إرشادات تطبيق الضوابط:** • العمل على تحديد أساليب اختبار التحمل للمكونات التقنية للأنظمة الحساسة، باستخدام أحد الأساليب التالية:

		○ اختبار التحمل الموزع (Distributed Stress Testing): وهو عبارة عن توزيع التحمل على عدة أجهزة قد تكون في مناطق جغرافية مختلفة، واختبارها بذات الوقت لفحص قدرتها على التحمل. ○ اختبار التحمل الاستكشافي/التحليلي (Exploratory Stress Testing): وهو عبارة عن اختبار يركز على اكتشاف وتحليل الأخطاء في المكونات التقنية بعد القيام باختبارها وتحليلها بسيناريوهات مختلفة والتي لا يمكن تغطيتها بسهولة في نطاق الاختبارات الأخرى. ○ اختبار التحمل الخاص بالتطبيق (Application Stress Testing): وهو عبارة عن اختبار يركز على الكشف عن الأخطاء المرتبطة بالتطبيقات، والمتعلقة بالأداء ومشكلات الشبكة وحظر البيانات. ○ اختبار التحمل الخاص بالنظام (Systemic Stress Testing): وهو عبارة عن اختبار العديد من الأنظمة التي تعمل على الخادم، لاكتشاف الأخطاء مثل: حظر بيانات أحد البرامج برنامجًا آخر. ○ اختبار التحمل الانتقالي (Transactional Stress Testing): وهو عبارة عن اختبار الضغط الذي يتم إجراؤه على الانتقالات التي تحدث بين التطبيقات، للتأكد من ضبط النظام وتحسينه. • التأكد من توثيق نتائج اختبارات التحمل للمكونات التقنية للأنظمة الحساسة. • التعامل مع البيانات اعتماداً على تصنيفها، بحيث يتم تحديد بيانات وأنظمة خاصة لاختبار التحمل، وألا يتم استخدام بيانات النظام الموجودة في بيئة الإنتاج في عملية اختبار التحمل. • العمل على تحديد و توثيق خطة للتحسين بناء على نتائج الاختبار وتحديث حالة التنفيذ.
		المخرجات المتوقعة: • تقارير تقييم واختبار التحمل للمكونات التقنية للأنظمة الحساسة. • وثيقة توضح عينة البيانات المستخدمة لاختبار التحمل للمكونات التقنية للأنظمة الحساسة وألا تكون من بيانات بيئات الإنتاج. • خطة تحسين وحالة التنفيذ لاختبار التحمل للمكونات التقنية للأنظمة الحساسة.
	١-٣-١-٢	التأكد من تطبيق متطلبات استمرارية الأعمال.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج أدوار ومسؤوليات الأمن السيبراني • نموذج قائمة التحقق من متطلبات الأمن السيبراني لمشاريع تقنية المعلومات وإدارة التغيير • نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال **إرشادات تطبيق الضوابط:** • العمل على إجراء تقييم للمخاطر التي قد تؤثر على استمرارية أعمال.

		• العمل على معالجة الثغرات لتجنب الحوادث التي قد تؤثر على استمرارية الأعمال. • العمل على تحديد المتطلبات التشريعية والتنظيمية الخاصة التي قد تؤثر على إستمرارية أعمال. • العمل على وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال. • العمل على وضع خطط التعافي من الكوارث (Disaster Recovery Plan) لاستمرارية الأعمال. • العمل على تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في الجهة. • تقارير طلبات التغييرات على البنية التحتية على الأصول من أجل تطبيق متطلبات استمرارية الأعمال. • العمل على استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات الأمن السيبراني الخاصة باستمرارية الأعمال.
		المخرجات المتوقعة: • تقارير نتائج عملية تقييم المخاطر التي تؤثر على استمرارية الأعمال. • تقارير نتائج عملية تقييم ومعالجة الثغرات التي تؤثر باستمرارية الاعمال. • تقارير او اثبات يوضح شمول المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال. • خطة الاستجابة لحوادث الأمن السيبراني التي تؤثر على استمرارية الأعمال. • خطط التعافي من الكوارث (Disaster Recovery Plan). • وثيقة توضح تحديد وتوثيق الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في الجهة. • تقارير طلبات التغييرات في الجهة. • تقارير نتائج مؤشر قياس الأداء (KPI) ذات العلاقة باستمرارية الأعمال.
١-٣-٢	بالإضافة للضوابط الفرعية ضمن الضابط ١-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، لمشاريع تطوير التطبيقات، والبرمجيات الخاصة بالأنظمة الحساسة للجهة، بحد أدنى؛ ما يلي:	
	١-٣-٢-١	إجراء مراجعة أمنية للشفرة المصدرية قبل إطلاقها (Security Source Code Review).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة **إرشادات تطبيق الضوابط:** • العمل على تحديد نطاق الشفرة المصدرية المراد مراجعتها قبل إطلاق المشروع. • العمل على مراجعة الشفرة المصدرية إما عن طريق استخدام أدوات تقنية، أو المراجعة بطريقة يدوية، وأن تكون أساليب المراجعة للشفرة المصدرية فعالة للمراجعة على سبيل المثال لا الحصر: (مراجعة الثغرات في الشفرة المصدرية، التأكد من عدم وجود معلومات سرية في الشفرة المصدرية، التاكد من عدم وجود مشاكل أمنية في تصميم الشفرة المصدرية، التأكد من عدم استخدام خوارزميات غير آمنة، مراجعة الشفرة المصدرية باستخدام OWASP).

		• العمل على توثيق نتائج المراجعة وتحديد خطة لمعالجة الملاحظات الخاصة بالشفرة المصدرية. • العمل على تطبيق ومتابعة خطة المعالجة بشكل كامل قبل إطلاق المشروع.
		المخرجات المتوقعة: • إجراءات المراجعة الأمنية للشفرة المصدرية والتي تشمل على: تحديد نطاق الشفرة المصدرية، الأساليب المتخذة لإجراء المراجعة الأمنية للشفرة المصدرية (Source Code). • تقارير نتائج المراجعة الأمنية للشفرة المصدرية (Security Source Code Review). • تقارير خطط التحسين للشفرة المصدرية (Source Code). • تقارير توضح تطبيق ومتابعة خطة التحسين للشفرة المصدرية (Source Code).
	١-٣-٢-٢	تأمين الوصول، والتخزين، والتوثيق للشفرة المصدرية (Source Code) وإصداراتها.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة **إرشادات تطبيق الضوابط:** • العمل على تحديد نطاق الشفرة المصدرية. • العمل على تقييد الوصول للشفرة المصدرية على المطورين ومراجعي الشفرة المصدرية، وذلك من خلال تحديد صلاحيات الوصول على حسب احتياجات ومدة ونطاق العمل. • العمل على تحديد إجراءات للحصول على صلاحيات الوصول من الأشخاص المسؤولين. • العمل على مراجعة صلاحيات الوصول للشفرة المصدرية، وإلغاء الصلاحيات في حال انتهت حاجة العمل أو مدته. • العمل على ضمان تخزين وتوثيق الشفرة المصدرية بطرق آمنة وموثوقة.
		المخرجات المتوقعة: • إجراءات تأمين الوصول، والتخزين، والتوثيق للشفرة المصدرية والتي تشمل على: تحديد نطاق الشفرة المصدرية (Source Code)، والنسخ الاحتياطية للشفرة المصدرية (Source Code). • إجراءات طلب صلاحيات الوصول للشفرة المصدرية (Source Code) من الأشخاص المسؤولين. • عينة من طلبات صلاحيات الوصول للشفرة المصدرية (Source Code). • تقارير من مراجعة صلاحيات الوصول للشفرة المصدرية (Source Code). • قائمة القيود المطبقة على مستوى تأمين الوصول والتخزين للشفرة المصدرية. • قائمة الإصدارات السابقة للشفرة المصدرية والقيود المطبقة لتأمينها.
	١-٣-٢-٣	تأمين واجهة برمجة التطبيقات (Authenticated API).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات

		• نموذج سياسة دورة حياة تطوير البرمجيات الآمنة **إرشادات تطبيق الضوابط:** • العمل على تأمين واجهة التطبيقات عند وجود تكامل (Integration) مع تطبيقات أخرى. • العمل على تقييد الوصول إلى واجهة برمجة التطبيقات، مثل: إعطاء صلاحيات الوصول على حسب نطاق العمل. • التحقق من صلاحيات الوصول إلى واجهة برمجة التطبيقات. • استخدام بروتوكولات آمنة (مثل: TLS) في واجهة برمجة التطبيقات. • العمل على إجراء اختبارات اختراق دورية على واجهة برمجة التطبيقات.
		المخرجات المتوقعة: • لقطة شاشة توضح تأمين واجهة التطبيقات عند جود تكامل (Integration) مع تطبيقات أخرى. • تقارير تقييد الوصول إلى واجهة برمجة التطبيقات. • تقارير التحقق من صلاحيات الوصول إلى واجهة برمجة التطبيقات. • لقطة شاشة من استخدام بروتوكولات آمنة في واجهة برمجة التطبيقات. • تقارير نتائج اختبارات الاختراق على واجهة برمجة التطبيقات.
	٤-٢-٣-١	النقل الآمن والموثوق للتطبيقات من بيئات الاختبار (Testing Environment) إلى بيئات الإنتاج (Production Environment) مع حذف أي بيانات، أو هويات، أو كلمات مرور، متعلقة ببيئات الاختبار، قبل عمليات النقل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات • نموذج سياسة دورة حياة تطوير البرمجيات الآمنة **إرشادات تطبيق الضوابط:** • العمل على حذف أي بيانات أو هويات أو كلمات مرور متعلقة ببيئات الاختبار (Testing Environment) قبل عملية النقل لبيئات الإنتاج (Production Environment). • العمل على تشفير جميع بيانات الأنظمة الحساسة أثناء النقل. • العمل على استخدام أدوات نقل آمنة ومحدثة ومعتمدة. • العمل على توفير خطة عمل لتوضيح نطاق ووقت النقل. • العمل على مراجعة تطبيق خطة العمل للنقل الآمن والتأكد من فعاليتها. • العمل على تطوير إجراءات للنقل واعتمادها.
		المخرجات المتوقعة: • تقارير توضح حذف أي بيانات أو هويات أو كلمات مرور متعلقة ببيئات الاختبار (Testing Environment) قبل عملية النقل لبيئات الإنتاج (Production Environment). • تقارير توضح تشفير جميع بيانات الأنظمة الحساسة أثناء عملية النقل. • تقارير توضح الأدوات المستخدمة لعملية النقل.

		• خطة عمل عملية النقل. • تقارير مراجعة تطبيق خطة العمل لعملية النقل. • إجراءات معتمدة لعملية النقل.
٤-١	المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Assessment Periodical and Audit)	
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرَة تنظيميا على الجهة.	
الضوابط		
١-٤-١	رجوعًا للضابط ١-٨-١ في الضوابط الأساسية للأمن السيبراني، فإنه يجب على الإدارة المعنية بالأمن السيبراني؛ مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة، مرة واحدة سنوياً؛ على الأقل.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على وضع خطة مراجعة تطبيق متطلبات الأمن السيبراني بحيث تشمل جميع الأنظمة الحساسة في الجهة. • العمل على توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية. • التأكد من عرض النتائج على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية، كما يجب أن تشمل النتائج نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وتقييم المخاطر السيبرانية وخطة معالجة الملاحظات. • مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة بشكل سنوي.	
	المخرجات المتوقعة: • خطة مراجعة تطبيق متطلبات أو ضوابط الأمن السيبراني. • تقارير المراجعة الدورية لتطبيق ضوابط الأمن السيبراني للأنظمة الحساسة في الجهة وتشمل خطة معالجة الملاحظات. • محضر اجتماع اللجنة الإشرافية للأمن السيبراني.	
٢-٤-١	رجوعًا للضابط ١-٨-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة؛ من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة، مرة واحدة؛ كل ثلاث سنوات على الأقل.	

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني • نموذج سياسة مراجعة وتدقيق الأمن السيبراني • نموذج سجل خطة تدقيق الأمن السيبراني **إرشادات تطبيق الضوابط:** • التأكد بأن خطة تدقيق الأمن السيبراني من قبل أطراف مستقلة تشمل جميع الأنظمة الحساسة في الجهة. • العمل على مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة يتم على الأقل كل ثلاث سنوات.
	المخرجات المتوقعة: • تقارير التدقيق لضوابط الأمن السيبراني للأنظمة الحساسة؛ من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني من داخل الجهة، مرة واحدة؛ كل ثلاث سنوات على الأقل. • خطة مراجعة تطبيق متطلبات ضوابط الأمن السيبراني. • محضر اجتماع اللجنة الإشرافية للأمن السيبراني. • العمل على توثيق التقارير ومناقشة خطة معالجة الملاحظات مع الإدارات المعنية.
١-٥	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-٩-٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن تغطي متطلبات الأمن السيبراني، قبل بدء علاقة العاملين المهنية بالجهة، بحد أدنى؛ ما يلي:
١-٥-١-١	إجراء المسح الأمني (Screening or Vetting) للعاملين على الأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية **إرشادات تطبيق الضوابط:** • العمل على تحديد المناصب الوظيفية للعاملين المتعلقة بالأنظمة الحساسة المراد إجراء المسح الأمني لها، والتي تشمل على سبيل المثال لا الحصر: ○ مسؤولي قواعد البيانات (Database Administrator) للأنظمة الحساسة.

