الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

الضوابط الأساسية للأمن السيبراني

Essential Cybersecurity Controls

ليبيا
فبراير - 2026
رقم الإصدار 1.0
www.nissa.gov.ly
© NISSA - Feb. 2026

إعداد

قسم السياسات والمعايير

مراجعة

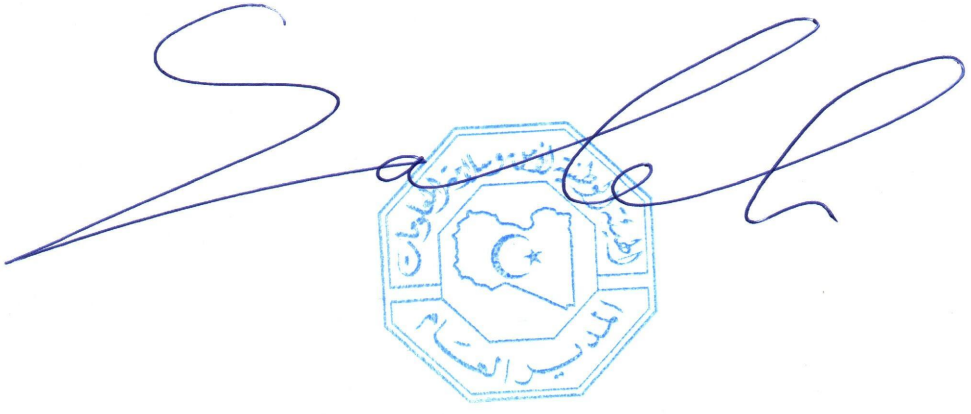
نائب المدير العام

مدير إدارة أمن وسلامة النظم والتطبيقات

رئيس قسم السياسات والمعايير

اعتماد

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات



دولـــــــة ليبيـا

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات
رقم (20) لسنة 2026 ميلادي
بشأن اعتماد الضوابط الأساسية للأمن السيبراني في ليبيا

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات:

- بعد الاطلاع على الإعلان الدستوري الصادر في أغسطس 2011ميلادي وتعديلاته.
- وعلى الاتفاق السياسي الموقع بتاريخ 17ديسمبر 2015ميلادي.
- وعلى القانون رقم (12) لسنة 2010 م بإصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى القانون رقم (5) لسنة 2022م بشأن مكافحة الجرائم الالكترونية.

وعلى القانون رقم (6) لسنة 2022م بشأن المعاملات الالكترونية.

- وعلى ما قرره مجلس النواب في جلسته بتاريخ 2021/3/10م بشأن منح الثقة لحكومة الوحدة الوطنية.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013ميلادي بشأن إنشاء الهيئة الوطنية لأمن وسلامة المعلومات.
- وعلى قرار وزير الاتصالات والمعلوماتية رقم (52) لسنة 2013ميلادي بشأن اعتماد الهيكل التنظيمي للهيئة الوطنية لأمن وسلامة المعلومات وتعديلاته.
- وعلى قرار رئيس الهيئة العامة للاتصالات والمعلوماتية رقم (55) لسنة 2018ميلادي بشأن تكليف بمهام.

وعلى قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات رقم (44) لسنة 2021م بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات.

وعلى قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات رقم (5) لسنة 2023م بشأن اعتمادة الاستراتيجية الوطنية للأمن السيبراني.

- وعلى كتاب مدير مكتب المدير العام رقم (2/500) بتاريخ 2026/5/17 ميلادي.

قـــــــــــــــرر

(المادة الأولى)

تعتمد بموجب أحكام هذا القرار **الضوابط الأساسية للأمن السيبراني في ليبيا**، بوصفها إطارا وطنيا ملزما لحماية البنية التحتية الرقمية، وتعزيز أمن وسلامة المعلومات والبيانات، ودعم متطلبات التحول الرقمي الآمن في الدولة الليبية.

(المادة الثانية)

على كافة الوزارات والقطاعات والدوائر الحكومية والجهات التابعة لها الالتزام بتطبيق الضوابط الأساسية للأمن السيبراني المعتمدة بموجب هذا القرار، كل بحسب اختصاصه، واتخاذ ما يلزم من إجراءات لضمان تنفيذها.

(المادة الثالثة)

يعمل بهذا القرار اعتبارا من تاريخ صدوره، وعلى الجهات المعنية تنفيذه.

م. صلاح الدين ابوزيد التبيني
مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

صدر في طرابلس بتاريخ 21 / 05 /2026 ميلادي
الشؤون القانونيـــــة

info@nissa.gov.ly | +218 21 361 4277 | +218 21 361 4127 / +218 21 361 4115
www.cert.gov.ly | www.nissa.gov.ly

المحتويات

مقدمة 5

الهدف العام 5

نطاق العمل 5

الامتثال 6

مكونات وهيكلية الضوابط 6

الضوابط الأساسية للأمن السيبراني 7

تنظيم وإدارة أمن المعلومات 7

الأدوار والمسؤوليات المتعلقة بأمن المعلومات 7

التوثيق ومتابعة الامتثال 7

حماية البيانات والمعلومات 8

إدارة الأصول الرقمية والتقنية 11

التوعية والتدريب 11

أمن الكمبيوتر والشبكات 12

الحماية من البرمجيات الخبيثة 12

حماية الشبكة 12

إدارة الاتصال عن بعد والشبكة الافتراضية الخاصة (VPN) 13

ضوابط استخدام الوسائط القابلة للإزالة 13

إدارة الأجهزة المحمولة والشخصية 14

ضوابط ومتطلبات الأمان المادي 14

مدى نضج ومرونة المؤسسة 15

إدارة المخاطر المتعلقة بالأمن السيبراني 15

إدارة حوادث وتهديدات الأمن السيبراني 15

إدارة سجلات الأحداث ومراقبة الأمن السيبراني 16

إدارة الثغرات 16

إدارة عمليات اختبار الاختراق 17

إدارة عمليات النسخ الاحتياطي 17

إدارة الأطراف الثالثة أو الخارجية 18

إدارة استمرارية الأعمال والتعافي من الكوارث 18

مقدمة

في ظل التهديدات المتزايدة التي يشهدها الفضاء السيبراني، وتنامي الاعتماد على الأنظمة الرقمية والتقنية في مختلف القطاعات، ولأن الأمن السيبراني بات يمثل أحد أكبر التحديات التي تواجه المؤسسات بمختلف أحجامها، أصبح من الضروري على المؤسسات تعزيز قدراتها ورفع كفاءتها في هذا المجال واتخاذ الإجراءات اللازمة لضمان حماية بياناتها والامتثال للمعايير الوطنية والدولية ذات العلاقة.

وانطلاقًا من الصلاحيات التنظيمية الممنوحة للهيئة الوطنية لأمن وسلامة المعلومات (NISSA)، واستنادًا إلى دليل السياسات الوطنية لأمن المعلومات، يقدم هذا المستند إطارًا تنظيميًا واضحًا وشاملًا لضوابط ومتطلبات الأمن السيبراني الأساسية التي يجب على جميع المؤسسات الالتزام بها وتطبيقها بما يضمن حماية أصولها المعلوماتية والتقنية من التهديدات السيبرانية المختلفة وتقليل المخاطر إلى الحد الأدنى. ويرتكز هذا المستند على (4) أربع محاور رئيسية ليكون بمثابة مرجع أساسي وتوجيهي للمؤسسات الراغبة في تطوير قدرتها وكفاءتها السيبرانية.

الهدف العام

يهدف هذا المستند إلى وضع الحد الأدنى من متطلبات وضوابط الأمن السيبراني اللازمة لحماية الأصول المعلوماتية والتقنية للمؤسسات بدولة ليبيا والحفاظ على سرية وتكامل وتوافر المعلومات وذلك من خلال وضع إطار عمل شامل مبني على نهج منظم لإدارة وحوكمة أمن المعلومات، وتعزيز البنية التحتية الرقمية والأمان المادي بما يرفع مستوى نضج ومرونة المؤسسة في مواجهة التهديدات والمخاطر وصولا إلى ضمان استمرارية الأعمال. بالإضافة إلى تمكين المؤسسات من تحقيق التوازن المطلوب بين الاستخدام الفعال للتقنية والامتثال لمتطلبات الحماية والخصوصية بما يتماشى مع أفضل الممارسات والمعايير الوطنية والدولية في مجال الأمن السيبراني.

نطاق العمل

تُطبق ضوابط الأمن السيبراني الأساسية الواردة بهذه الوثيقة على جميع الجهات والمؤسسات التابعة للقطاعين العام والخاص في دولة ليبيا، يشمل هذا الالتزام كل من يمتلك أو يدير أو يشغل أصولًا معلوماتية أو تقنية ضمن نطاق عمله مع التركيز على الجهات التي تصنف أنها جزء من البنية التحتية الحيوية للبلاد والتي يؤدي تعطلها إلى تأثير كبير على الأمن الوطني والاقتصاد والمجتمع .كما تُطبق هذه الضوابط على جميع الأصول المعلوماتية والتقنية التابعة للجهات المشمولة بنطاق العمل.

يمكن تعديل هذا النطاق وتوسيعه أو تضييقه من قبل الهيئة الوطنية لأمن وسلامة المعلومات بناءً على تقييم المخاطر واحتياجات الأمن السيبراني الخاصة بدولة ليبيا.

الامتثال

يجب على جميع الجهات والمؤسسات ضمن نطاق العمل أن تلتزم بتطبيق ضوابط الأمن السيبراني الواردة في هذه الوثيقة والامتثال التام لها، بما يضمن حماية الأصول المعلوماتية والتقنية من التهديدات السيبرانية المحتملة. ويشمل ذلك الالتزام أن تقوم كل جهة بإصدار وتطبيق سياسات وإجراءات الأمن السيبراني بما يتناسب مع مجال عملها، ومراجعتها بشكل دوري وفقاً للتغيرات التنظيمية والتقنية والتشريعية. تقوم الهيئة الوطنية لأمن وسلامة المعلومات بالتحقق من مدى التزام الجهات والمؤسسات بضوابط الأمن السيبراني الأساسية الواردة بهذه الوثيقة من خلال زيارات التدقيق الميدانية لتلك الجهات بالإضافة إلى التقارير والتوصيات الناتجة عنها لتقييم ومتابعة الأداء.

مكونات وهيكلية الضوابط

1	تنظيم وإدارة أمن المعلومات	1.1	الأدوار والمسؤوليات المتعلقة بأمن المعلومات		
		1.2	التوثيق ومتابعة الامتثال	1.2.1	سياسات وإجراءات أمن المعلومات
				1.2.2	إدارة عمليات التدقيق
		1.3	حماية البيانات والمعلومات	1.3.1	ملكية البيانات والمعلومات
				1.3.2	إدارة التعامل مع البيانات
				1.3.3	إدارة صلاحيات الوصول للبيانات
				1.3.4	الاستخدام المقبول
				1.3.5	إدارة كلمة المرور
				1.3.6	إدارة البريد الالكتروني
				1.3.7	إدارة التشفير
		1.4	إدارة الأصول الرقمية والتقنية		
		1.5	التوعية والتدريب	1.5.1	التوعية
				1.5.2	التدريب
2	أمن الكمبيوتر والشبكات	2.1	الحماية من البرمجيات الخبيثة		
		2.2	حماية الشبكة		
		2.3	إدارة الاتصال عن بعد والشبكة الافتراضية الخاصة (VPN)		
		2.4	ضوابط استخدام الوسائط القابلة للإزالة		
		2.5	إدارة الأجهزة المحمولة والشخصية		
3	ضوابط ومتطلبات الأمان المادي				
4	مدى نضج ومرونة المؤسسة	4.1	إدارة المخاطر المتعلقة بالأمن السيبراني		
		4.2	إدارة حوادث وتهديدات الأمن السيبراني		
		4.3	إدارة سجلات الأحداث ومراقبة الأمن السيبراني		
		4.4	إدارة الثغرات		
		4.5	إدارة عمليات اختبار الاختراق		
		4.6	إدارة عمليات النسخ الاحتياطي		
		4.7	إدارة الأطراف الثالثة أو الخارجية		
		4.8	إدارة استمرارية الأعمال والتعافي من الكوارث		