	○ مسؤولي الشبكة (Network Administrator) للأنظمة الحساسة. ○ مسؤولي النطاق (Domain Administrator) للأنظمة الحساسة. ○ مدراء الأنظمة (System Administrators) من الجانب التقني (Technical Owner) ومن جانب الأعمال (Business Owner) للأنظمة الحساسة. ○ جميع الموظفين المتعاقدين. • العمل على تطوير وتوثيق واعتماد إجراء لعمل المسح الأمني على العاملين على الأنظمة الحساسة بشكل دوري. • إجراء المسح الأمني للمرشحين للعمل على الأنظمة الحساسة كجزء من عملية التوظيف والذي يشمل على سبيل المثال لا الحصر: ○ مراجعة توصيات جهات العمل السابقة، المقدمة من المرشح، والتأكد من صحتها (لذوي الخبرة). ○ التحقق من صحة السيرة الذاتية لمقدم الطلب. ○ التأكد من المؤهلات الأكاديمية والمهنية لمقدم الطلب. ○ التحقق المستقل من الهوية (الهوية الشخصية أو جواز السفر وما شابهه). ○ مراجعة السجلات الجنائية من الجهات المعنية. • العمل على إجراء مسح أمني على جميع العاملين على الأنظمة الحساسة. والذي يمكن أن يشمل على التحقق من: ○ التأكد من كفاءة المرشح اللازمة لأداء دوره بحماية المعلومات. ○ التأكد من أن المرشح محل ثقة لتولي مهام الوظيفة.
	المخرجات المتوقعة: • تقارير مسح أمني للعاملين على الأنظمة الحساسة والتي تشمل على سبيل المثال لا حصر: ○ قائمة بجميع العاملين على الأنظمة الحساسة من الجانب التشغيلي والتقني موضحة جنسياتهم وأدوارهم ومسؤولياتهم. ○ مسح أمني لمسؤولي قواعد البيانات (Database Administrator) للأنظمة الحساسة. ○ مسح أمني لمسؤولي الشبكة (Network Administrator) للأنظمة الحساسة. ○ مسح أمني لمسؤولي النطاق (Domain Administrator) للأنظمة الحساسة. ○ مسح أمني لمدراء الأنظمة (System Administrators) من الجانب التقني (Custodian) ومن جانب الأعمال (Business Owner) للأنظمة الحساسة.
٢-١-٥-١	أن يشغل وظائف الدعم، والتطوير التقني، للأنظمة الحساسة؛ مواطنون ذوو كفاءة عالية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للموارد البشرية **إرشادات تطبيق الضوابط:**

	• العمل على تحديد الوظائف الحساسة الخاصة بالعاملين على الأنظمة الحساسة والتي تشمل على سبيل المثال لا الحصر: ○ الوظائف الإدارية. ○ وظائف الدعم. ○ التطوير التقني. • التأكد من تحديد وتوثيق المتطلبات الخاصة بالكفاءة لكل وصف وظيفي خاص بالعاملين على الأنظمة الحساسة. • التأكد من اختيار وترشيح المواطنين ذوو الكفاءة العالية لشغل الوظائف الإدارية ووظائف الدعم ووظائف التطوير التقني الخاصة بالأنظمة الحساسة.
	المخرجات المتوقعة: • الوصف الوظيفي الخاص بالعاملين الحاليين على الأنظمة الحساسة لدى الجهة والذي يشمل على سبيل المثال لا الحصر: ○ المسمى الوظيفي ○ الغرض من الوظيفة ○ الواجبات والمسؤوليات ○ المؤهلات المطلوبة ○ المؤهلات المفضلة ○ ظروف العمل • السير الذاتية للموظفين العاملين على الأنظمة الحساسة ومنها الوظائف الإدارية ووظائف الدعم والتطوير التقني .

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها.
الضوابط	
٢-١-١	بالإضافة للضوابط ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى؛ ما يلي:
٢-١-١-١	الاحتفاظ بقائمة محدثة سنوياً، لجميع الأصول التابعة للأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول • نموذج معيار تصنيف الأصول • نموذج معيار إدارة الأصول **إرشادات تطبيق الضوابط:** • العمل على تطوير قائمة جرد الأصول للأنظمة الحساسة بصيغة إلكترونية. ويمكن تطبيق عدة طرق لتخزين واستخدام قائمة جرد وحصر الأصول ، على سبيل المثال لا الحصر: ○ قاعدة بيانات إدارة الإعدادات (CMDB). ○ برامج إدارة الأصول. ○ أداة متخصصة في إدارة الأصول. ○ جداول البيانات (spreadsheet). ○ قاعدة البيانات. • العمل على أن تحتوي قائمة جرد الأصول المعلوماتية والتقنية للأنظمة الحساسة على سبيل المثال لا الحصر التالي: ○ نوع الأصول ووصف الأصول. ○ مستوى تصنيف الأصول وتاريخ إعادة التصنيف. ○ متطلبات الالتزام (مثل: تسجيل ما إذا كانت الأصول تندرج ضمن نطاق الخصوصية أو الاحتفاظ بالبيانات أو أي التزام قانوني آخر).

	○ موقع الأصول. ○ مالك الأصول (مثل القائم على حماية الأصول). ● العمل على أن تكون قائمة الجرد مركزية بين الإدارة المعنية بالأمن السيبراني وتقنية المعلومات والإدارات المعنية الأخرى، وعلى أن يتم تحديثها والتأكد من دقتها على الأقل مرة واحدة سنوياً.
	المخرجات المتوقعة: ● قائمة جرد لجميع الأصول للأنظمة الحساسة ومكوناتها التقنية. ● تقارير المراجعة السنوية لقوائم جرد الأصول للأنظمة الحساسة.
٢-١-١-٢	تحديد ملاك الأصول (Asset Owner) وإشراكهم في دورة حياة إدارة الأصول، التابعة للأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة إدارة الأصول **إرشادات تطبيق الضوابط:** ● العمل على تحديد جميع ملاك الأصول للأنظمة الحساسة وتطوير قائمة بجميع المهام والمسؤوليات المترتبة عليهم فيما يخص إدارة الأصول. ● العمل على برنامج توعوي لجميع ملاك الأصول على كيفية القيام بمسؤولياتهم. ● العمل على تطبيق آلية لإشراك جميع الملاك في دورة حياة الأصول، على سبيل المثال لا الحصر: ○ التأكد من إدراج الأصول في قائمة الجرد وتحديثها باستمرار على الأقل سنوياً. ○ تصنيف الأصول. ○ وصف الأصول. ○ الإتلاف الآمن للأصول. ○ التغييرات التي تحدث للأصول.
	المخرجات المتوقعة: ● وثيقة تتضمن جميع ملاك الأصول للأنظمة الحساسة وجميع المهام والمسؤوليات المترتبة عليهم. ● وثيقة إجراءات إشراك الملاك في دورة حياة الأصول.
٢-٢	**إدارة هويات الدخول والصلاحيات (Identity and Access Management)**
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	

٢-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات للأنظمة الحساسة في الجهة، بحد أدنى؛ ما يلي:	
	٢-٢-١-١	منع الدخول عن بعد من خارج المملكة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التصميم والاعدادات الخاصة بالشبكة يجب ألا تسمح بالدخول عن بعد من خارج المملكة للأنظمة الحساسة الغير مرتبطة بالإنترنت، وكذلك للدعم التقني من خارج المملكة للأنظمة الحساسة سواء أكانت مرتبطة بالإنترنت أو غير مرتبطة. ولا يعني ذلك عدم السماح للمستفيدين من الأنظمة الحساسة المرتبطة بالانترنت من الدخول لها. مثل: (ضبط إعدادات VPN لمنع الدخول من خارج السعودية).	
	المخرجات المتوقعة: • قائمة إعدادات ضوابط تقنية لمنع الدخول عن بعد من خارج المملكة للأنظمة الحساسة.	
	٢-٢-١-٢	تقييد الدخول عن بعد من داخل المملكة؛ على أن يتم التأكد عن طريق مركز العمليات الأمنية الخاص بالجهة، عند كل عملية دخول؛ ومراقبة الأنشطة المتعلقة بالدخول عن بعد باستمرار.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات لتقييد الدخول عن بعد من داخل المملكة على سبيل المثال لا الحصر: ○ منع الدخول من داخل المملكة بشكل تلقائي لجميع المستخدمين للأنظمة الحساسة الغير مرتبطة بالإنترنت، وكذلك منع الدخول من داخل المملكة بشكل تلقائي للدعم التقني للأنظمة الحساسة مرتبطة بالإنترنت، وعند الحاجة يتم تقديم سبب الحاجة ثم أخذ الموافقات اللازمة من الإدارة المعنية والإدارة المعنية بالأمن السيبراني وذلك حسب الإجراءات المعتمدة لدى الجهة. ○ إعطاء صلاحية الدخول لمدة محددة فقط حسب الحاجة. ○ إعطاء صلاحية الدخول للنظام الذي تم تحديده في الطلب فقط. ○ إعطاء صلاحية الدخول من داخل المملكة عن طريق أنظمة متخصصة ومعتمدة لدى الجهة على سبيل المثال لا الحصر: نظام (VPN) ونظام (MDM). ○ العمل على حفظ جميع الأنشطة والسجلات لعمليات الدخول عن بعد والتأكد من إرسالها لمركز العمليات والمراقبة لضمان مراقبتها باستمرار من قبل الفرق المتخصصة عن طريق ربط سجلات الدخول مع أنظمة المراقبة مثال: نظام (SEIM).	
	المخرجات المتوقعة:	

• وثيقة إجراءات تقييد الدخول عن بعد من داخل المملكة للأنظمة الحساسة. • وثيقة ضبط إعدادات أنظمة الدخول عن بعد مثل: نظام (VPN). • دليل يوضح مراقبة أحداث الدخول عن بعد عن طريق مركز العمليات الأمنية الخاص بالجهة.	
٢-٢-١-٣	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") لجميع المستفيدين.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات لعمليات الدخول والتي تحتوي على التحقق من الهوية متعدد العناصر (Multi-Factor Authentication). • العمل على تفعيل التحقق متعدد العناصربجانب اسم المستخدم وكلمة المرور وقد يكون مثلًا: ○ كلمة المرور الصالحة لمرة واحدة (One Time Password) في رسالة نصية ترسل لرقم الجوال المسجل للمستفيد. ○ كلمة المرور الصالحة لمرة واحدة (One Time Password) تعرض في برنامج أو جهاز توليد أرقام عشوائية (HardToken) للتحقق من الهوية متعدد العناصر. ○ التحقق من الهوية باستخدام سمات حيوية (مثال: بصمة الإصبع).	
المخرجات المتوقعة: • دليل يوضح تطبيق متطلبات التحقق من الهوية متعدد العناصر لجميع المستخدمين بالانظمة الحساسة على سبيل المثال لا الحصر: لقطة شاشة توضح ضبط إعدادات الأنظمة الحساسة حتى يتم ضمان التأكد من طلب التحقق من الهوية متعدد العناصر.	
٢-٢-١-٤	التحقق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") للمستخدمين ذوي الصلاحيات الهامة، والحساسة؛ وعلى الأنظمة المستخدمة لإدارة الأنظمة الحساسة المذكورة في الضابط ٢-٣-١-٤ ومتابعتها.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات • نموذج معيار أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة **إرشادات تطبيق الضوابط:** • العمل على تحديد الصلاحيات الهامة والحساسة للأنظمة الحساسة (System Administrator) وذلك يشمل على مستوى البنية التحتية والشبكات مثل: (Network Administrtive) والتطبيقات مثل: (Application Administrtive) قواعد البيانات مثل: (Database Administrtive) في الجهة.	

- العمل على تحديد وحصر العاملين الذين لديهم هذه الصلاحيات الهامة والحساسة.
- العمل على تطوير إجراءات إدارة الصلاحيات الهامة والحساسة المعتمدة في الجهة، مع الأخذ بعين الاعتبار التالي:
  - التأكد من الهوية متعدد العناصر لجميع مستخدمي الأنظمة الحساسة ذوي الصلاحيات الهامة والحساسة
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في الأعمال اليومية
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة للوصول إلى الانترنت
  - منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة للوصول للبريد الالكتروني
  - منع استخدا م الحسابات ذات الصلاحيات الهامة والحسّاسة لعمليات الدخول عن بعد، ومنح صلاحية الاستخدام بعد الحصول على موافقة مع تبرير عملي
  - تعطيل الحسابات الحساسة الافتراضية (Default Accounts)
  - التأكد من وجود نظام حماية أجهزة المستخدمين مثبت ومحدث على الجهاز الذي سوف يتم استخدامه للدخول للحسابات ذات الصلاحيات الهامة والحسّاسة
  - بناء نسخ آمنة من أنظمة التشغيل المستخدمة في الجهة وإعدادها بشكل آمن
  - تثبيت برامج الحماية وتعطيل الخدمات الغير مستخدمة. ليتم استخدام هذه النسخ في تهيئة الأجهزة المكتبية والخوادم
- العمل على تحديد التقنيات والآليات الحديثة والمتقدمة لإدارة الصلاحيات الهامة والحساسة.
- التأكد من منح الصلاحيات الهامة والحساسة بناءً على المهام الوظيفية بعد أخذ الموافقات اللازمة، مع الأخذ بالاعتبار مبدأ فصل المهام.
- العمل على تسجيل عمليات الدخول على الحسابات ذات الصلاحيات الها مة والحسّاسة للمتابعة والمراقبة.

المخرجات المتوقعة:.

- قائمة حصر حسابات العاملين الذين لديهم الصلاحيات الهامة والحساسة.
- دليل يوضح تطبيق متطلبات التحقق من الهوية متعدد العناصر لعمليات الدخول على سبيل المثال لا الحصر: لقطة شاشة توضح ضبط إعدادات الأنظمة الحساسة حتى يتم ضمان التأكد من طلب التحقق من الهوية متعدد العناصر للمستخدمين ذوي الصلاحيات الهامة، والحساسة.
- طلبات منح الصلاحيات الهامة والحساسة والموافقات .
- تقارير مراجعة أنشطة الحسابات ذات الصلاحيات الهامة والحساسة.