الضوابط الأساسية للأمن السيبراني

1	تنظيم وإدارة أمن المعلومات
1.1	الأدواروالمسؤوليات المتعلقة بأمن المعلومات
الهدف	ضمان وضوح الأدوار والمسؤوليات والمهام المتعلقة بالأمن السيبراني داخل المؤسسة لتطبيق السياسات والإجراءات الأمنية بشكل فعال وحماية البيانات والمعلومات من المخاطر الداخلية والخارجية وتحقيق استجابة سريعة وفعالة للتهديدات والهجمات الأمنية وتقليل الأضرار الناتجة عنها.
الضوابط	1.1.1 يجب إعداد وتوثيق ضوابط للتحكم في الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بالمؤسسة، على أن تشمل بحد أدنى ما يلي:
	1.1.1.1 **قسم أمن المعلومات:** يجب على جهة العمل إنشاء إدارة أو قسم خاص بأمن المعلومات بجميع تخصصاته، ويجب على صاحب الصلاحية تحديد وتوزيع الأدوار والمسؤوليات وتوثيقها.
	1.1.1.2 **فريق استجابة الحوادث:** يجب على جهة العمل تشكيل فريق استجابة لحوادث الأمن السيبراني.
	1.1.2 يجب تطبيق ضوابط التحكم في الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بالمؤسسة ومتابعة الالتزام بها.
	1.1.3 يجب مراجعة ضوابط التحكم في الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.
1.2	التوثيق ومتابعة الامتثال
1.2.1	سياسات وإجراءات أمن المعلومات
الهدف	وضع إطار عمل واضح لمتطلبات وضوابط الأمن السيبراني في صورة سياسات وإجراءات وضمان تطبيقها بشكل متسق وموحد، بالإضافة إلى تسهيل متابعة الامتثال وتوجيه الموظفين والمراجعة المستمرة لفعالية تلك السياسات والإجراءات في مواجهة التهديدات الأمنية المتجددة.
الضوابط	1.2.1.1 يجب إعداد وتوثيق واعتماد سياسات وإجراءات شاملة لأمن المعلومات تكون خاصة بالمؤسسة، تمتثل للمتطلبات الواردة في دليل السياسات الوطنية لأمن المعلومات الصادر عن الهيئة الوطنية لأمن وسلامة المعلومات، على أن تكون مُصممة ومُكيفة بناءً على مجال عمل المؤسسة وبيئة التهديدات التي تعمل ضمنها وتستند إلى تقييم دقيق للمخاطر المحتملة.
	1.2.1.2 يجب أن تكون السياسات والإجراءات متفقة مع اللوائح التنظيمية والتنفيذية للمؤسسة والقوانين والتشريعات المعمول بها في البلاد ومواكبة للمعايير العالمية.
	1.2.1.3 يجب نشر السياسات إلى الموظفين والعاملين ذوي العلاقة والأطراف المعنية وتوفير التوعية بأهمية الالتزام بها.
	1.2.1.4 يجب تطبيق سياسات وإجراءات الأمن السيبراني الخاصة بالمؤسسة وإيجاد الآلية المناسبة لإلزام الموظفين بها.
	1.2.1.5 إعداد وثيقة أمن المعلومات والخصوصية للحفاظ على سرية بيانات المؤسسة، يجب على جميع الموظفين التوقيع عليها لإلزامهم بما ورد بها وبالسياسات الصادرة عن المؤسسة.
	1.2.1.6 يجب متابعة امتثال الموظفين لسياسات وإجراءات الأمن السيبراني الخاصة بالمؤسسة.
	1.2.1.7 يجب مراجعة سياسات وإجراءات الأمن السيبراني بشكل دوري وتحديثها إذا تطلب الأمر، كحدوث تغييرات في البيئة التنظيمية أو التنفيذية للمؤسسة أو التشريعات والقوانين المحلية داخل الدولة

أو عند حدوث تطور وتغير في المعايير والتكنولوجيا عالميا لضمان فعاليتها وملائمتها للتهديدات السيبرانية المحتملة.

1.2.2 إدارة عمليات التدقيق

الهدف ضمان الامتثال لسياسات وإجراءات الأمن السيبراني والمتابعة والتأكد أنه يتم تطبيقها بشكل صحيح وفعال والكشف عن المخاطر والتهديدات المحتملة.

الضوابط

1.2.2.1 يجب إعداد وتوثيق متطلبات عمليات التدقيق بالمؤسسة، تشمل على الأقل ما يلي:

- إجراء عمليات تدقيق داخلي (Internal Audit) بالمؤسسة بانتظام وبشكل دوري لقياس مستوى امتثالها لضوابط الأمن السيبراني.
- النماذج والمستندات اللازمة لإجراء عملية التدقيق بما في ذلك قائمة التحقق.
- تقارير تفصيلية تتضمن نتائج عملية التدقيق، وأي توصيات أو إجراءات تصحيحية مقترحة، ليتم الاستفادة منها كجزء من عملية تحسين الأداء ورفع مستوى الامتثال.

1.2.2.2 يجب تطبيق وتنفيذ متطلبات عمليات التدقيق بالمؤسسة ومتابعة الالتزام بها.

1.2.2.3 يجب مراجعة متطلبات عمليات التدقيق بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

1.3 حماية البيانات والمعلومات

1.3.1 ملكية البيانات والمعلومات

الهدف تحديد المسؤوليات والحقوق المتعلقة بالبيانات والمعلومات لضمان حمايتها بفعالية.

الضوابط

1.3.1.1 يجب إعداد وتوثيق ضوابط التحكم في ملكية البيانات والمعلومات في المؤسسة، ويجب أن تغطي على الأقل ما يلي:

- يجب تحديد مالك البيانات بشكل واضح، سواء كان فرد أو مؤسسة.
- تحديد من يملك الحق في تعديل أو إضافة، أو إزالة البيانات.
- تحديد من يحق له الوصول إلى البيانات.

1.3.1.2 يجب تطبيق ضوابط التحكم في ملكية البيانات والمعلومات في المؤسسة.

1.3.1.3 يجب مراجعة ضوابط التحكم في ملكية البيانات والمعلومات في المؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

1.3.2 إدارة التعامل مع البيانات

الهدف تأمين البيانات والمعلومات بناءً على تصنيفها وحمايتها طوال دورة حياتها من المخاطر والتهديدات المختلفة والحفاظ على خصوصية وسرية البيانات الحساسة حسب المعايير والقوانين المحلية والدولية ذات العلاقة.

الضوابط

1.3.2.1 يجب إعداد وتوثيق ضوابط التعامل الآمن مع البيانات والمعلومات بالمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- تصنيف البيانات والمعلومات بالمؤسسة بناءً على حساسيتها وأهميتها.
- خصوصية البيانات والمعلومات: يجب إلزام الموظفين بالتوقيع على اتفاقية أمن المعلومات والخصوصية للحفاظ على سرية بيانات المؤسسة.
- الالتزام بمتطلبات الأمان الأساسية عند التعامل مع البيانات (تخزين المعلومات، والإفصاح عنها، وحفظ السجلات، واتلافها، ونشرها).

1.3.2.2 يجب تطبيق ضوابط التعامل الآمن مع البيانات والمعلومات بالمؤسسة ومتابعة الالتزام بها.

1.3.2.3 يجب مراجعة ضوابط التعامل الآمن مع البيانات والمعلومات بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

1.3.3 إدارة صلاحيات الوصول للبيانات

الهدف حماية البيانات والمعلومات من الوصول الغير مصرح وتقليل المخاطر والتهديدات المرتبطة به كتسريب البيانات أو استغلالها أو التلاعب بها.

الضوابط 1.3.3.1 يجب إعداد وتوثيق ضوابط لإدارة صلاحيات الوصول إلى جميع البيانات بالمؤسسة، تشمل على الأقل ما يلي:

- التحكم في الوصول: يجب تحديد مستوى الوصول إلى البيانات بناءً على دور المستخدم والمهام الموكلة إليه استنادا على المبادئ التالية:
  - **مبدأ الحاجة إلى المعرفة والاستخدام.**
  - **مبدأ الحد الأدنى من الامتيازات.**
  - **مبدأ فصل المهام.**
- إدارة الوصول للحسابات السرية والحساسة **(Privileged Access Management - PAM).**
- التحقق من هوية المستخدم قبل منح الوصول إلى البيانات و**تفويض الوصول (Authorization)** للتأكد من صلاحيات المستخدم بناءً على دوره والبيانات التي يحتاج إلى الوصول إليها.

1.3.3.2 يجب تطبيق ضوابط إدارة صلاحيات الوصول بالمؤسسة ومتابعة الالتزام بها.

1.3.3.3 يجب مراجعة ضوابط صلاحيات الوصول بالمؤسسة بشكل دوري وتحديثها إذا لزم الأمر.

1.3.4 الاستخدام المقبول

الهدف ضمان الاستخدام الآمن والمسؤول للأصول المعلوماتية والتقنية للمؤسسة ومنع الأنشطة الضارة والغير قانونية وسوء الاستخدام للحد من الأخطاء البشرية وتقليل تعرض المؤسسة للمخاطر والهجمات السيبرانية المرتبطة بها.

الضوابط 1.3.4.1 يجب إعداد وتوثيق ضوابط للتحكم في الاستخدام المقبول للأصول الرقمية التابعة للمؤسسة، ويجب أن تغطي على الأقل ما يلي:

- ضوابط الاستخدام الآمن لجميع الأصول الرقمية بما في ذلك أجهزة الكمبيوتر وملحقاته.
- ضوابط استخدام موارد الانترنت.
- يجب أن يتم نشر هذه الضوابط وتوعية الموظفين بأهمية الامتثال لها باستمرار وتنفيذ الإجراءات التي تضمن التزامهم بها.

1.3.4.2 يجب تطبيق ضوابط التحكم في الاستخدام المقبول للأصول الرقمية التابعة للمؤسسة ومتابعة التزام جميع الموظفين بها.

1.3.4.3 يجب مراجعة ضوابط التحكم في الاستخدام المقبول للأصول الرقمية التابعة للمؤسسة بشكل دوري وتحديثها إذا لزم الأمر.

1.3.5 إدارة كلمة المرور

الهدف حماية الحسابات والأنظمة والمعلومات من الوصول الغير مصرح به وتقليل مخاطر الاختراقات والأضرار التي قد تحدث بسبب تسريب أو سرقة كلمات المرور.

الضوابط

1.3.5.1 يجب إعداد وتوثيق سياسة للتحكم في إنشاء واستخدام كلمات المرور بالمؤسسة، على أن تشمل بحد أدنى ما يلي:

- ضوابط تكوين كلمة المرور.
- أمن كلمة المرور والحفاظ على سريتها أثناء التخزين والنقل، واستخدام بروتوكولات التشفير.
- إجراءات التحقق من هوية المستخدم عند الدخول/ تغيير كلمة المرور.
- إجراءات منع الوصول بعد عدد معين من المحاولات الخاطئة للدخول إلى النظام.

1.3.5.2 يجب تطبيق سياسة التحكم في إنشاء واستخدام كلمات المرور بالمؤسسة وفرض الإجراءات التي تضمن التقيد والالتزام بها.

1.3.5.3 يجب مراجعة سياسة التحكم في إنشاء واستخدام كلمات المرور بالمؤسسة بشكل دوري وتحديثها إذا لزم الأمر.

1.3.6 إدارة البريد الالكتروني

الهدف حماية البريد الإلكتروني والبيانات التي يتم تبادلها عبره من الهجمات الخبيثة والتهديدات والمخاطر المتعددة التي قد تؤثر على سرية المعلومات أو تؤدي إلى اختراق الأنظمة بالمؤسسة، تشمل هذه المخاطر على سبيل المثال التصيد الاحتيالي والرسائل المزعجة أو أي برامج ضارة قد تنتقل عبر المرفقات والروابط في رسائل البريد الالكتروني.

الضوابط

1.3.6.1 يجب إعداد وتوثيق ضوابط استخدام البريد الالكتروني بالمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- استخدام النطاق الرسمي للمؤسسة (Official Domain) لجميع عناوين البريد الإلكتروني الخاصة بالموظفين وعدم استخدام نطاقات خارجية.
- ضوابط الاستخدام المقبول للبريد الالكتروني والالتزام بسياسات المؤسسة ذات العلاقة.
- استخدام التحقق من الهوية متعدد العناصر **Multi-Factor Authentication.**
- استخدام تقنيات وآليات متقدمة لحماية البريد الالكتروني من التهديدات المحتملة مثل رسائل التصيد الالكتروني (**Phishing Emails**) والرسائل الاقتحامية (**Spam Emails**) والمرفقات الخبيثة.

1.3.6.2 يجب تطبيق ضوابط استخدام البريد الالكتروني بالمؤسسة بشكل شامل ومتابعة التزام جميع الموظفين بها وفرض الإجراءات التي تضمن امتثالهم لها.

1.3.6.3 يجب مراجعة ضوابط استخدام البريد الالكتروني بالمؤسسة بشكل دوري وتحديثها إذا لزم الأمر.

1.3.7 إدارة التشفير

الهدف حماية الأصول المعلوماتية للمؤسسة من الوصول الغير مصرح به أثناء النقل والتخزين والوصول إلى أعلى مستوى ممكن من الأمان والسرية والخصوصية للبيانات والمعلومات الحساسة وتقليل المخاطر المرتبطة بسرقة البيانات أو تعرضها للتسريب.

الضوابط

1.3.7.1 يجب إعداد وتوثيق ضوابط استخدام تقنيات التشفير بالمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- استخدام التشفير لحماية البيانات التي تم تصنيفها كبيانات سرية أو حساسة أثناء النقل والتخزين.
- ضوابط استخدام خوارزميات ومعايير التشفير.
- إدارة مفاتيح التشفير بشكل آمن.

1.3.7.2 يجب تطبيق ضوابط استخدام تقنيات التشفير بالمؤسسة ومتابعة الالتزام بها.

1.3.7.3 يجب مراجعة ضوابط استخدام تقنيات التشفير بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

1.4 إدارة الأصول الرقمية والتقنية

الهدف حماية الأصول الرقمية والتقنية بالمؤسسة والحفاظ عليها من الضياع والتلف وضمان توافرها بحالة جيدة وفعالة وسلامتها من المخاطر السيبرانية المحتملة، بالإضافة إلى أن تحديد المسؤوليات والمهام يهدف إلى متابعة حالة الأصول بشكل دوري وتحقيق الكفاءة في إدارة الأصول.