٢-٢-١-٥	وضع سياسة آمنة لكلمة المرور ذات معايير عالية، وتطبيقها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور

	• نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • ضمان تعريف جميع الموظفين بمعرّف مغاير، قد يكون رقم وظيفي، أو اسم الموظف، أو آليات التسمية الأخرى لضمان أن تكون أسماء المستخدمين فريدة. • العمل على إعداد معايير كلمة المرور على سبيل المثال لا الحصر: ○ أن يكون أقل عدد لرموز كلمة المرور للصلاحيات الهامة والحساسة هو ١٠ وباقي الصلاحيات هو ٨ ○ مدة صلاحية كلمة المرور (Expiration Period) على الأقل ٣٠ يوماً للصلاحيات الهامة والحساسة وباقي الصلاحيات ٩٠ يوماً على الأقل ○ تعقيد كلمة المرور (Complexity) ○ تأمين كلمة المرور (Lockout) ○ تفعيل كلمة المرور (Activation) ○ سجل كلمة المرور (History) ○ أن يكون عدد المحاولات المسموحة هي 3 محاولات ○ أن لا يتم تكرار كلمات المرور التي أُستخدمت خلال المرات الـ 12 الأخيرة ○ أن لا يتم استخدام كلمات المرور بناءً على البيانات الشخصية للمستخدم ذي الصلاحيات والامتيازات، مثل تاريخ الميلاد ○ أن تكون كلمة المرور معقدة وتتضمن على الأقل ٤ رموز من التالي: ▪ أحرف كبيرة (Upper case letters) ▪ أحرف صغيرة (Lower case letters) ▪ أرقام (١٢٣٤) ▪ رموز خاصة (@#%*)
	المخرجات المتوقعة: • ضبط الإعدادات تتضمن المعايير الآمنة لكلمة المرور للأنظمة الحساسة.
٢-٢-١-٦	استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال الاختزال (Hashing Functions).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على توفير الأنظمة والحلول الأمنية لحفظ ومعالجة كلمات المرور والتأكد من أن متطلبات التشفير متوفرة بناءً على المعايير الوطنية للتشفير على سبيل المثال لا الحصر:

	○ العمل على استخدام دوال الاختزال المقبولة بناءً على المعايير الوطنية للتشفير للمستوى المتقدم على سبيل المثال لا الحصر: SHA-256. ○ التأكد من أن دوال الاختزال أن تكون مقاومة للانعكاس (Resistant Inversion) ومقاومة للتعارض (Collision Resistant) ،ومقاومة لإيجاد أصل الصورة (Pre-Resistant image).
	المخرجات المتوقعة: ● وثيقة إجراءات حفظ ومعالجة كلمات المرور للأنظمة الحساسة.
٢-١-٢-٧	الإدارة الآمنة لحسابات الخدمات (Service Account) مابين التطبيقات والأنظمة؛ وتعطيل الدخول البشري التفاعلي (Interactive login) من خلالها.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** ● العمل على تطوير إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن مابين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (Interactive Login) من خلالها على سبيل المثال لا الحصر: ○ العمل على تعطيل جميع حسابات الخدمات وتفعيل الضروري منها فقط. ○ العمل على تحديد حسابات الخدمات التي يحتاجها العمل ويتم استخدامها من قبل الجهة مع الإدارات المعنية. ○ العمل على تعيين مالك لكل حساب للخدمات للتأكد من إدارتها بشكل آمن.
	المخرجات المتوقعة: ● وثيقة إجراءات الإدارة الآمنة لحسابات الخدمات. ● قائمة حصر حسابات الخدمات وملاكها وتبين حالتها (مفعلة أو معطلة). ● القيود المطبقة على عمليات الدخول لهذه الحسابات. ● طلبات الحصول على صلاحية الوصول لحسابات الخدمات.
٢-١-٢-٨	فيما عدا مشرفي قواعد البيانات (Database Administrators)، يمنع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات؛ ويتم ذلك من خلال التطبيقات فقط، وبناءً على الصلاحيات المخوّل بها؛ مع مراعاة تطبيق حلول أمنية تحد، أو تمنع من اطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data).
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة امن قواعد البيانات

	• نموذج معيار امن قواعد البيانات • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات للتعامل مع قواعد البيانات على سبيل المثال لا الحصر: ○ عدم منح صلاحيات الوصول أو التعامل المباشر إلا لمشرفي قواعد البيانات. ○ العمل على تحديد المستخدمين والمشرفين المطلوب وصولهم أو تعاملهم مع قواعد البيانات لمنح الصلاحيات لهم لحاجة العمل مع الإدارة المعنية. ○ العمل على تطوير إجراءات للتأكد من أن المخول له الدخول والوصول لقواعد البيانات عن طريق أجهزة محمية ومحدثة وتحتوي على جميع الحلول الأمنية المطلوبة. ○ العمل على منح الصلاحيات بناءً على الحاجة فقط وإعطاء الصلاحيات لتنفيذ متطلبات العمل المحددة فقط. ○ العمل على تحديد صلاحيات الوصول أو التعامل لتكون من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات. ○ العمل على توفير التقنيات والحلول الأمنية لمنع الاطلاع على البيانات المصنفة (Classified Data) مثل حجب البيانات كلياً أو جزئياً (Data Masking).
	المخرجات المتوقعة: • وثيقة إجراءات التعامل الأمن مع قواعد البيانات للأنظمة الحساسة. • قائمة قواعد البيانات التي تحتوي على البيانات المصنفة وتصنيف البيانات المخزنة عليها. • آلية الموافقة على طلبات صلاحية الدخول لقواعد البيانات. • طلبات الحصول على صلاحية الوصول لقواعد البيانات من خلال مشرفي قواعد البيانات. • القيود المطبقة على الاطلاع على البيانات المصنفة.
٢-٢-٢	رجوعًا للضابط ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول على الأنظمة الحساسة، مرة واحدة، كل ثلاثة أشهر، على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • العمل على مراجعة هويات الدخول والصلاحيات للأنظمة الحساسة في الجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة كل ثلاثة أشهر على الأقل). • العمل على مراجعة جميع هويات الدخول والصلاحيات من جميع النواحي على سبيل المثال لا الحصر: ○ مبدأ الحد الأدنى من الصلاحيات والامتيازات.

	○ مبدأ فصل المهام ومبدأ الحاجة إلى المعرفة والاستخدام بالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). ○ مدة الصلاحية الممنوحة. ○ حالة المخوّل له بالصلاحيات الممنوحة على سبيل المثال لا الحصر: إن كان لا يزال موجود في الإدارة أو تم نقله إلى فريق آخر أو تمت استقالته من الجهة. ● العمل على توثيق جميع المراجعات والتغييرات التي تتم على هويات الدخول والصلاحيات للأنظمة الحساسة الخاصة في الجهة على سبيل المثال لا الحصر: ○ المراجعات الدورية للصلاحيات الممنوحة. ○ التغييرات التي حصلت من آخر مراجعة تمت. ○ التغييرات أو التعديلات المتطلب تغييرها للصلاحيات الممنوحة.
	المخرجات المتوقعة: ● نتائج مراجعة هويات الدخول والصلاحيات للأنظمة الحساسة في الجهة. ● وثيقة تحدد دورة مراجعة هويات الدخول والصلاحيات للأنظمة الحساسة في الجهة (جدول تقييم).
٢-٣	**حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)**
الهدف	ضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنية التحتية للجهة، من المخاطر السيبرانية.
الضوابط	
٢-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢ - ٣ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة الحساسة، وأجهزة معالجة المعلومات الخاصة بها، بحد أدنى؛ ما يلي:
٢-٣-١-١	السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج؛ للعمل على الخوادم الخاصة بالأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة أمن الخوادم ● نموذج معيار أمن الخوادم ● نموذج سياسة الحماية من البرمجيات الضارة ● نموذج معيار الحماية من البرمجيات الضارة ● نموذج معيار أمن البيئة الافتراضية ● نموذج معيار الحماية من التهديدات المستمرة المتقدمة (APT)

إرشادات تطبيق الضوابط:

- العمل على تحديد قائمة ملفات تشغيل للتطبيقات والبرامج المسموح العمل عليها في الخوادم الخاصة بالأنظمة الحساسة واعتمادها، وذلك بإجراء تقييم مخاطر ينتج عنه قائمة بالملفات المسموحة.
- العمل على تحديد تلك القائمة كملفات مسموحة من خلال نظام الحماية الخاص بالخوادم أو من خلال اعدادات الخادم مباشرة.
- العمل على ربط تلك القائمة بالقواعد (Rules) المحددة في نظام إدارة المعلومات والأحداث الأمنية التي تعمل على مراقبة سجلات الخوادم، بحيث يتم متابعة اي استخدام لملفات تشغيل خارج عن تلك القائمة.

المخرجات المتوقعة:

- قائمة ملفات التشغيل المسموحة والمعتمدة التي تم مطابقتها في النظام أو الخادم الخاص بالانظمة الحساسة.

٢-١-٣-٢	حماية الخوادم الخاصة بالأنظمة الحساسة بتقنيات حماية الأجهزة الطرفية (End-point Protection) المعتمدة لدى الجهة.

أدوات الأمن السيبراني ذات العلاقة:

- موذج سياسة أمن الخوادم
- نموذج معيار أمن الخوادم
- نموذج سياسة الحماية من البرمجيات الضارة
- نموذج معيار الحماية من البرمجيات الضارة
- نموذج معيار أمن البيئة الافتراضية
- نموذج معيار الحماية من التهديدات المستمرة المتقدمة (APT)

إرشادات تطبيق الضوابط:

- العمل على تحديد تقنيات الحماية للأجهزة الحساسة والتأكد من احتوائه على التقنيات المناسبة للحماية من الهجمات المتقدمة والمستمرة.
- العمل على تنزيل هذه التقنيات على جميع الخوادم الخاصة بالأنظمة الحساسة في الجهة.
- العمل على متابعة أنظمة الحماية الخاصة بالأنظمة الحساسة بشكل مستمر والتأكد من تفعيل تنبيهات تحديثات النسخ الجديدة.
- العمل على ربط نظام الحماية الخاصة بالأنظمة الحساسة مع نظام إدارة المعلومات والأحداث الأمنية.

المخرجات المتوقعة:

- قائمة أنظمة الحماية الخاصة بالأنظمة الحساسة.
- أنظمة الحماية الخاصة التي تم تنزيلها على الأنظمة الحساسة.

٢-١-٣-٣	تطبيق حزم التحديثات، والإصلاحات الأمنية، مرة واحدة شهرياً على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية؛ مع اتباع آليات التغيير المعتمدة لدى الجهة.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة أمن الخوادم

	• نموذج معيار أمن الخوادم • نموذج معيار أمن الأنظمة الافتراضية • نموذج سياسة إدارة حزم التحديثات والإصلاحات • نموذج معيار إدارة حزم التحديثات والإصلاحات **إرشادات تطبيق الضوابط:** • العمل على تحديد اجراءات تطبيق حزم التحديثات والإصلاحات الأمنية لدى الجهة واعتمادها من قبل صاحب الصلاحية، والتي من الممكن أن تشمل: ○ تطبيق حزم التحديثات والإصلاحات للأنظمة الحساسة الخارجية على الأقل مرة واحدة شهرياً، على سبيل المثال لا الحصر: تطبيقات الويب الخارجية. ○ تطبيق حزم التحديثات والإصلاحات للأنظمة الحساسة الداخلية كل ثلاثة أشهر على الأقل، على سبيل المثال لا الحصر: أنظمة البيانات الخاصة بالتطبيقات الحساسة. ○ التأكد من أن موافقة إدارة التغيير في الجهة جزء من الموافقات المطلوبة لتطبيق حزم التحديثات والإصلاحات الأمنية للأنظمة الحساسة. • متابعة تطبيق حزم التحديثات والإصلاحات الأمنية على الأنظمة الحساسة بشكل مستمر من خلال استخدام أدوات وتقنيات إدارة حزم التحديثات وإدارة الثغرات.
	المخرجات المتوقعة: • اجراءات تطبيق حزم التحديثات والإصلاحات الأمنية للأنظمة الحساسة. • تقارير تطبيق حزم التحديثات والاصلاحات حسب المدة المخطط لها للأنظمة الحساسة.
٢-٣-١-٤	تخصيص أجهزة حاسب (Workstations) للعاملين في الوظائف التقنية، ذات الصلاحيات الهامة والحساسة؛ على أن تكون معزولة في شبكة خاصة، لإدارة الأنظمة (Management Network) وعلى ألا ترتبط بأي شبكة، أو خدمة أخرى (مثل: خدمة البريد الإلكتروني، الإنترنت).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم • نموذج معيار أمن الخوادم • نموذج سياسة الإعدادات والتحصين • نموذج معايير الإعدادات والتحصين الآمن • نموذج معيار أمن البيئة الافتراضية **إرشادات تطبيق الضوابط:** • العمل على تحديد اجهزة حاسب مختلف عن جهاز المستخدم الخاص بالعاملين في الوظائف التقنية ذات الصلاحيات الهامة والحساسة لإدارة الأنظمة الحساسة بها. • العمل على عزل هذه الأجهزة في شبكة خاصة بها ولا ترتبط بأي من شبكات الجهة الأخرى.

- العمل على عزل هذه الأجهزة عن شبكة الانترنت والخدمات والتطبيقات الأخرى المستخدمة من قبل المستخدمين، على سبيل المثال لا الحصر: خدمة البريد الالكتروني، التطبيقات الخاصة لإدارة معلومات العاملين، التطبيقات التي يتم الوصول لها عبر الانترنت.
- العمل على إنشاء حسابات خاصة بهذه الأجهزة ويتم مراقبتها بشكل مستمر من ضمن الحسابات الهامة والحساسة الخاصة بالجهة.

المخرجات المتوقعة:

- أجهزة الحواسيب المعزولة والمخصصة للدخول على الأنظمة الحساسة.
- قائمة الحسابات ذات صلاحية الدخول على هذه الإجهزة والقيود المطبقة لضمان عدم إمكانية استخدامها على أجهزة أخرى.