الضوابط 1.4.1 يجب إعداد وتوثيق ضوابط لإدارة الأصول الرقمية والتقنية بالمؤسسة، ويجب أن تشمل على الأقل مايلي:

- **قائمة جرد أصول البيانات:** إنشاء قائمة جرد لجميع الأصول الرقمية بالمؤسسة وتحديثها باستمرار، على أن تشمل القائمة أسماء المستخدمين لهذه الأصول وتتبع لحالة وحركة كل أصل.
- **مسؤول أصول البيانات:** يجب تحديد مسؤول (فرد أو فريق) عن الأصول الرقمية مع تحديد صلاحيتهم ومسؤولياتهم.
- **وحدة تخزين البيانات:** يجب تهيئة وحدة تخزين البيانات للمؤسسة بأحدث المعايير الأمنية ووفقاً للضوابط الواردة بدليل السياسات الوطنية لأمن المعلومات الصادر عن الهيئة الوطنية لأمن وسلامة المعلومات.

1.4.2 يجب تطبيق ضوابط إدارة الأصول الرقمية والتقنية بالمؤسسة ومتابعة الالتزام بها.

1.4.3 يجب مراجعة ضوابط إدارة الأصول الرقمية والتقنية بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

1.5 التوعية والتدريب

1.5.1 التوعية

الهدف تعزيز ثقافة الأمن السيبراني لدى الموظفين بالمؤسسة وزيادة الوعي والمعرفة بأنواع التهديدات والهجمات والمخاطر المحتملة وكيفية التعامل معها وتقليل المخاطر السيبرانية المرتبطة بالأخطاء البشرية قدر الإمكان.

الضوابط 1.5.1.1 يجب إعداد وتوثيق برنامج توعوي مُواكب لأحدث التطورات في مجال الأمن السيبراني ويستهدف جميع الموظفين العاملين بالمؤسسة كل بما يتناسب مع مهامه واحتياجاته. يجب أن يغطي البرنامج التوعوي على الأقل الأوجه التالية:

- الهجمات الالكترونية الشائعة والمخاطر والتهديدات المحتملة.
- التعامل الآمن مع رسائل البريد الإلكتروني.
- الاستخدام الآمن لموارد تقنية المعلومات.
- الاستخدام الآمن للإنترنت ووسائل التواصل الاجتماعي.
- إمكانية وسهولة الوصول للمواد التوعوية لجميع الموظفين.

1.5.1.2 يجب تطبيق البرنامج التوعوي بشكل دوري ومنتظم ومتابعة التزام المُستهدفين به.

1.5.1.3 يجب مراجعة محتوى وآلية تنفيذ البرنامج التوعوي بالمؤسسة بشكل دوري وقياس مدى فعاليته وتحديثه كلما تطلب الأمر.

1.5.2 التدريب

الهدف تطوير مهارات وقدرات الموظفين في مجال الأمن السيبراني لتأمين الأنظمة وحماية البيانات والاستجابة السريعة والفعالة للحوادث الأمنية.

الضوابط

1.5.2.1 يجب إعداد وتوثيق برنامج تدريبي على المهارات المطلوبة في مجال الأمن السيبراني للموظفين العاملين بالمؤسسة كل بما يتناسب مع مهامه واحتياجاته، ويجب أن يشمل على الأقل ما يلي:

- توفير التدريب اللازم لموظفي الإدارة المعنية بالأمن السيبراني.
- توفير التدريب اللازم للموظفين المشغلين للأصول المعلوماتية والتقنية للجهة.
- توفير التدريب للعاملين بالوظائف الإدارية والإشرافية والتنفيذية.

1.5.2.2 يجب تطبيق البرنامج التدريبي في مجال الأمن السيبراني للموظفين العاملين بالمؤسسة ومتابعة الالتزام به.

1.5.2.3 يجب مراجعة البرنامج التدريبي في مجال الأمن السيبراني للموظفين العاملين بالمؤسسة بشكل دوري وتعديلها وتحديثها حسب الاحتياج.

2 أمن الكمبيوتر والشبكات

2.1 الحماية من البرمجيات الخبيثة

الهدف حماية جميع الأجهزة والأنظمة بالمؤسسة من الفيروسات والبرمجيات الخبيثة وغيرها من المخاطر السيبرانية.

الضوابط

2.1.1 يجب إعداد وتوثيق ضوابط وآليات الحماية والوقاية من البرمجيات الخبيثة بالمؤسسة، يجب أن تغطي على الأقل ما يلي:

- تشمل هذه الضوابط جميع الأنظمة والأجهزة والخوادم بالمؤسسة بما في ذلك الأجهزة المحمولة والوسائط القابلة للإزالة.
- استخدام تقنيات متقدمة وبرامج محدثة لمكافحة الفيروسات والحماية من البرمجيات الخبيثة والكشف عن الأنشطة المشبوهة.
- تشغيل الفحص التلقائي لجميع الملفات والبرامج وفحص البريد الالكتروني والروابط الواردة عبره.
- منع تحميل البرامج والملفات من مصادر غير موثوقة.

2.1.2 يجب تطبيق ضوابط وآليات الحماية والوقاية من البرمجيات الخبيثة بالمؤسسة ومتابعة الالتزام بها.

2.1.3 يجب مراجعة ضوابط وآليات الحماية من البرمجيات الخبيثة بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

2.2 حماية الشبكة

الهدف حماية شبكات المؤسسة من المخاطر والتهديدات المحتملة.

الضوابط

2.2.1 يجب إعداد وتوثيق ضوابط ومتطلبات حماية شبكة المؤسسة من المخاطر والتهديدات السيبرانية، ويجب أن تغطي على الأقل ما يلي:

- **تحديد مستويات الوصول إلى الشبكة** بناءً على أدوار المستخدمين والتقسيم المادي لأجزاء الشبكات.
- **إجراء تحديثات وتصحيحات** بصورة شاملة ودورية لكل الأجهزة والأنظمة في المؤسسة.

- **استخدام أنظمة مراقبة آلية** لاكتشاف ومنع الاختراقات والأنشطة المشبوهة قدر الإمكان وبالتالي تقليل تعرض المؤسسة للتهديدات والمخاطر للحد الأدنى.
- ضوابط التحكم في معايير التهيئة لأجهزة التوجيه ومبدلات الشبكة بالمؤسسة.
- ضوابط التحكم في معايير تهيئة الجدار الناري بشبكة المؤسسة.
- ضوابط للتحكم في معايير الشبكة اللاسلكية **(WiFi)** الخاصة بالمؤسسة.
- أمن التصفح والاتصال بالإنترنت ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة ومواقع مشاركة وتخزين الملفات.

2.2.2 يجب تطبيق ضوابط ومتطلبات حماية شبكة المؤسسة ومتابعة الالتزام بها.