٢-٣-١-٥	تشفير أي وصول إشرافي عبر الشبكة (Non-console Administrative Access) لأي من المكونات التقنية للأنظمة الحساسة، باستخدام خوارزميات، وبروتوكولات التشفير الآمنة.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة أمن الخوادم
- نموذج معيار أمن الخوادم
- نموذج معيار أمن البيئة الافتراضية
- نموذج سياسة التشفير
- نموذج معيار التشفير

إرشادات تطبيق الضوابط:

- العمل على تحديد معايير التشفير للوصول الإشرافي عبر الشبكة للأنظمة الحساسة والتأكد من مواءمتها مع معايير التشفير الوطنية للمستوى المتقدم ، بحيث:
  - يتم تحديد التقنيات والبروتوكولات الآمنة للاتصال، على سبيل المثال لا الحصر: SSH و TLS.
  - يتم تحديد الحد الأدنى من الطول الخاص بالمفتاح.
- العمل على تخصيص صلاحيات الوصول الإشرافي عبر الشبكة للأنظمة الحساسة واستخدام التحقق من الهوية متعدد العناصر لعمليات الدخول.

المخرجات المتوقعة:

- معيار التشفير للوصول الإشرافي عبر الشبكة.

٢-٣-١-٦	مراجعة إعدادات الأنظمة الحساسة وتحصيناتها (Secure Configuration and Hardening) كل ستة أشهر على الأقل.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة امن الخوادم
- نموذج معيار أمن الخوادم
- نموذج سياسة الإعدادات والتحصين
- نموذج معايير لإعدادات والتحصين الآمن

	• نموذج معيار أمن البيئة الافتراضية **إرشادات تطبيق الضوابط:** • العمل على تحديد المعايير التقنية الآمنة لإعدادات وتحصين الأنظمة الحساسة والتأكد من الحصول عليها من مصادر موثوقة، على سبيل المثال لا الحصر: ○ الشركات المطورة لتلك الأنظمة. ○ المصادر المرجعية الخاصة بالإعدادات والتحصين. • العمل على أن تشمل المعايير التقنية الآمنة لإعدادات وتحصين الأنظمة الحساسة، على سبيل المثال لا الحصر: ○ إدارة الصلاحيات وجلسات الدخول. ○ التشفير. ○ إدارة السجلات. ○ اعدادات النظام الآمنة. • العمل على إجراء مراجعة لإعدادات وتحصين الأنظمة الحساسة بشكل دوري حسب الخطة المحددة بحيث يتم كل ستة أشهر على الأقل. • العمل على توثيق نتائج مراجعة إعدادات وتحصين الأنظمة الحساسة.
	المخرجات المتوقعة: • المعايير الآمنة لتطبيق إعدادات وتحصين الأنظمة الحساسة. • تقارير تطبيق الإعدادات والتحسين الدورية حسب المدة المخطط لها للأنظمة الحساسة.
٢-٣-١-٧	مراجعة الإعدادات المصنعية (Default Configuration) وتعديلها والتأكد من عدم وجود كلمات مرور ثابتة، وخلفية، وافتراضية (Hard-Coded, Backdoor and Default Passwords) ما أمكن تطبيقه.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الخوادم • نموذج معيار أمن الخوادم • نموذج سياسة الإعدادات والتحصين • نموذج معايير الإعدادات الآمنة والتحصين • نموذج معيار أمن البيئة الافتراضية **إرشادات تطبيق الضوابط:** • العمل على مراجعة الإعدادات المصنعية لجميع الأنظمة الحساسة الخاصة بالجهة وتعديلها وتوثيق نتائج المراجعة. • العمل على التأكد من عدم وجود أي كلمات مرور ثابتة، وخلفية، وافتراضية في الأنظمة الحساسة، بحيث: ○ يتم مراجعة الشفرة المصدرية الخاصة بالتطبيقات الخاصة بالجهة وإزالة أي كلمات مرور ثابتة. ○ مراجعة صلاحيات الدخول على الأنظمة الحساسة وتعطيل أي حسابات لا تستخدم أو تم انتهاء صلاحية انشاءها.

	○ تعطيل أو تعديل الحسابات الافتراضية الخاصة بالأنظمة الحساسة، على سبيل المثال لا الحصر: تعطيل الحساب الافتراضي الخاص بقواعد البيانات. ● العمل على توثيق نتائج مراجعة ومعالجة كلمات المرور للأنظمة الحساسة بناء على ما سبق.
	المخرجات المتوقعة: ● تقرير مراجعة الإعدادات المصنعية الخاصة بجميع الأنظمة الحساسة. ● تقارير مراجعة كلمات المرور الخاصة بالأنظمة الحساسة.
٢-٣-١-٨	حماية السجلات، والملفات الحساسة للأنظمة، من الوصول غير المصرح به، أو العبث، أو التغيير، أو الحذف غير المشروع.
	أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة أمن الخوادم ● نموذج معيار أمن الخوادم ● نموذج معيار أمن البيئة الافتراضية ● نموذج الكشف عن تهديدات النقاط النهائية والاستجابة لها(EDR) ● نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني ● نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** ● العمل على حماية السجلات والملفات الحساسة للأنظمة من الوصول غير المصرح به، من خلال التشفير أو وضع كلمة مرور. ● العمل على تخصيص صلاحيات الوصول للسجلات والملفات الحساسة للأنظمة لتشمل مجموعة محددة من العاملين. ● العمل على حماية السجلات والملفات الحساسة من العبث أو التغيير أو الحذف الغير مصرح به من خلال تقييد صلاحيات الكتابة والتعديل والحذف لجميع السجلات والملفات، على سبيل المثال لا الحصر: سجلات الأحداث (logs)، الملفات الخاصة بقواعد البينات، والملفات الخاصة بأنظمة التطبيقات. ● العمل على اخذ نسخ احتياطية من جميع السجلات والملفات الحساسة الخاصة بالأنظمة الحساسة بشكل مستمر.
	المخرجات المتوقعة: ● صلاحيات الدخول للسجلات والملفات الحساسة الخاصة بالأنظمة الحساسة. ● تقارير النسخ الاحتياطي الخاص بالسجلات والملفات الحساسة الخاصة بالأنظمة الحساسة.
٢-٤	إدارة أمن الشبكات (Networks Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.

الضوابط		
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الأنظمة الحساسة للجهة بحد أدنى ما يلي:	
	٢-٤-١-١	العزل والتقسيم المادي، أو المنطقي، لشبكات الأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها (NDR) **إرشادات تطبيق الضوابط:** • العمل على تطبيق العزل والتقسيم المادي (Physical) أو المنطقي (Logical) لشبكة الأنظمة الحساسة على سبيل المثال لا الحصر: ○ العزل باستخدام جدار الحماية (Firewall). ○ العزل للأنظمة الحساسة التي يتم الوصول لها من خارج الجهة في منطقة محايدة (DMZ). ○ العزل لأجزاء الشبكة للأنظمة الحساسة عن طريق الشبكة الداخلية الافتراضية (VLAN). • العمل على منع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية للجهة ولا توجد هناك حاجة للدخول على الخدمة من خارج الجهة. • العمل على ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكات للأنظمة الحساسة تلقائيًا (Explicitly) ، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال ومراجعتها دوريًا.	
	المخرجات المتوقعة: • تخطيط ورسم البنية التحتية لشبكات الأنظمة الحساسة. • قوائم جدار الحماية للأنظمة الحساسة والإعدادات الأخرى الأمنية للشبكات.	
	٢-٤-١-٢	مراجعة إعدادات جدار الحماية (Firewall rules) وقوائمه؛ كل ستة أشهر، على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية	

	• نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها (NDR) **إرشادات تطبيق الضوابط:** • العمل على مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) كل ستة أشهر على الأقل لجدار الحماية الخاص بشبكات الأنظمة الحساسة على سبيل المثال لا الحصر: ○ مراجعة القوائم الغير مستخدمة/مفعلة خلال آخر ٩٠ يوم ليتم حذفها وتعطيلها. ○ تحديث الإعدادات حسب إصدارات المورد الحديثة. ○ ترتيب القوائم حسب الفعالية والأداء. ○ مراجعة وتحليل قوائم VPN. • توثيق نتائج المراجعة بحيث يشمل على سبيل المثال لا الحصر: ○ التغييرات بعد المراجعة. ○ تاريخ المراجعة. ○ الاعتماد.
	المخرجات المتوقعة: • تقرير مراجعة إعدادات جدار الحماية للأنظمة الحساسة في الجهة (جدول تقييم).
٢-٤-١-٣	منع التوصيل المباشر، لأي جهاز بالشبكة المحلية للأنظمة الحساسة؛ إلا بعد الفحص، والتأكد من توافر عناصر الحماية المحققة، للمستويات المقبولة للأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:** • العمل على توفير أنظمة لإدارة تحكم الوصول الأجهزة للشبكات على سبيل المثال لا الحصر: Network Access Control (NAC). • العمل على تطوير إجراءات (لفحص الأجهزة) الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة إلا بعد فحصه باستخدام أدوات فحص واكتشاف البرمجيات الضارة المعتمدة لدى الجهة (End-point protection solutions) والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة على سبيل المثال لا الحصر: ○ العمل على التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة، (مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات

	التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits) وغيرها من البرمجيات الضارة).
	المخرجات المتوقعة: • وثيقة إجراءات الربط الآمن للأنظمة الحساسة بالشبكة المحلية. • إثبات يوضح القيود المطبقة لضمان منع التوصيل المباشر.
٢-٤-١-٤	منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات لمنع ربط الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية على سبيل المثال لا الحصر: ○ عزل شبكة الأنظمة الحساسة عن باقي الشبكات في الجهة. ○ ضبط إعدادات الأنظمة الحساسة أو إعدادات التقنيات الأمنية لمنع الوصول للشبكة اللاسلكية.
	المخرجات المتوقعة: • وثيقة إجراءات منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية. • دليل يوضح ضبط إعدادات الأنظمة الحساسة لمنع الاتصال للشبكة اللاسلكية.
٢-٤-١-٥	الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:**

	• العمل على توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) وتحديثها بشكل مستمر على سبيل المثال لا الحصر: ○ العمل على توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات مثل (Intrusion Prevention/Detection Systems (IDS/IPS,HIDS/HIPS على جميع أجزاء الشبكة وتحديثها بشكل مستمر.
	المخرجات المتوقعة: • قائمة لجميع الأنظمة المتوفرة للحماية من التهديدات المتقدمة المستمرة للأنظمة الحساسة.
٢-٤-١-٦	منع الأنظمة الحساسة من الاتصال بالإنترنت في حال أن كانت تقدم خدمة داخلية للجهة؛ ولا توجد هناك حاجة ضرورية جدًا، للدخول على الخدمة من خارج الجهة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات منع ربط الأنظمة الحساسة على سبيل المثال لا الحصر: ○ العمل مع الإدارات المعنية لتحديد الأنظمة الحساسة التي لا تتطلب للدخول على خدمة من خارج الجهة. ○ العمل على ضبط إعدادات الشبكة لعزل الأنظمة الحساسة الداخلية من الاتصال بالإنترنت على سبيل المثال لا الحصر: ضبط إعدادات جدار الحماية لمنع الاتصال أو تصميم الشبكة يعزل الأنظمة الحساسة من الاتصال بالإنترنت بشكل كلي.
	المخرجات المتوقعة: • وثيقة إجراءات عزل الأنظمة الحساسة بالإنترنت. • دليل يوضح الإعدادات المطبقة على مستوى أجهزة الشبكة والخوادم والتي توضح منع الاتصال بالإنترنت.
٢-٤-١-٧	تقديم خدمات الأنظمة الحساسة، من خلال شبكات مستقلة عن الإنترنت، في حال أن كانت خدمات تلك الأنظمة، موجهة لجهات محدودة؛ وليست للأفراد.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية

	• نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات لتقديم خدمات الأنظمة الحساسة التي تقدم لجهات محدودة عن طريق شبكات مستقلة عن الإنترنت على سبيل المثال لا الحصر: ○ العمل مع الإدارات المعنية لتحديد الأنظمة الحساسة التي تقدم خدمات لخارج الجهة. ○ العمل على توفير الحلول الأمنية لتقديم الخدمات للجهات المحدودة بشكل آمن على سبيل المثال لا الحصر: Site-to-Site VPN. **المخرجات المتوقعة:** • وثيقة إجراءات تقديم خدمات الأنظمة الحساسة. • دليل يوضح الإعدادات المطبقة على مستوى أجهزة الشبكة والخوادم والتي توضح الاتصال من خلال شبكات مستقلة.
٢-٤-١-٨	الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة أمن الشبكات • نموذج معيار أمن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) • نموذج معيار الحماية من هجمات حجب الخدمة الموزعة(DDoS Attacks) **إرشادات تطبيق الضوابط:** • العمل على توفير أنظمة الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على الأنظمة الحساسة وتحديثها بشكل مستمر. • ضبط إعدادات جدار الحماية (Firewall) للحماية من هجمات تعطيل الشبكات والخدمات (Distributed Denial of Service Attack "DDoS"). • العمل على تطبيق مبدأ التوافر المتعدد (High Availability) على الأنظمة الحساسة للجهة والتي تقدم خدمة خارجية على سبيل المثال لا الحصر: أنظمة جدار الحماية, أنظمة الويب (Web Proxy). • العمل على عقد اتفاقية مع مقدم الخدمات أو مزود خدمات الإنترنت من تطبيق آليات وضمان الحماية ضد هجمات تعطيل الشبكات ("DDoS" Distributed Denial of Service Attack). **المخرجات المتوقعة:**

	• أنظمة وتقنيات الحماية من هجمات تعطيل الشبكات للأنظمة الحساسة. • قائمة توضح إعدادات وضوابط الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS"). ٢-٤-١-٩ السماح بقائمة محددة (Whitelisting) فقط، لقوائم جدار الحماية، الخاصة بالأنظمة الحساسة. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة امن الشبكات • نموذج معيار امن الشبكات • نموذج معيار أمن الشبكات اللاسلكية • نموذج معيار الكشف عن تهديدات الشبكات والاستجابة لها(NDR) **إرشادات تطبيق الضوابط:** • العمل على تطوير قائمة سماح محددة (Whitelisting) فقط، لقوائم جدار الحماية، الخاصة بالأنظمة الحساسة ومراجعتها باستمرار. • العمل على ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائيًا (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال ومراجعتها دوريًا. **المخرجات المتوقعة:** • قائمة توضح السماح المحددة لقوائم جدار الحماية الخاصة بالأنظمة الحساسة.
٢-٥	أمن الأجهزة المحمولة (Mobile Devices Security)
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة لبذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بأعمال الجهة؛ وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخثية للعاملين في الجهة (مبدأ «BYOD»).
الضوابط	
٢-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، الخاصة بأمن الأجهزة المحمولة، وأجهزة (BYOD) للجهة، بحد أدنى؛ مايلي: ٢-٥-١-١ منع الوصول من الأجهزة المحمولة للأنظمة الحساسة، إلا لفترة مؤقتة فقط؛ وذلك بعد إجراء تقييم المخاطر، وأخذ الموافقات اللازمة من الإدارة المعنية بالأمن السيبراني في الجهة. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية • نموذج معيار امن أجهزة المستخدمين