2.2.3 يجب مراجعة ضوابط ومتطلبات حماية شبكة المؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

2.3 إدارة الاتصال عن بعد والشبكة الافتراضية الخاصة (VPN)

الهدف حماية موارد المؤسسة المعلوماتية وشبكاتها من المخاطر والتهديدات المحتملة التي قد تنشأ من استخدام الاتصال عن بُعد أو عبر الشبكة الافتراضية الخاصة(VPN) ، وضمان أقصى مستويات الأمان للبيانات والمعلومات.

الضوابط 2.3.1 يجب إعداد وتوثيق ضوابط للتحكم في الاتصال عن بعد والشبكة الافتراضية الخاصة **(VPN)** في المؤسسة، تشمل على الأقل ما يلي:

- استخدام المصادقة متعددة العوامل **(MFA)** للتحقق من هوية الشخص الذي يحاول الاتصال عن بعد.
- تحديد صلاحيات الوصول لمستخدمي الاتصال عن بعد بحيث يعطى لكل مستخدم حق الوصول الذي يحتاجه لأداء عمله فقط.
- مراقبة وتسجيل جميع الأنشطة التي تحدث خلال الاتصال عن بعد، ومراجعتها وتحليلها للكشف عن أي نشاط مشبوه أو غير اعتيادي.
- يجب على مستخدمي الاتصال عن بُعد الالتزام بسياسات الأمان للمؤسسة بما في ذلك سياسة الاستخدام المقبول وسياسة الخصوصية.
- التأكد من موثوقية مزودي خدمة **(VPN)** الخارجيين ومدى امتثالهم لسياسات ومعايير الأمن السيبراني المحلية والدولية خصوصا سياسة الخصوصية وعدم الاحتفاظ بالسجلات.

2.3.2 يجب تطبيق ضوابط للتحكم في الاتصال عن بعد والشبكة الافتراضية الخاصة **(VPN)** في المؤسسة ومتابعة الالتزام بها.

2.3.3 يجب مراجعة ضوابط التحكم الاتصال عن بعد والشبكة الافتراضية الخاصة **(VPN)** في المؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

2.4 ضوابط استخدام الوسائط القابلة للإزالة

الهدف التعامل الآمن مع الوسائط القابلة للإزالة لضمان حماية أنظمة وأجهزة المؤسسة من أي مخاطر محتملة وحماية بيانات ومعلومات المؤسسة أثناء النقل والتخزين باستخدام هذه الوسائط.

الضوابط 2.4.1 يجب إعداد وتوثيق ضوابط للتحكم في استخدام الوسائط القابلة للإزالة بالمؤسسة، تشمل على الأقل ما يلي:

- التحكم في الوصول وتحديد من يستطيع استخدام أو توصيل الوسائط القابلة للإزالة على النظام.

- التأكد من أن كافة الوسائط القابلة للإزالة يتم فحصها باستخدام برامج مكافحة الفيروسات قبل استخدامها على النظام.
- تشفير بيانات المؤسسة الهامة والحساسة عند تخزينها على الوسائط القابلة للإزالة لضمان حماية المعلومات في حال تم فقدان الجهاز أو سرقته.
- مراقبة وتسجيل جميع الأنشطة المرتبطة باستخدام الوسائط القابلة للإزالة، مثل عمليات النقل والنسخ والكتابة لرصد أي سلوكيات غير عادية أو مشبوهة.

2.4.2 يجب تطبيق ضوابط التحكم في استخدام الوسائط القابلة للإزالة بالمؤسسة ومتابعة التزام الموظفين بها.

2.4.3 يجب مراجعة ضوابط التحكم في استخدام الوسائط القابلة للإزالة بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

2.5 إدارة الأجهزة المحمولة والشخصية

الهدف حماية الأجهزة المحمولة (بجميع أنواعها) التابعة للمؤسسة والتعامل الآمن مع الأجهزة الشخصية الخاصة بالعاملين وحماية بيانات ومعلومات المؤسسة أثناء النقل والتخزين على هذه الأجهزة.

الضوابط 2.5.1 يجب إعداد وتوثيق ضوابط للتحكم في أمن الأجهزة المحمولة والأجهزة الشخصية بالمؤسسة، تشمل على الأقل ما يلي:

- تحديد صلاحيات وصول الأجهزة المحمولة والشخصية للأنظمة أو البيانات الحساسة.
- استخدام تقنيات التحقق من الهوية والمصادقة الثنائية (**Multi-Factor Authentication**).
- المراقبة وتقييد الأنشطة على الأجهزة المحمولة والشخصية والتأكد من الامتثال للسياسات الأمنية للمؤسسة.
- تشفير البيانات الحساسة الخاصة بالمؤسسة المخزنة على الأجهزة المحمولة لضمان أمانها في حال فقدان أو سرقة الجهاز.
- يجب أن تكون هناك سياسة فقدان للأجهزة المحمولة تتضمن إجراءات مثل الإبلاغ الفوري عند فقدان أو سرقة أي جهاز وإمكانية مسح البيانات عن بعد وتغيير كلمات المرور.

2.5.2 يجب تطبيق ضوابط التحكم في أمن الأجهزة المحمولة والأجهزة الشخصية بالمؤسسة ومتابعة مدى الالتزام والتقيد بها.

2.5.3 يجب مراجعة ضوابط التحكم في أمن الأجهزة المحمولة والأجهزة الشخصية بالمؤسسة بشكل دوري وتحديثها في حال تطلب الأمر.

3 ضوابط ومتطلبات الأمان المادي

الهدف حماية الأصول الرقمية والتقنية للمؤسسة من الوصول الغير مصرح به والفقدان والتلف والتهديدات البيئية.

الضوابط 3.1 يجب إعداد وتوثيق ضوابط ومتطلبات الأمان المادي لحماية الأصول الرقمية والتقنية بالمؤسسة من الوصول الغير مصرح به والسلامة من التهديدات البيئية، ويجب أن تغطي على الأقل ما يلي:

- الحماية من الوصول الغير مصرح به والسرقة والتسلل، وتطبيق الإجراءات اللازمة لذلك مثل تركيب أجهزة مراقبة وأنظمة حماية وضوابط تحكم بالدخول، وهذا ينطبق على:
  - مبنى المؤسسة والمواقع التابعة له كالفروع ومواقع العمل.

- مراكز البيانات وغرف الخوادم وغيرها من الأماكن التي تحتوي على بيانات أو أجهزة هامة وحساسة.

- متطلبات وضوابط السلامة من التهديدات والكوارث البيئية لمبنى المؤسسة بشكل عام ومراكز البيانات بشكل خاص، تتضمن هذه الضوابط تركيب أنظمة إطفاء الحرائق وأنظمة التبريد ومصادر الطاقة البديلة وأجهزة إنذار مبكر.
- متطلبات ومواصفات مراكز البيانات وغرف الخوادم، بحيث تمتثل لما ورد في دليل السياسات الوطنية لأمن المعلومات الصادر عن الهيئة الوطنية لأمن وسلامة المعلومات.