	• نموذج معيار امن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • العمل على منع الوصول من جميع الأجهزة المحمولة للأنظمة الحساسة مع الأخذ بالاعتبار أن المقصود به الوصول لأغراض أخرى وليس الوصول كمستخدم نهائي. • العمل على تطوير إجراءات للسماح للوصول لفترة مؤقتة فقط عن الحاجة على سبيل المثال لا الحصر: ○ العمل على تطوير إجراءات لتقييم مخاطر الوصول من الأجهزة المحمولة للأنظمة الحساسة بناءً على حاجة العمل وأخذ الموافقات اللازمة من الإدارة المعنية وإدارة الأمن السيبراني حسب الإجراءات المعتمدة. ○ السماح للوصول لفترة مؤقتة فقط ويتم تعطيل الوصول فور إنتهاء المدة بشكل فوري. ○ السماح للوصول لنظام معين فقط حسب الطلب وليس كل الأنظمة. • تسجيل ومراقبة محاولات الوصول من الأجهزة المحمولة والأنشطة المتعلقة بعمليات الوصول.
	المخرجات المتوقعة: • وثيقة إجراءات تقييم مخاطر الأنظمة الحساسة. • وثيقة إجراءات آليات منح الصلاحيات للأنظمة الحساسة. • عينات من طلبات الموافقة.
٢-١-٥-٢	تشفير أقراص الأجهزة المحمولة، ذات صلاحية الوصول للأنظمة الحساسة، تشفيرًا كاملًا (Full Disk Encryption).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار امن الأجهزة المحمولة • نموذج معيار امن أجهزة المستخدمين • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية **إرشادات تطبيق الضوابط:** • العمل على تشفير جميع أقراص الأجهزة المحمولة للأنظمة الحساسة، تشفيرًا كاملًا باستخدام الطرق المقبولة بناءً على معايير التشفير الوطنية للمستوى المتقدم على سبيل المثال لا الحصر: AES-256-FIPS. • العمل على توفير الأنظمة التقنية والحلول الأمنية التي تطبق متطلبات التشفير المطلوبة.
	المخرجات المتوقعة: • دليل يوضح تطبيق متطلبات التشفير للأنظمة الحساسة.
٢-٦	حماية البيانات والمعلومات (Data and Information Protection)

الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ «BYOD»).	
الضوابط		
٢-٦-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات؛ بحد أدنى، ما يلي:	
٢-٦-١-١	عدم استخدام بيانات الأنظمة الحساسة في غير بيئة الإنتاج (Production Environment) إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Scrambling Data).	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن السيبراني لحماية البيانات • نموذج سياسة الأمن السيبراني لحماية البيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد وتصنيف بيانات الأنظمة الحساسة اعتماداً على المتطلبات التشريعية والتنظيمية ذات العلاقة. • العمل على تحديد واستخدام تقنيات / آليات لحماية بيانات الأنظمة الحساسة عند استخدامها في غير بيئة الإنتاج (Production Environment)، مثل: تقنيات منع تسريب البيانات (Data Leakege Pervention). **المخرجات المتوقعة:** • تقارير من تحديد وتصنيف بيانات الأنظمة الحساسة في الجهة. • قائمة تقنيات / آليات المستخدمة لحماية بيانات الأنظمة الحساسة في الجهة.	
٢-٦-١-٢	تصنيف جميع بيانات الأنظمة الحساسة.	
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني لحماية البيانات • نموذج معيار الأمن السيبراني لحماية البيانات **إرشادات تطبيق الضوابط:** • التأكد من أنه تم تصنيف جميع بيانات الأنظمة الحساسة اعتماداً على المتطلبات التشريعية والتنظيمية ذات العلاقة.	

• العمل على تحديد آليات وطرق التعا مل مع البيانات بناءً على تصنيفها.	
المخرجات المتوقعة: • وثيقة توضح تصنيف جميع بيانات الأنظمة الحساسة مع القواعد المتخذه بناء على تصنيف البيانات.	
٢-١-٦-٣	حماية البيانات المصنفة الخاصة بالأنظمة الحساسة من خلال تقنيات، منع تسريب البيانات (Data Leakage Prevention).
أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن السيبراني للبيانات • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الحماية من فقدان البيانات **إرشادات تطبيق الضوابط:** • العمل على تحديد واستخدام التقنيات / الآليات لمنع تسرب البيانات. • العمل على إعداد حل منع تسرب البيانات (Data Loss Prevention (DLP)) اعتماداً على آلية تصنيف البيانات في الجهة وبناء على الحجم والنوع، وأن يتم تفعيل خاصية التنبيهات عندما تتم محاولة مشاركة البيانات الحساسة خارج الجهة. • العمل على وضع إجراءات للتعامل مع حالات تسرب بيانات الأنظمة الحساسة.	
المخرجات المتوقعة: • تقارير من التقنيات / الآليات المستخدمة لمنع تسرب بيانات الأنظمة الحساسة. • لقطة شاشة توضح تطبيق تقنية تسريب البيانات (DLP) وتفعيل خاصية لتلقي تنبيهات عندما تتم محاولة مشاركة بيانات الأنظمة الحساسة خارج الجهة. • إجراءات التعامل مع حالات تسرب بيانات الأنظمة الحساسة.	
٢-١-٦-٤	تحديد مدة الاحتفاظ المطلوبة (Retention Period) لبيانات الأعمال المتعلقة بالأنظمة الحساسة؛ حسب التشريعات ذات العلاقة، ويتم الاحتفاظ بالبيانات المطلوبة فقط، في بيئات الإنتاج للأنظمة الحساسة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على عقد ورشة عمل مع أصحاب المصلحة للأنظمة الحساسة، بالإضافة إلى أصحاب المصلحة الآخرين ذوي الصلة من وحدات الأعمال لتحديد فترات الاحتفاظ لبيانات الأعمال في الأنظمة الحساسة بناء على نوعية البيانات، حاجة البيانات والتشريعات ذات العلاقة.	

	• العمل مع الإدارات المعنية لحذف بيانات الأعمال التي انتهت مدة الاحتفاظ لها المطلوبة وفقًا لفترات الاحتفاظ لبيانات الأعمال في الأنظمة الحساسة وباستخدام أدوات للتأكد من حذف البيانات، مثل: اتلاف وتدمير الأجهزة التي تحتوي على البيانات الحساسة، الكتابة فوق البيانات الحساسة (Data Overwrite Method).	
	المخرجات المتوقعة: • تقارير فترات الاحتفاظ ببيانات الأعمال في الأنظمة الحساسة، بناء على نوعية وحاجة البيانات. • تقارير من حذف بيانات الأعمال التي انتهت مدة الإحتفاظ لها المطلوبة في الأنظمة الحساسة. • تقارير من الأدوات المستخدمة لحذف بيانات الأنظمة الحساسة.	
	منع نقل أي من بيانات بيئة الإنتاج الخاصة بالأنظمة الحساسة إلى أي بيئة أخرى.	٢-١-٦-٥
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار الأمن السيبراني للبيانات • نموذج سياسة الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • العمل على منع النقل غير المصرح به لبيانات الأنظمة الحساسة من بيئة الإنتاج إلى بيئات أخرى (مثل التطوير والاختبار) وذلك من خلال أساليب مثل: تقييد الوصول وتحديد صلاحيات الوصول إلى بيئة الإنتاج على الفريق المسؤول عن تشغيلها فقط، وضمان عدم وصول المطورين أو المختبرين إلى بيئة الإنتاج.	
	المخرجات المتوقعة: • إجراءات تقييد الوصول وتحديد صلاحيات الوصول إلى بيئة الإنتاج على الفريق المسؤول عن تشغيلها فقط.	
٢-٧	**التشفير (Cryptography)**	
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
الضوابط		
٢-٧-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير، بحد أدنى، ما يلي:	
	تشفير جميع بيانات الأنظمة الحساسة؛ أثناء النقل (Data-In-Transit).	٢-١-٧-١

إرشادات تطبيق الضوابط:

- العمل على تحديد التقنيات المناسبة والمتقدمة؛ لتشفير بيانات الأنظمة الحساسة أثناء النقل، على سبيل المثال لا الحصر:
  - استخدام بروتوكول طبقة النقل الآمنة والتي تعتبر من البروتوكولات التشفير الأكثر شيوعا TLS (Transport Layer Security).
  - تطبيق التقنيات المناسبة والمتقدمة لتشفير بيانات الأنظمة الحساسة أثناء النقل على المستوى المتقدم وفقا لمعيار الهيئة الوطنية للأمن السيبراني.
  - مراجعة فعالية التقنيات المستخدمة لتشفير بيانات الأنظمة الحساسة أثناء النقل.

المخرجات المتوقعة:

- إجراءات تشفير البيانات أثناء النقل في الجهة.
- معايير التشفير المعتمدة في الجهة.
- البروتوكولات والتقنيات المستخدمة لتشفير بيانات الأنظمة الحساسة أثناء النقل.
- تقارير مراجعة فعالية تقنيات التشفير المستخدمة.

٢-١-٧-٢	تشفير جميع بيانات الأنظمة الحساسة؛ أثناء التخزين (Data-At-Rest) على مستوى الملفات، أو قاعدة البيانات، أو على مستوى أعمدة محددة، داخل قاعدة البيانات.

إرشادات تطبيق الضوابط:

- العمل على تحديد التقنيات المناسبة والمتقدمة؛ لتشفير بيانات الأنظمة الحساسة أثناء التخزين، على سبيل المثال لا الحصر:
  - استخدام تشفير البيانات الشفافة التي تستخدم على الأنظمة المحدودة ذات الموارد المقيدة TDE (Transparent Data Encryption)، على سبيل المثال لا الحصر: خوارزميات التشفير الكتلية.
- تطبيق التقنيات المناسبة والمتقدمة لتشفير بيانات الأنظمة الحساسة أثناء التخزين.
- مراجعة فعالية التقنيات المستخدمة لتشفير بيانات الأنظمة الحساسة أثناء التخزين.

المخرجات المتوقعة:

- إجراءات تشفير بيانات الأنظمة الحساسة أثناء التخزين سواء على مستوى الملفات، أو قاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات، في الجهة.
- البروتوكولات والتقنيات المستخدمة لتشفير بيانات الأنظمة الحساسة أثناء التخزين.

٢-١-٧-٣	استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وآمنة وفقًا لما تصدره الهيئة بهذا الشأن.

أدوات الأمن السيبراني ذات العلاقة:

	• نموذج معيار إدارة مفاتيح التشفير **إرشادات تطبيق الضوابط:** • العمل على تحديد خوارزميات ومفاتيح وأجهزة تشفير آمنة عبر الالتزام بمعايير التطبيق الصحيح ومحدثة عبر مراجعتها سنويا والتأكد من أنها تتماشى وفقًا لما تصدره هيئة الأمن السيبراني من معايير تشفير. • استخدام المستوى المتقدم (Advanced) من طرق وخوارزميات التشفير بناءً على المعايير الوطنية للتشفير. • مراجعة فعالية التقنيات المستخدمة للإدارة الآمنة للخوارزميات ومفاتيح وأجهزة التشفير.
	المخرجات المتوقعة: • إجراءات الأمن السيبراني التي تغطي الإدارة الآمنه لخوارزميات ومفاتيح وأجهزة التشفير في الجهة (مثال: نسخة إلكترونية أو نسخة ورقية رسمية). • وثيقة تحدد دورة مراجعة فعالية التقنيات المستخدمة؛ للإدارة الآمنة للخوارزميات ومفاتيح وأجهزة التشفير خلال عمليات دورة حياتها في الجهة. • البروتوكولات والتقنيات المستخدمة لتشفير بيانات الأنظمة الحساسة.
٢-٨	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات الجهة ومعلوماتها والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الاضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية، بحد أدنى؛ ما يلي:
٢-٨-١-١	نطاق عمل النسخ الاحتياطية المتصل، وغير المتصل (Online and Offline Backup) ليشمل جميع الأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار النسخ الاحتياطية • نموذج سياسة النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • العمل على تحديد قواعد البيانات للأنظمة الحساسة. • العمل على تحديد التطبيقات للأنظمة الحساسة. • العمل على تحديد الخوادم للأنظمة الحساسة. • العمل على تحديد أجهزة الشبكة للأنظمة الحساسة.

- تحديد التقنيات المخصصة لعمل النسخ الاحتياطية على الأنظمة الحساسة.
- تطبيق النسخ الاحتياطية لكافة الأنظمة الحساسة.

المخرجات المتوقعة:

- تقارير عمليات النسخ الاحتياطية المتصل وغير المتصل (Online and Offline Backup) الذي يشمل جميع الأنظمة الحساسة التي تحتوي على: نطاق النسخة الإحتياطية، التقنيات المستخدمة لعملية النسخ الإحتياطية في الجهة.
- تقارير من تطبيق النسخ الاحتياطية لكافة الأنظمة الحساسة.

٢-١-٨-٢	عمل النسخ الاحتياطية على فترات زمنية مخطط لها؛ بناءً على تقييم المخاطر للجهة وتوصي الهيئة بأن يتم عمل النسخ الاحتياطية للأنظمة الحساسة بشكل يومي.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج معيار النسخ الاحتياطية
- نموذج سياسة النسخ الاحتياطية

إرشادات تطبيق الضوابط:

- العمل على تقييم المخاطر للجهة وفقًا للسياسات والإجراءات التنظيمية للجهة، ووفقًا المتطلبات التشريعية والتنظيمية ذات العلاقة.
- العمل على تحديد حساسية النظام ومدى الحاجة للبيانات وحداثتها وذلك اعتماداً على نتيجة تقييم المخاطر.
- العمل على تحديد خطة عمل لفترات عمل النسخ الاحتياطية للأنظمة الحساسة.
- العمل على تطبيق خطة عمل النسخ الاحتياطية للأنظمة الحساسة على الفترات الزمنية المتفق عليها.

المخرجات المتوقعة:

- تقارير تقييم المخاطر للجهة.
- خطة عمل للنسخ الاحتياطية للأنظمة الحساسة حسب الخطة الزمنية المبنية على تقييم المخاطر للجهة.
- لقطة شاشة توضح تطبيق النسخ الإحتياطية للأنظمة الحساسة على الفترات الزمنية المتفق عليها.

٢-١-٨-٣	تأمين الوصول، والتخزين، والنقل لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها، وحمايتها من الإتلاف، أو التعديل، أو الاطلاع غير المصرح به.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة أمن وسائط التخزين
- نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي

	• نموذج سياسة النسخ الاحتياطية • نموذج معيار النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • العمل على تأمين الوصول والتعديل والإطلاع غير المصرح به لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها وذلك من خلال على سبيل المثال لا الحصر: تحديد الوصول على حسب الحاجة ونطاق العمل، مراجعة صلاحيات الوصول على فترات منتظمة. • العمل على تأمين التخزين لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها وذلك من خلال على سبيل المثال لا الحصر: تخزين وسائط النسخ الاحتياطي المادية وغير المتصلة بالإنترنت (Offline and physical) خارج الموقع في مكان آمن وموثوق، وتخزين النسخ الاحتياطية المتصلة بالإنترنت بشكل منفصل عن بيئات الإنتاج والاختبار والتطوير. • العمل على تحديد إجراءات النقل الأمن لمحتوى النسخ الاحتياطية للأنظمة الحساسة ووسائطها، وذلك من خلال على سبيل المثلا لا الحصر: تشفير بيانات النسخ الإحتياطية أثناء النقل، استخدام أدوات نقل آمنة ومحدثة ومعتمدة.
	المخرجات المتوقعة: • تقارير صلاحيات الوصول لوسائط التخزين الخاصة بالأنظمة الحساسة. • تقارير مراجعة صلاحيات الوصول خلال فترات منتظمة. • إجراءات النسخ الإحتياطية. • تقارير تشفير النسخ الإحتياطية أثناء النقل. • تقارير الأدوات المستخدمة لنقل الأمن للنسخ الإحتياطية.
٢-٨-٢	رجوعًا للضابط ٢-٩-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب إجراء فحص دوري؛ كل ثلاثة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بالأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار النسخ الاحتياطية • نموذج سياسة النسخ الاحتياطية **إرشادات تطبيق الضوابط:** • العمل على تطوير خطة لإجراء فحص دوري كل ثلاثة أشهر على الأقل؛ لقياس مدى فعالية استعادة النسخ الاحتياطية للأنظمة الحساسة. • العمل على التأكد من فعالية اجراءات الاستعادة، من خلال اجراء اختبار لاستعادة النسخ الاحتياطية للأنظمة الحساسة بشكل دوري؛ كل ثلاثة أشهر على الأقل.
	المخرجات المتوقعة: • خطة عمل لفحص فعالية النسخ الإحتياطية للأنظمة الحساسة.

	• تقارير اختبارات فحص فعالية النسخ الاحتياطية (Backup Restoration Testing) للأنظمة الحساسة لكل ثلاثة أشهر على الأقل.
٢-٩	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٩-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأنظمة الحساسة، بحد أدنى، ما يلي:
٢-٩-١-١	استخدام وسائل وأدوات موثوقة لإكتشاف الثغرات.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية • نموذج سجل الثغرات • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات **إرشادات تطبيق الضوابط:** • العمل على تحديد الأدوات المستخدمة لإكتشاف الثغرات ومراجعتها للتأكد من فعاليتها. • العمل على استخدام أكثر من وسيلة لإكتشاف الثغرات في الأنظمة الحساسة ومن ضمنها: ○ استخدام أكثر من أداة واحدة معتمدة من جهات موثوقة لاكتشاف الثغرات ومن ضمنهم أدوات مفتوحة المصدر (open source) ○ استخدام أدوات اكتشاف الثغرات المعترف بها والموثوقة، والتي يوجد لديها تقارير مستقلة عن اختبار فعالية الأداة ○ مراجعة تنبيهات الثغرات من الموردين ذو العلاقة بالأنظمة الحساسة ○ مراجعة تنبيهات الثغرات من الهيئة الوطنية للأمن السيبراني والمركز الوطني الإرشادي للأمن السيبراني ○ الفحص اليدوي لإكتشاف الثغرات في الأنظمة الحساسة ○ تحديث الأدوات المستخدمة اكتشاف الثغرات
	المخرجات المتوقعة: • قائمة الوسائل والأدوات المستخدمة لإكتشاف الثغرات.

٢-١-٩-٢	تقييم الثغرات ومعالجتها (بتنصيب حزم التحديثات والإصلاحات) على المكونات التقنية للأنظمة الحساسة، مرة واحدة شهرياً، على الأقل، للأنظمة الحساسة الخارجية، والمتصلة بالإنترنت؛ وكل ثلاثة أشهر على الأقل، للأنظمة الحساسة الداخلية.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج إجراء تقييم الثغرات الأمنية
- نموذج سجل الثغرات
- نموذج سياسة إدارة الثغرات
- نموذج معيار إدارة الثغرات

إرشادات تطبيق الضوابط:

- العمل على تحديد الأنظمة الحساسة الخارجية (أي المتصلة بالإنترنت) والأنظمة الحساسة الداخلية ومكوناتهم التقنية حسب جرد الأنظمة الحساسة في الجهة.
- تقييم الثغرات على جميع مكونات الأنظمة الحساسة وتحديد نوعيتها وتصنيف نسبة خطورتها واسناد مالك لها ليتم معالجتها بتنصيب حزم التحديثات والإصلاحات.
- التأكد من أن خطة معالجة الثغرات تتضمن معالجة الثغرات المكتشفة على الأنظمة الحساسة الخارجية ومكوناتها التقنية خلال شهر واحد من وقت اكتشافها.
- التأكد من أن خطة معالجة الثغرات تتضمن معالجة الثغرات المكتشفة على الأنظمة الحساسة الداخلية ومكوناتها التقنية خلال ثلاثة أشهر من وقت اكتشافها.

المخرجات المتوقعة:

- تقارير التقييم وخطط معالجة الثغرات المكتشفة في الأنظمة الحساسة وتقارير تنفيذ هذه الخطط.

٢-١-٩-٣	معالجة فورية للثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثًا؛ مع اتباع آليات إدارة التغيير، المعتمدة لدى الجهة.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج إجراء تقييم الثغرات الأمنية
- نموذج سجل الثغرات
- نموذج سياسة إدارة الثغرات
- نموذج معيار إدارة الثغرات

إرشادات تطبيق الضوابط:

- التأكد من أن خطة معالجة الثغرات تتضمن معالجة الثغرات الحرجة المكتشفة على الأنظمة الحساسة ومكوناتها التقنية فور اكتشافها أو فور الأعلان عنها من مطوري الأنظمة المعتمدين وتحديد الثغرات عبر

	متابعة خطط المعالجة مع اتباع الإجراءات المعتمدة للتغيرات الطارئة عبر رفع الطلبات والحصول على الموافقات اللازمة.
	المخرجات المتوقعة: • خطة معالجة الثغرات الحرجة المكتشفة في الأنظمة الحساسة.
٢-٩-٢	رجوعًا للضابط ٢-١٠-٣-١ في الضوابط الأساسية للأمن السيبراني، يجب فحص الثغرات واكتشافها على المكونات التقنية، للأنظمة الحساسة، مرة واحدة شهريًا؛ على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تقييم الثغرات الأمنية • نموذج سجل الثغرات • نموذج سياسة إدارة الثغرات • نموذج معيار إدارة الثغرات **إرشادات تطبيق الضوابط:** • التأكد من جدولة فحص واكتشاف الثغرات لمكونات الأنظمة الحساسة على سبيل المثال لا الحصر: (التطبيقات، وأجهزة التشفير، وقواعد البيانات، وأجهزة الشبكة) مرة واحدة شهريًا على الأقل.
	المخرجات المتوقعة: • جدول تقارير الفحص واكتشاف الثغرات للأنظمة الحساسة.
٢-١٠	**اختبار الاختراق (Penetration Testing)**
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الاثار المترتبة على أعمال الجهة.
الضوابط	
٢-١٠-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق للأنظمة الحساسة، بحد أدنى؛ ما يلي:
٢-١٠-١-١	نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية للأنظمة الحساسة، وجميع الخدمات المقدمة داخليًا وخارجيًا.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة اختبار الاختراق

	• نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • التأكد من أن أنشطة اختبار الاختراق تشمل جميع الأنظمة الحساسة وجميع مكوناتها التقنية على سبيل المثال: ○ البنية التحتية ○ المواقع الإلكترونية ○ تطبيقات الويب ○ تطبيقات الهواتف الذكية واللوحية ○ البريد الإلكتروني ○ الدخول عن بعد **المخرجات المتوقعة:** • قائمة نطاق عمل أنشطة اختبار الاختراق.
٢-١٠-١-٢	عمل اختبار الاختراق من قبل فريق مؤهل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • استقطاب موارد بشرية مؤهلة لعمل اختبارات الاختراق على الأنظمة الحساسة، او التعاقد مع مزودي خدمات أمن سيبراني، ومن هذه المؤهلات: ○ شهادات مهنية في اختبارات الاختراق (مثل CEH ، GPEN ، OSCP ، eCPPT وغيرها) ○ خبرة عملية في اختبارات الاختراق ○ أن يكون سعودي الجنسية ○ حاصل على درجة علمية في ذات التخصص ○ مكتشف ثغرات حرجة ضمن برامج مكافأة الثغرات **المخرجات المتوقعة:** • السير الذاتية لفريق اختبار الاختراق للأنظمة الحساسة.
٢-١٠-٢	رجوعًا للضابط ٢-١١-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على الأنظمة الحساسة، كل ستة أشهر؛ على الأقل.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة اختبار الاختراق • نموذج معيار اختبار الاختراق **إرشادات تطبيق الضوابط:** • التأكد من أن خطة اختبار الاختراق تشمل عمل اختبارات الاختراق كل ستة أشهر (على الأقل) على جميع الأنظمة الحساسة ومكوناتها التقنية والتي تشمل: ○ التطبيقات ○ الأجهزة والخوادم ○ قواعد البيانات ○ أجهزة الشبكة مثل الموجهات والمبدلات وجدران الحماية • العمل على معالجة الملاحظات المكتشفة خلال اختبار الاختراق
	المخرجات المتوقعة: • خطة عمل اختبار الاختراق للأنظمة الحساسة. • تقارير دورية لاختبارات الاختراق على الأنظمة الحساسة. • دليل يوضح متابعة معالجة الملاحظات المكتشفة.
٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)
الهدف	ضمان تجميع سجلات أحداث الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار المترتبة على أعمال الجهة أو تقليلها.
الضوابط	
٢-١١-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني للأنظمة الحساسة، بحد أدنى؛ ما يلي:
٢-١١-١-١	تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني؛ على جميع المكونات التقنية للأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

إرشادات تطبيق الضوابط:

- العمل على توفير أنظمة مراقبة تتوافق مع مستوى الخطر تقوم بجمع سجلات الاحداث و التحليلات اللازمة، لجمع سجلات الأحداث السيبرانية للأصول التقنية للأنظمة الحساسة ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حدًا أدنى:
  - نوع الحدث (Event Type).
  - مصدر الحدث (IIS, EDR, AV, Sysmon, security logs, etc...)
  - النظام الذي تم تنفيذ الحدث منه (e.g. mailserver)
  - وقت الحدث وتاريخه (Date and Time of Event).
  - المستخدم أو الأداة المستخدمة لتنفيذ الحدث.
  - حالة الحدث أو نتيجته (Success vs. Failure).
- العمل على تفعيل وجمع سجلات الأحداث (Event Logs) والتدقيق (Audit Trial) وعمليات الدخول (Login) لجميع الأصول التقنية للأنظمة الحساسة.
- العمل على إنشاء تنبيهات لأصول المعلومات والتقنية عند حدوث أحداث مراقبة أمنية محددة مسبقًا و / أو استيفاء مستويات المؤشرات المتعلقة بأي نشاط ضار محتمل.

المخرجات المتوقعة:

- إعدادات سجلات الأحداث للأنظمة الحساسة.

٢-١١-١-٢	تفعيل التنبيهات وسجلات الأحداث المتعلقة بإدارة تغييرات الملفات (File Integrity Management) ومراقبتها.

أدوات الأمن السيبراني ذات العلاقة:

- نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

إرشادات تطبيق الضوابط:

- العمل على تحديد وتثبيت التقنيات المناسبة لإدارة ومراقبة تغييرات الملفات.
- العمل على تفعيل التنبيهات وتسجيل الأحداث المتعلقة بإدارة تغييرات الملفات ومراقبتها باستمرار.
- العمل على حماية سجلات أحداث الأمن السيبراني من التغيير والإفشاء والتلف والوصول غير المصرح به والإصدار غير المصرح به على سبيل المثال لا الحصر: تطبيق التشفير وكلمات المرور على السجلات.

المخرجات المتوقعة:

- التقنيات المناسبة لإدارة ومراقبة تغييرات الملفات.