3.2 يجب تطبيق ضوابط ومتطلبات الأمان المادي لحماية الأصول الرقمية والتقنية بالمؤسسة من الوصول الغير مصرح به والسلامة من التهديدات البيئية ومتابعة الالتزام بهذه الضوابط.

3.3 يجب مراجعة ضوابط ومتطلبات الأمان المادي لحماية الأصول الرقمية والتقنية بالمؤسسة من الوصول الغير مصرح به والسلامة من التهديدات البيئية بشكل دوري وتحديثها إذا تطلب الأمر.

4 مدى نضج ومرونة المؤسسة

4.1 إدارة المخاطر المتعلقة بالأمن السيبراني

الهدف فهم وتحديد المخاطر السيبرانية المحتملة ووضع استراتيجيات لمعالجتها سواء بتقليلها أو تجنبها وتحسين تدابير الوقاية والاستجابة ودعم المؤسسة في اتخاذ القرارات حول كيفية تخصيص الموارد ومعالجة المخاطر.

الضوابط 4.1.1 يجب إعداد وتوثيق متطلبات إدارة المخاطر المتعلقة بالأمن السيبراني في المؤسسة، تشمل على الأقل مايلي:

- تحديد وتحليل المخاطر المحتملة والتهديدات ونقاط الضعف التي من الممكن أن تؤثر على الموارد المعلوماتية والتقنية في المؤسسة وتقييم التأثير المحتمل لتلك المخاطر.
- تصنيف المخاطر حسب درجة تأثيرها من جهة، وحسب احتمالية حدوثها من جهة أخرى (منخفضة، متوسطة، عالية).
- تحليل وتقييم مدى فعالية الخطط والتدابير والاستراتيجيات الوقائية والتصحيحية والرقابية في التخفيف والحد من المخاطر.
- توثيق عملية تقييم وتحليل المخاطر بجميع مراحلها بما في ذلك التقارير والتوصيات اللازمة.

4.1.2 يجب تطبيق متطلبات إدارة المخاطر المتعلقة بالأمن السيبراني في المؤسسة.

4.1.3 يجب مراجعة متطلبات إدارة المخاطر المتعلقة بالأمن السيبراني في المؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.2 إدارة حوادث وتهديدات الأمن السيبراني

الهدف تحسين قدرة المؤسسة على مواجهة الحوادث والهجمات السيبرانية وتحقيق الاستجابة السريعة والفعالة للحد من الأضرار والتأثير السلبي على الأعمال.

الضوابط 4.2.1 يجب إعداد وتوثيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني بالمؤسسة، ويجب أن تغطي على الأقل ما يلي:

- خطة مفصلة للاستجابة لحوادث الأمن السيبراني والتعامل مع الانتهاكات الأمنية.

- يجب أن يكون إلزاميا في الخطة إبلاغ الهيئة الوطنية لأمن وسلامة المعلومات في حال حدوث أي انتهاك أو حادثة.
- إلزام الاتصال بالعملاء المتأثرين بهذه الانتهاكات أو الحوادث .
- تصنيف حوادث الأمن السيبراني.
- الالتزام بتنفيذ خطة الاستجابة للحوادث عند حدوث ما يستدعي ذلك.

4.2.2 يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني بالمؤسسة.

4.2.3 يجب مراجعة متطلبات إدارة حوادث وتهديدات الأمن السيبراني بالمؤسسة بشكل دوري وقياس مدى فعاليتها وتحديثها إذا تطلب الأمر.

4.3 إدارة سجلات الأحداث ومراقبة الأمن السيبراني

الهدف تحسين قدرة المؤسسة على الاكتشاف الاستباقي والمبكر للتهديدات والأنشطة المشبوهة وبالتالي منع الهجمات السيبرانية قبل وقوعها أو الاستجابة السريعة والفعالة لها في حال حدوثها وتقليل الأضرار إلى الحد الأدنى.

الضوابط 4.3.1 يجب إعداد وتوثيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بالمؤسسة، تشمل على الأقل ما يلي:

- تفعيل سجلات الأحداث (**Event Logs**) الخاصة بالأمن السيبراني مع التركيز على الأصول المعلوماتية الحساسة والحسابات ذات الصلاحيات الهامة.
- جمع سجلات الأحداث من مختلف الأجهزة والأنظمة بشكل مستمر، بالإضافة إلى توحيد وتنسيق السجلات المجمعة من مصادر متعددة لتسهيل تحليلها بشكل فعال.
- مراقبة وتحليل سجلات الأحداث بشكل مستمر واستخدام الأدوات المتخصصة (SIEM - Security Information and Event Management) لاكتشاف الأنشطة غير المعتادة أو المشبوهة.
- التخزين الآمن لسجلات الأحداث وتأمينها ضد التعديل والمسح وتحديد مدة الاحتفاظ بها على ألا تقل عن 12 شهرا.

4.3.2 يجب تطبيق متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بالمؤسسة ومتابعة مدى الالتزام بها.

4.3.3 يجب مراجعة متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.4 إدارة الثغرات

الهدف اكتشاف الثغرات التقنية ومعالجتها في وقت مبكر من أجل منع أو التقليل من فرص استغلال هذه الثغرات في تنفيذ الهجمات والاختراقات السيبرانية التي قد تهدد الموارد الرقمية والتقنية للمؤسسة.

الضوابط 4.4.1 يجب إعداد وتوثيق متطلبات إدارة الثغرات التقنية بالمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- إجراء فحص واكتشاف الثغرات بانتظام وبشكل دوري.
- تصنيف الثغرات وفقا لدرجة خطورتها (من منخفض إلى عالي) وتقييم تأثيرها المحتمل على النظام والشبكة والعمل.
- تحديد الأولويات عند معالجة الثغرات بحيث يتم التركيز على الثغرات ذات الخطورة العالية والحرجة أولا (مثل الثغرات التي يمكن استغلالها عن بُعد أو تؤدي إلى تسريب البيانات او تلك التي تؤثر على استمرارية العمل.

- معالجة الثغرات وإجراء التحديثات والتصحيحات والرقع الأمنية اللازمة، بالإضافة إلى إجراء اختبار للتأكد من أن الثغرات قد تم إغلاقها بنجاح.
- متابعة قواعد بينات الثغرات العالمية والتعاون التواصل مع المجتمع الأمني للحصول على التنبيهات والمعلومات الأمنية المحدثة حول الثغرات الجديدة.

4.4.2 يجب تطبيق متطلبات إدارة الثغرات التقنية بالمؤسسة ومتابعة الالتزام بها.