• إعدادات سجلات الأحداث لإرسال تنبيهات تغييرات الملفات للأنظمة الحساسة للفرق المخصصة حتى يتم ضمان التأكد من مراقبتها باستمرار وضمان عدم العبث بها.	
٢-١١-١-٣	مراقبة سلوك المستخدم ("User Behavior Analytics" UBA) وتحليله.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على توفير أنظمة متخصصة لمراقبة سلوك المستخدم وتحليله. • العمل مع الإدارات المعنية في الجهة لتحديد السلوك المقبول للمستخدم على الأنظمة الحساسة ليتم تحديد السلوك المشبوه به. • العمل على تطوير إجراءات أمنية (Incedint response playbook) يتم اتخاذها للحالات التي تم دراستها وتحديدها مع الإدارات المعنية تحت إطار السلوك المشبوه به.	
المخرجات المتوقعة: • قائمة بجميع الأنظمة والإعدادات لمراقبة سلوك المستخدم لضمان التحليل المستمر. • قائمة بجميع الحالات التي تمت دراستها وتحليلها (Use cases). • الإجراءات الأمنية (Incedint response playbook).	
٢-١١-١-٤	مراقبة سجلات الأحداث، الخاصة بالأنظمة الحساسة على مدار الساعة.
أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على مراقبة جميع أحداث الأمن السيبراني للأنظمة الحساسة على مدار الساعة (٣٦٥/٧/٢٤) عن طريق فرق متخصصة.	
المخرجات المتوقعة:	

	• مراقبة سجلات الأحداث الخاصة بالأنظمة على مدار الساعة، على سبيل المثال لا الحصر: جدول يوضح أوقات الفرق المتخصصة للمراقبة على مدار الساعة.
٢-١١-١-٥	الاحتفاظ بسجلات الأحداث، الخاصة بالأمن السيبراني، المتعلقة بالأنظمة الحساسة وحمايتها؛ على أن تكون شاملة، ومتضمنة للتفاصيل كاملة (مثل: الوقت، التاريخ، الهوية، النظام المتأثر).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تطوير إجراءات الاحتفاظ بسجلات الأحداث وعلى أن تكون شاملة ومتضمنة للتفاصيل كاملة بحد أدنى مايلي: ○ نوع سجل الأحداث: مثل النظام، والأمن، والتدقيق، (Kernel)، والتصريح، والبريد، وغيرها. ○ موقع الحدث أو مصدر السجل ونظامه. ○ تاريخ سجل الحدث وختمه الزمني. ○ النظام المتأثر. ○ هوية المستخدم أو الأداة المستخدمة لتنفيذ الحدث. ○ حالة الحدث: مثل ناجح، أو فاشل، أو نشط، أو غير نشط، أو مسموح، أو مرفوض، أو غيره. ○ مستوى خطورة الحدث: مثل طارئ، أو تنبيه، أو حرج، أو خطأ، أو تحذير، أو إشعار معلوماتي، أو إشعار تصحيحي. ○ رسالة الحدث: رسالة فعلية من الحدث. • العمل على تقييد أرشفة وحذف سجلات الأحداث وحصره على المستخدمين المصرّح لهم وذلك فقط بعد انتهاء المدّة الزمنية المحدّدة للاحتفاظ بالسجلات، والسماح للمديرين المعنيين بالأصول المعلوماتية والتقنية بإجراء عملية أرشفة سجلات الأحداث وحذفها.
	المخرجات المتوقعة: • وثيقة إجراءات الاحتفاظ بسجلات الأحداث للأنظمة الحساسة.
٢-١١-٢	رجوعًا للضابط ٢-١٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب أن لا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني، على الأنظمة الحساسة عن ١٨ شهرًا؛ حسب المتطلبات التشريعية، والتنظيمية، ذات العلاقة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:**

	• العمل على تطوير إجراءات الاحتفاظ بسجلات الأحداث لمدة ١٨ شهرًا بالنسبة للأصول الحسّاسة كحد أدنى أو لفترة أطول.
	المخرجات المتوقعة: • وثيقة إجراءات الاحتفاظ بسجلات الأحداث للأنظمة الحساسة.
٢-١٢	**حماية تطبيقات الويب (Web Application Security)**
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، لحماية تطبيقات الويب الخارجية للأنظمة الحساسة للجهة، بحد أدنى؛ ما يلي:
٢-١٢-١-١	الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة حماية تطبيقات الويب • نموذج معيار حماية تطبيقات الويب **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق عملية إدارة آمنة للجلسات (Secure Session Management) حيث يشمل على: ○ موثوقية الجلسات (Authenticity) ○ الدخول (Access) ○ التحكم (Control) ○ الدخول المصرح (Authorization) ○ الإقفال (Lockout) ○ إنهاء مهلتها (Timeout) • العمل على استخدام خادمًا موثوقًا به (Trusted server) لإنشاء معرفات للجلسات. • التأكد من أن وظيفة تسجيل الخروج تنهي الاتصال / الجلسة تمامًا.

	• التأكد من أن مهلة عدم نشاط الجلسة قصيرة قدر الإمكان، ويوصى بأن تكون مهلة نشاط الجلسة أقل من عدة ساعات.	
	المخرجات المتوقعة: • تقرير لأحد الجلسات الآمنة حيث تشمل على: ○ موثوقية الجلسة. ○ وإقفال الجلسة. ○ إنهاء مهلة الجلسة.	
	٢-١-١٢-٢	تطبيق معايير أمن التطبيقات وحمايتها (OWASP Top Ten) في حدها الأدنى.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة حماية تطبيقات الويب • نموذج معيار حماية تطبيقات الويب **إرشادات تطبيق الضوابط:** • العمل على إنشاء منهج للتحقق من تطبيق معايير أمن تطبيقات الأنظمة بشكل دوري حيث لا يقل عن تحديثات سنوية تتبعاً لمنظمة OWASP. • العمل على تطبيق كل معيار أمني للتطبيقات وحمايتها حيث يشمل: ○ خدمة التحكم في الوصول المتعطلة (Broken Access Control). ○ فشل التشفير (Cryptographic Failures). ○ حقن/ضخ (Injection). ○ تصميم غير آمن (Insecure design). ○ خطأ في التكوين الأمني (Security Misconfiguration). ○ المكونات الضعيفة والقديمة (Vulnerable and Outdated Components). ○ فشل تحديد الهوية والمصادقة (Identification and Authentication Failures). ○ فشل البرامج وسلامة البيانات (Software and Data Integrity Failures). ○ تسجيل الأمان وفشل المراقبة (Security Logging and Monitoring Failures). ○ تزوير الطلب من جانب الخادم (Server-Side Request Forgery).	
	المخرجات المتوقعة: • وثيقة توضح تطبيق معايير أمن التطبيقات يوضح فيها الحد الأدنى ومدى التزام الجهة للمعايير.	

٢-١٢-٢	رجوعًا للضابط ٢-١٥-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب استخدام مبدأ المعمارية ذات المستويات المتعددة (Multi-tier Architecture) على أن لا يقل عدد المستويات عن ٣ (3-Tier Architecture).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة حماية تطبيقات الويب • نموذج معيار حماية تطبيقات الويب **إرشادات تطبيق الضوابط:** • العمل على استخدام مبدأ المعمارية ذات المستويات متعددة (Multi-tier Architecture) حيث يتم فصل مكونات تطبيقات الويب الحساسة على ثلاث مستويات على الأقل والتي تتكون من: ▪ طبقة العرض (Presentation/client tier). ▪ طبقة الأعمال (Application/business tier). ▪ طبقة قاعدة البيانات (Database tier).
	المخرجات المتوقعة: • رسم تخطيطي واقعي لتطبيقات الجهة حيث يوضح فيه استخدام مبدأ المعمارية ذات المستويات المتعددة (Multi-tier Architecture).
٢-١٣	**حماية التطبيقات (Application Security)**
الهدف	ضمان حماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة، من المخاطر السيبرانية.
الضوابط	
٢-١٣-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة من المخاطر السيبرانية.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات • نموذج إجراء تطوير وثائق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على تضمين وتوثيق متطلبات الأمن السيبراني لحماية تطبيقات الويب الداخلية في الجهة من المخاطر السيبرانية ومن هذه المتطلبات وعلى سبيل المثال لا الحصر:

	○ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ○ استخدام بروتوكولات آمنة مثل بروتوكول(HTTPS). ○ توضيح سياسة الاستخدام الأمن للمستخدمين. ○ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). • العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بحماية تطبيقات الويب الداخلية. • تضمين متطلبات الأمن السيبراني المتعلقة بحماية التطبيقات الداخلية في إجراءات حماية التطبيقات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثيقة سياسة الأمن السيبراني التي تغطي متطلبات حماية التطبيقات الداخلية للجهة من المخاطر السيبرانية (نسخة الكترونية أو نسخة ورقية رسمية). • موافقة رسمية من قبل رئيس الجهة أو من ينيبه على الوثيقة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني). • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية التطبيقات الدالخلية للجهة. • دليل يؤكد القيام بالمراجعة الدورية لتطبيق متطلبات الأمن السيبراني لحماية التطبيقات الداخلية للجهة. • دليل يوضح تطبيق ضوابط حماية التطبيقات الداخلية الجهة، على سبيل المثال لا الحصر: ○ عينة من تصاميم أحد التطبيقات التي توضح استخدام مبدأ المعمارية متعددة المستويات. ○ لقطة شاشة من تطبيق يوضح فيه استخدام بروتوكول HTTPS. ○ لقطة شاشة من التطبيق يوضح فيه نشر سياسة الاستخدام الأمن للمستخدمين. ○ لقطة شاشة لأحد الجلسات الآمنه حيث تشمل على الموثوقية، وإقفالها، وإنهاء مهلتها.
٢-١٣-٢	يجب تطبيق متطلبات الأمن السيبراني؛ لحماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة.
	إرشادات تطبيق الضوابط: • العمل على تطبيق كافة متطلبات الأمن السيبراني عند تطبيق إجراءات حماية التطبيقات في الجهة، كما يجب أن تغطي إجراءات حماية التطبيقات للجهة بحد أدنى ما يلي وعلى سبيل المثال لا الحصر: ○ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). ○ استخدام بروتوكولات آمنة مثل بروتوكول (HTTPS). ○ توضيح سياسة الاستخدام الأمن للمستخدمين. ○ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

	• العمل على وضع خطة عمل لتطبيق كافة متطلبات الأمن السيبراني المتعلقة بحماية التطبيقات. • تضمين متطلبات الأمن السيبراني المتعلقة بحماية التطبيقات في إجراءات حماية التطبيقات في الجهة لضمان الالتزام بمتطلبات الأمن السيبراني لجميع أصحاب المصلحة الداخليين والخارجيين.
	المخرجات المتوقعة: • وثيقة إجراءات حماية التطبيقات. • وثائق تؤكد تطبيق متطلبات الأمن السيبراني المتعلقة بحماية التطبيقات والتي تم توثيقها في وثيقة السياسات. • وثيقة خطة عمل لتطبيق متطلبات الأمن السيبراني لحماية التطبيقات • دليل يوضح تطبيق ضوابط حماية التطبيقات، على سبيل المثال لا الحصر: ○ لقطة شاشة توضح استخدام مبدأ المعمارية متعددة المستويات في التطبيقات. ○ لقطة شاشة من تطبيق يوضح فيه استخدام بروتوكول HTTPS. ○ لقطة شاشة من التطبيق يوضح فيه نشر سياسة الاستخدام الأمن للمستخدمين. ○ لقطة شاشة لأحد الجلسات الآمنه حيث تشمل على الموثوقية، والإقفال، وإنهاء المهلة.
٢-١٣-٣	يجب أن تغطي متطلبات الأمن السيبراني؛ لحماية التطبيقات الداخلية، الخاصة بالأنظمة الحساسة للجهة، بحد أدنى، ما يلي:
٢-١٣-٣-١	استخدام مبدأ المعمارية ذات المستويات المتعددة (Architecture Multi-tier) على أن لا يقل عدد المستويات عن ٣ (3-Tier Architecture).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات **إرشادات تطبيق الضوابط:** • في حال وجود تطبيقات داخلية تم شراؤها وتشغيلها من طرف خارجي، يجب: ○ التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني والتي تشمل استخدام مبدأ المعمارية متعددة المستويات. • في حال وجود تطبيقات يتم تطويرها داخليًا أو تطبيقات داخلية تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة، يجب: ○ تحديد مستويات مبدأ المعمارية المناسبة لطبيعة تطبيق الويب والتي يجب ألّا تقل عن ثلاثة مستويات: ▪ طبقة العرض (Presentation/client tier). ▪ طبقة الأعمال (Application/business tier). ▪ طبقة قاعدة البيانات (Database tier).

	• العمل على تحديد الإدارات ذات الصلة لتطبيق مبدأ المعمارية متعددة المستويات. • العمل على تطبيق مبدأ المعمارية متعددة المستويات والتي يجب ألّا تقل عن ثلاثة مستويات لجميع تطبيقات الداخلية الخاصة بالجهة.
	المخرجات المتوقعة: • تصميم أحد التطبيقات الداخلية التي توضح استخدام مبدأ المعمارية متعددة المستويات لأحد التطبيقات الخاصة بـ الجهة التي تم تطويرها داخليًا. • تصميم أحد التطبيقات الداخلية التي توضح استخدام مبدأ المعمارية متعددة المستويات لأحد التطبيقات الخاصة بالجهة التي تم شراؤها من طرف خارجي.
٢-١٣-٣-٢	استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات **إرشادات تطبيق الضوابط:** • في حال وجود تطبيقات داخلية تم شراؤها وتشغيلها من طرف خارجي، يجب: ○ التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني والتي تشمل استخدام بروتوكولات آمنة. • في حال وجود تطبيقات يتم تطويرها داخليًا أو تطبيقات داخلية تم شراؤها من طرف خارجي ولكن يتم تشغيلها بالجهة، يجب: ○ العمل على تحديد بروتوكول الاتصالات الآمنة المُراد تطبيقها على التطبيقات الداخلية الخاصة بالجهة والتي تشمل على سبيل المثال لا الحصر: ▪ بروتوكول نقل النص التشعبي الآمن (HTTPS) ▪ بروتوكول نقل الملفات الآمن (SFTP) ▪ بروتوكول أمن طبقة النقل (TLS) ○ العمل على تطبيق وتنزيل بروتوكولات الاتصالات الآمنة في التطبيقات الداخلية الخاصة بالجهة لحمايتها. ○ العمل على إدراج تطبيق وتنزيل بروتوكولات الاتصالات الآمنة في دورة حياة تطوير التطبيقات لضمان حماية التطبيقات المُراد تطويرها مستقبلًا.
	المخرجات المتوقعة: • قائمة البروتوكولات الآمنة المستخدمة في التطبيقات. • تطبيق داخلي يوضح فيه استخدام بروتوكول HTTPS.
٢-١٣-٣-٣	توضيح سياسة الاستخدام الآمن للمستخدمين.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات

	إرشادات تطبيق الضوابط: • العمل على توثيق سياسة الاستخدام الأمن للتطبيقات الداخلية الخاصة بالجهة للمستخدمين. • العمل على تضمين سياسة الاستخدام الأمن في صفحة الدخول للتطبيقات. • التأكد من مشاركة سياسة الاستخدام الأمن للمستخدمين على التطبيقات الداخلية الخاصة بالجهة.
	المخرجات المتوقعة: • سياسة الاستخدام الأمن لمستخدمين للتطبيقات الداخلية. • دليل يوضح نشر سياسة الاستخدام الأمن لمستخدمين التطبيقات الداخلية.
٢-١٣-٣-٤	الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار التطوير الآمن للتطبيقات **إرشادات تطبيق الضوابط:** • العمل على تحديد وتوثيق عملية إدارة آمنة للجلسات (Secure Session Management) حيث يشمل على: ○ موثوقية الجلسات (Authenticity). ○ الدخول (Access). ○ التحكم (Control). ○ الدخول المصرح (Authorization). ○ الإقفال (Lockout). ○ إنهاء مهلتها (Timeout). • العمل على استخدام خادمًا موثوقًا به (Trusted server) لإنشاء معرفات للجلسات. • التأكد من أن وظيفة تسجيل الخروج تنهي الاتصال / الجلسة تمامًا. • التأكد من أن مهلة عدم نشاط الجلسة قصيرة قدر الإمكان، ويوصى بأن تكون مهلة نشاط الجلسة أقل من عدة ساعات.
	المخرجات المتوقعة: • لقطة شاشة لأحد الجلسات الآمنه حيث تشمل على: ○ موثوقية الجلسة. ○ إقفال الجلسة. ○ إنهاء مهلة الجلسة.
٢-١٣-٤	مراجعة متطلبات الأمن السيبراني لحماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة دورياً.

	أدوات الأمن السيبراني ذات العلاقة: • نموذج إجراء تطوير وثائق الأمن السيبراني **إرشادات تطبيق الضوابط:** • العمل على مراجعة تطبيق متطلبات الأمن السيبراني لحماية التطبيقات للجهة من خلال إجراء تقييم دوري (وذلك حسب خطة موثقة ومعتمدة للمراجعة، وبناء على فترة زمنية محددة "على سبيل المثال، بشكل ربع سنوي") لحماية التطبيقات من قبل الإدارة المعنية بالأمن السيبراني وبالتعاون مع الإدارات ذات العلاقة (كالإدارة المعنية بتقنية المعلومات). • مراجعة التطبيق قد تتم من خلال القنوات التقليدية (مثل البريد الإلكتروني) أو قد يكون مؤتمت باستخدام نظام لإدارة الالتزام. الجهة قد تضع خطة مراجعة توضح فيها جدول مراجعة تطبيق متطلبات الأمن السيبراني لحماية التطبيقات للجهة. • مراجعة وتحديث متطلبات الأمن السيبراني لحماية التطبيقات للجهة بشكل دوري حسب خطة موثقة ومعتمدة للمراجعة بناءً على فترة زمنية محددة أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. • توثيق المراجعة والتغييرات التي تتم على متطلبات الأمن السيبراني لحماية التطبيقات في الجهة واعتمادها من قبل رئيس الجهة أو من ينيبه. **المخرجات المتوقعة:** • وثيقة السياسة بما يوضح أنه تم مراجعتها وتحديثها وتم توثيق التغييرات واعتمادها من قبل رئيس الجهة أو من ينيبه. • الموافقة الرسمية والاعتماد من قبل رئيس الجهة أو من ينيبه على السياسة المحدثة (مثال: عن طريق البريد الإلكتروني الرسمي للجهة، أو التوقيع الورقي أو الإلكتروني).

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

١-٣	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

الضوابط		
١-١-٣	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي إدارة استمرارية الأعمال في الجهة، بحد أدنى؛ ما يلي:	
	١-١-١-٣	وضع مركز للتعافي من الكوارث للأنظمة الحساسة.
	إرشادات تطبيق الضوابط: • العمل على وضع مركز للتعافي من الكوارث للأنظمة الحساسة، حيث يشمل: ○ تحديد إما أن يكون مركز التعافي منشأ من قبل الجهة أو يكون خدمة سحابية مقدمة من طرف ثالث، في حال كانت الخدمة مقدمة من طرف ثالث: ▪ يجب أن يكون مقر استضافة مركز التعافي من الكوارث داخل المملكة العربية السعودية. ○ في حال أن الجهة أرادت إنشاء مركز تعافي خاص بها، يلزم بإعداد وتجهيز مركز التعافي حيث يشمل على سبيل المثال لا الحصر: ▪ فصل مركز التعافي من الكوارث الخاص بالأنظمة الحساسة عن الأنظمة الأخرى. ▪ التخزين الكلي للأجهزة (Hardware) والبرامج (Software) والمعدات الأخرى. ▪ توثيق أهداف العمل (Business objectives). ▪ تعريف وتحديد الوقت/الحد المسموح للعطل وخسارة البيانات. ▪ وجود فريق مختص بمركز التعافي. ▪ وجود مساحات عمل بديلة/احتياطية. ▪ تفعيل خيار الوصول عن بعد (Remote access). ▪ تأمين النسخ الاحتياطية. ▪ استراتيجية اختبار شاملة. • العمل على تحديد منطقة جغرافية ونطاق لمركز التعافي من الكوارث الخاص بالأنظمة الحساسة بعيد عن مركز البيانات الخاصة بالأنظمة الحساسة.	
	المخرجات المتوقعة: • الرسم التخطيطي لشبكة الجهة. • تصميم مركز التعافي الخاص بالجهة.	
	٢-١-١-٣	إدراج الأنظمة الحساسة؛ ضمن خطط التعافي من الكوارث.

إرشادات تطبيق الضوابط:

- العمل على إدراج الأنظمة الحساسة؛ ضمن خطط التعافي من الكوارث، حيث يشمل:
  - تحديد فريق خاص بالأنظمة الحساسة لتفعيل الإجراءات في خطط التعافي من الكوارث.
  - تحديد وتقييم المخاطر المؤثرة على الأنظمة الحساسة.
  - تحديد إجراءات النسخ الاحتياطي والتخزين الخارجي للأنظمة الحساسة.

المخرجات المتوقعة:

- خطط التعافي من الكوارث الموثقة والمعتمدة للجهة والتي تشمل الأنظمة الحساسة.

٣-١-١-٣	إجراء اختبارات دورية؛ للتأكد من فعالية خطط التعافي، من الكوارث للأنظمة الحساسة، مرة واحدة سنوياً؛ على الأقل.

إرشادات تطبيق الضوابط:

- العمل على إجراء اختبارات دورية؛ للتأكد من فعالية خطط التعافي، من الكوارث للأنظمة الحساسة، مرة واحدة سنوياً؛ على الأقل، حيث يشمل:
  - تحديد وتوثيق جدول اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة.
  - العمل على تحديد و توثيق مدة إجراء الاختبار بشكل دوري حيث لا يقل عن مرة واحدة سنوياً.
  - اعتماد جدول الاختبارات الدورية للتأكد من فعالية خطط التعافي من قبل ذوي الصلاحية.
  - تـ حديد وتوثيق خطة لمعالجة الملاحظات المُكتشفة أثناء إجراء الاختبار الدوري للتأكد من فعالية خطط التعافي.

المخرجات المتوقعة:

- تقرير محدث لإجراء اختبار فعالية خطط التعافي من الكوارث للأنظمة الحساسة.
- خطة إجراء اختبارات فعالية خطط التعافي من الكوارث للأنظمة الحساسة في الجهة.

٣-١-١-٤	توصي الهيئة بإجراء اختبار دوري حي؛ للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.

إرشادات تطبيق الضوابط:

- توصي الهيئة بإجراء اختبار دوري حي؛ للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة، حيث يشمل:
  - تحديد الهدف والغاية والإجراءات التي يجب اتخاذها لإنشاء تحليل ما بعد الاختبار.
  - تحديد نطاق الاختبار.
  - تأكيد أن بيئة الاختبار جاهزة، ولن تؤثر على أنظمة الإنتاج أو تتعارض مع الأنشطة الأخرى.

	○ إيقاف ومراجعة الاختبار عند ظهور مشاكل وإعادة جدولته إذا لزم الأمر.
	المخرجات المتوقعة: • الجدول الدوري لاختبارات التعافي من الكوارث الدوري الحية للأنظمة الحساسة. المعتمد بالجهة (Live DR Testing Schedule). • تقرير حديث لأحد اختبارات التعافي من الكوارث الحية للأنظمة الحساسة.

٤ الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third Party Cybersecurity)
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services"). وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٤-١-١	بالإضافة للضوابط ضمن المكون الفرعي ٤-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني، المتعلقة بالأطراف الخارجية، بحد أدنى؛ ما يلي:
٤-١-١-١	إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • العمل مع الإدارات ذات العلاقة على ضمان إجراء المسح الأمني (Screening or Vetting) للأطراف الخارجية العاملة على الأنظمة الحساسة، للتحقق من السجل الجنائي للشركات والعاملين ومن ضمنهم: ○ شركات خدمات الإسناد. ○ موظفي خدمات الإسناد. ○ شركات الخدمات المدارة للأنظمة الحساسة. ○ موظفي الخدمات المدارة العاملين على الأنظمة الحساسة.
	المخرجات المتوقعة: • وثيقة رسمية من الجهات المختصة توضّح إجراء المسح الأمني للعاملين على الأنظمة الحساسة.
٤-١-١-٢	أن تكون خدمات الإسناد، والخدمات المدارة على الأنظمة الحساسة؛ عن طريق شركات، وجهات وطنية؛ وفقًا للمتطلبات التشريعية، والتنظيمية ذات العلاقة.
	أدوات الأمن السيبراني ذات العلاقة:

	• نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • التأكد من أن خدمات الإسناد ومراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة للأنظمة الحساسة تُدار عن طريق شركات وطنية من خلال بذل العناية الواجبة و عبر حصول الشركات على توصية الهيئة الوطنية للأمن السيبراني، وضمان التزام الشركات والجهات المحلية بالمتطلبات التشريعية والتنظيمية ذات العلاقة. **المخرجات المتوقعة:** • عقود واتفاقيات مستوى الخدمة (SLA) مع الأطراف الخارجية لخدمات الإسناد ومراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة للأنظمة الحساسة. • وثيقة رسمية تُثبت أن مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة للأنظمة الحساسة موجودة بالكامل داخل المملكة العربية السعودية، (مثال: وجوده كأحد بنود العقد الموقع أو وجود اتفاقية مستوى الخدمة (SLA) موقّعه بين الطرف الخارجي والجهة أو زيارة الجهة لمقر عمل مقدم الخدمة). • إقرار من مقدم خدمات الإسناد ومراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة للأنظمة الحساسة على الالتزام بكافة السياسات والإجراءات الداخلية الخاصة بخدمات الإسناد والخدمات المدارة للجهة والالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤-٢	**الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)**
الهدف	ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.
الضوابط	
٤-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٤-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة، بحد أدنى؛ ما يلي:
٤-٢-١-١	أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل الجهة، أو في خدمات الحوسبة السحابية، المقدمة من قبل جهات حكومية، أو شركات وطنية محققة لضوابط الحوسبة السحابية الصادرة من الهيئة مع مراعاة تصنيف البيانات المستضافة.
	أدوات الأمن السيبراني ذات العلاقة:

	• نموذج سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة **إرشادات تطبيق الضوابط:** • التأكد من تصنيف وترميز البيانات بما يتوافق مع آلية التصنيف والترميز في الجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة. • التأكد من استضافة الأنظمة الحساسة الخاصة بالجهة، أو أي جزء من مكوناتها التقنية في مكان موثوق وآمن داخل المملكة العربية السعودية، ومن هذه الأماكن ما يلي: ○ أن يتم استضافة البيانات داخل الجهة. ○ أن يتم استضافة البيانات لدى مقدمي خدمات الحوسبة السحابية المقدمة من قبل جهات حكومية في المملكة العربية السعودية. ○ أن يتم استضافة البيانات لدى مقدمي خدمات الحوسبة السحابية المقدمة من قبل شركات خاصة بحيث تكون شركات سعودية مُحقِقَة لضوابط الحوسبة السحابية «CCC» الصادرة من الهيئة الوطنية للأمن السيبراني. ○ اضافة دراسة جدوى وتقييم مخاطر للشركات الخاصة والحصول على توصية من الهيئة الوطنية للأمن السيبراني.
	المخرجات المتوقعة: • عقود واتفاقيات الجهة مع مقدم خدمة الحوسبة السحابية والاستضافة للأنظمة الحساسة. • إقرار من مقدم خدمة الحوسبة السحابية على الالتزام بكافة السياسات والإجراءات الداخلية الخاصة بخدمات الحوسبة السحابية والاستضافة للجهة والالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة. • قائمة البيانات التي تم تصنيفها قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية، وعلى سبيل المثال لا الحصر: (ملف) موضّح فيه البيانات التي تم تصنيفها قبل مشاركتها مع مقدم خدمة الحوسبة السحابية والاستضافة. • وثيقة رسمية تُثبت أن استضافة الأنظمة الحساسة الخاصة بالجهة، أو أي جزء من مكوناتها التقنية في مكان موثوق وآمن داخل المملكة العربية السعودية.