4.4.3 يجب مراجعة متطلبات إدارة الثغرات التقنية بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.5 إدارة عمليات اختبار الاختراق

الهدف تقييم قدرة الأنظمة والتطبيقات والخدمات التقنية على مقاومة الهجمات واختبار جاهزيتها لمواجهة التهديدات السيبرانية، والكشف عن أوجه القصور المحتملة، للحد من المخاطر وحماية الموارد الرقمية والتقنية للمؤسسة.

الضوابط 4.5.1 يجب إعداد وتوثيق ضوابط عمليات اختبار الاختراق بالمؤسسة، على أن تشمل ما يلي:

- إجراء اختبار الاختراق بانتظام وبشكل دوري، وقبل إطلاق أي منصات ومنظومات وتطبيقات.
- **تحديد نطاق الاختبار** بوضوح، بما في ذلك الأنظمة والتطبيقات والخدمات التي سيتم اختبارها. يجب أن يشمل هذا تحديد الأنظمة المستهدفة (مثل الخوادم، قواعد البيانات، الشبكات .... إلخ).
- **الاتفاق المسبق (Authorization):** تلتزم كلٌّ من الجهة المنفذة لاختبار الاختراق والجهة المستهدفة بالحصول على تفويض مكتوب وموقع من الطرفين قبل البدء في تنفيذ اختبار الاختراق يحدد نطاق الاختبار ومسؤوليات كل طرف. ويُعد هذا التفويض شرطًا إلزاميًا لضمان المشروعية القانونية.
- **تحديد الحدود** :يجب الاتفاق على الحدود التي سيشملها الاختبار، مثل الأنظمة التي لن يتم اختبارها أو الأنشطة التي يجب تجنبها لتفادي التأثير على العمليات التجارية.

4.5.2 يجب تطبيق ضوابط عمليات اختبار الاختراق بالمؤسسة ومتابعة الالتزام بها.

4.5.3 يجب مراجعة ضوابط عمليات اختبار الاختراق بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.6 إدارة عمليات النسخ الاحتياطي

الهدف حماية البيانات والأصول الرقمية للمؤسسة من الفقدان الدائم والتلف الذي قد يحدث بسبب الحوادث الأمنية أو الكوارث أو الأخطاء البشرية بالإضافة إلى تقليل تكلفة استعادة البيانات.

الضوابط 4.6.1 يجب إعداد وتوثيق ضوابط إدارة النسخ الاحتياطي بالمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- ذكر الOffsite backups
- تحديد نطاق النسخ الاحتياطي والتأكد أنه شامل جميع البيانات والأصول المعلوماتية المراد نسخها.
- إجراء عملية النسخ الاحتياطي بشكل دوري ومنتظم وحسب جدول زمني مناسب لاحتياجات المؤسسة (يومي، أسبوعي/ شهري).
- توثيق عمليات النسخ الاحتياطي.
- إجراء اختبار إمكانية استعادة للبيانات بشكل دوري ومنتظم للتأكد أن العملية تعمل كما هو مطلوب.
- أمن النسخ الاحتياطية أثناء النقل والتخزين وحمايتها من الوصول الغير مصرح به والفقدان والتلف.
- مدة حفظ النسخ الاحتياطية وفقاً لسياسات المؤسسة.

4.6.2 يجب تطبيق ضوابط إدارة النسخ الاحتياطي بالمؤسسة ومتابعة الالتزام بها.

4.6.3 يجب مراجعة ضوابط إدارة النسخ الاحتياطي بالمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.7 إدارة الأطراف الثالثة أو الخارجية

الهدف ضمان حماية بيانات وأنظمة المؤسسة من التهديدات والمخاطر السيبرانية التي قد تحدث نتيجة التعاون مع شركاء أو أطراف خارجيين.

الضوابط

4.7.1 يجب إعداد وتوثيق ضوابط ومتطلبات الأمن السيبراني عند العمل مع الأطراف الثالثة أو الخارجية للمؤسسة، ويجب أن تشمل على الأقل ما يلي:

- إجراء تقييم لمخاطر الأمن السيبراني وإيجاد حلول للتقليل من هذه المخاطر إلى الحد الأدنى، وذلك قبل توقيع العقود والاتفاقيات.
- ضوابط للتحكم في وصول الأطراف الثالثة أو الخارجية لأنظمة المؤسسة أو شبكتها.
- عند إجراء العقود والاتفاقيات يجب التأكد أنها تتضمن ما يلي:
  - اتفاقية عدم الإفصاح أو بنود المحافظة على سرية المعلومات (**Non-Disclosure Clauses**) وما تتطلبه من إجراءات حسب نوع العمل.
  - إلزام الطرف الثالث أو الخارجي بتطبيق ضوابط ومتطلبات الأمن السيبراني للمؤسسة.
  - إجراءات التواصل عند حدوث حادثة أمن سيبراني.

4.7.2 يجب تطبيق ضوابط ومتطلبات الأمن السيبراني عند العمل مع الأطراف الثالثة أو الخارجية للمؤسسة ومتابعة الالتزام بها.

4.7.3 يجب مراجعة ضوابط ومتطلبات الأمن السيبراني عند العمل مع الأطراف الثالثة أو الخارجية للمؤسسة بشكل دوري وتحديثها إذا تطلب الأمر.

4.8 إدارة استمرارية الأعمال والتعافي من الكوارث

الهدف ضمان استمرارية الأعمال الأساسية والحيوية بالمؤسسة وتعزيز مرونتها في مواجهة الكوارث والحوادث الكبرى كالحرائق والفيضانات والهجمات السيبرانية.

الضوابط

4.8.1 يجب إعداد وتوثيق متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال بالمؤسسة، ويجب أن تغطي على الأقل ما يلي:

- إجراء تقييم وتحليل للمخاطر المحتملة التي قد تؤثر على الأصول المعلوماتية وتهدد استمرارية الأعمال.
- خطة استجابة لحوادث الأمن السيبراني ذات الخطورة العالية والتي قد تؤثر على استمرارية الأعمال.
- خطة التعافي من الكوارث (**Disaster Recovery Plan**).
- خطة استمرارية الأعمال (**Business Continuity Plan**) والتي تتضمن الإجراءات والتدابير والخطط البديلة لضمان استمرارية الأعمال المتعلقة بالأصول المعلوماتية والتقنية بالمؤسسة.

4.8.2 يجب تطبيق متطلبات الأمن السيبراني ضمن إدارة استمرارية الأعمال بالمؤسسة ومتابعة مدى الالتزام بها.

4.8.3 يجب مراجعة متطلبات الأمن السيبراني ضمن خطة استمرارية الأعمال بالمؤسسة بشكل دوري وتحديثها في حال تطلب الأمر.


الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority