وزارة الاتصالات وتكنولوجيا المعلومات

Ministry of Information and
Communications Technology

البرنامج الوطني للأمن السيبراني

إطار سياسة الأمن السيبراني:
٥(ب) الحاويات والتخزين

جدول المحتويات

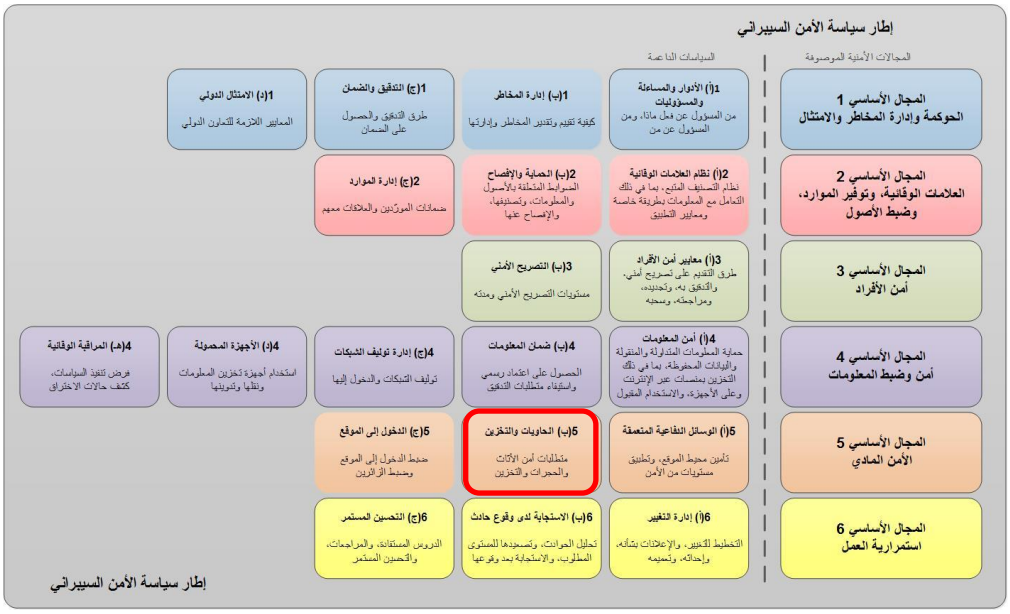
الأشكال

١ مقدمة

١-١ الهدف

الأمن السيبراني الوقائي، بما فيه الأمن المادي وأمن الأفراد وأمن المعلومات، متطلب أساسي ويتيح جعل العمل آمنا وأفضل.

هذه السياسة تساند **المجال ٥ - الأمن المادي** من مجالات إطار السياسة الوطنية للأمن السيبراني، كما هو مبيّن في المستطيل الأحمر في الشكل ١. للاطلاع على القائمة الكاملة لإطار سياسة الأمن السيبراني، يرجى الرجوع إلى **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.



الشكل ١ – إطار سياسة الأمن السيبراني

١-٢ الاستخدام

هذه السياسة ليس الغرض منها استخدامها كوثيقة مستقلة بمعزل عن غيرها، بل لتكون جزءا لا يتجزأ من المجموعة الكاملة من سياسات إطار سياسة الأمن السيبراني. لمعرفة تفاصيل كيفية انتهاج هذه السياسة، يُرجى الاطلاع على القسم ٥ من **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.

١-٣ المتطلبات

تُعتبر المتطلبات الرئيسية للحاويات والتخزين ضرورية من أجل استيفاء مستلزمات حماية الأثاث والغرف وتجهيزات التخزين. ويُمكن تحقيق ذلك من خلال الخطوات التالية:

المتطلب أ. تقييد الدخول إلى المواقع الحساسة

المتطلب ب. أخذ مواد وطرق التشييد بعين الاعتبار

المتطلب ج. تحديد مواقع الأثاث والمعدات

١-٤ المعنيون

تنطبق هذه السياسة على جميع موظفي الحكومة الأردنية، والمتعاقدين معها، وجميع مستخدمي المعلومات الحكومية وأنظمة المعلومات التي تدعم أعمال وأصول الحكومة. لمزيد من التفاصيل، يُرجى الرجوع إلى **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.

١-٥ المعايير الدولية

في سياق تطوير هذه السياسة ومتطلباتها، تمت الاستعانة بالمعايير والأطر الدولية المشار إليها فيما يلي. لمزيد من التفاصيل، وللحصول على روابط للمواقع الإلكترونية المتعلقة بها، يُرجى الرجوع إلى السياسة **١(د) - الامتثال الدولي** التي تضم قائمة أكثر شمولا.

١-٥-١ ISO/IEC ٢٧٠٠١ و27002

تتألف سلسلة ISO/IEC 27000 من مجموعة من المعايير المتعلقة بأمن المعلومات، والتي أعدتها ونشرتها آيزو (ISO) بالاشتراك مع IEC. اثنان من هذه المعايير - المعيار ISO/IEC 27001 والمعيار ISO/IEC 27002 - ينطبقان بشكل خاص على موضوع الحاويات المادية والتخزين، وهما معا يحددان مجموعة من المتطلبات المتعلقة بأنظمة إدارة أمن المعلومات، ومدونة لقواعد السلوك بشأن ضوابط أمن المعلومات.

١-٥-٢ BS EN 1143 (معيار أوروبي معترف به دوليا)

المعيار BS EN 1143 يحدد معيار اختبار الخزنات الآمنة، وخزنات أجهزة الصرف الآلي (ATM)، وأبواب الغرف محكمة الإغلاق والغرف نفسها. ودرجات مقاومة الخزنات مقسمة إلى سبع درجات، وترتفع درجة الأمن بنحو ٥٠% من درجة إلى أخرى.

ويُحسب مستوى الأمن بناء على درجات الأدوات والفترة اللازمة لاختراق خزنة. وبالنسبة لوحدات التخزين الآمن المؤمَّنة وفق هذا المعيار، يجب أن يستوفي نظام قفلها أيضا متطلبات المعيار BE EN 1300 (انظر ٢.٣).

١-٥-٣ BS EN 1627 وPAS 24 (معياران أوروبيان معترف بهما دوليا)

المعيار BS EN 1627 يحدد درجة مقاومة الدخول غير المصرح به من خلال الأبواب والنوافذ، والأغلفة والشبكات والمغالق الخارجية للمباني. وهو يعتبر عموما خط الأساس لأمن البيوت والمكاتب وغيرها. والمعيار PAS 24 يستند إلى مبادئ مماثلة، لكنه يتناول متطلبات أمنية أكثر شدة بالنسبة للأبواب في المواقع الأكثر أمانا.

٢ ضبط الحاويات والتخزين

تسهم سياسة الحاويات والتخزين في صياغة نهج المؤسسة من أجل الحفاظ على تخزين مادي آمن، وتطبيق ممارسات آمنة في عملية الاحتواء للحيلولة دون الدخول المادي لمن ليس لديهم تصريح إلى مواقع معينة أو مشاهدتها أو الاطلاع عليها.

من شأن هذه السياسة أن توفر توجيهات إرشادية وسبلا من أجل حماية المواقع وأصول المعلومات، ولمنع الأفراد غير المصرح لهم من الاطلاع على المعلومات والدخول إلى المواقع الحساسة.

٢-١ المواقع الآمنة

☑ **المتطلب أ. تقييد الدخول إلى المواقع الآمنة.** يجب تصميم وتنفيذ ضوابط الأمن المادي للمكاتب، والغرف، والأماكن الحساسة، ومرافق العمل، والمواقع الآمنة من أجل ضمان أن يكون الدخول إليها مقتصرا فقط على الأشخاص المُعتمَدين والمصرح لهم بالدخول.

الموقع الآمن قد يكون غرفة يمكن قفلها ومُحاطة بحاجز واق متواصل. ولا بد من التطبيق الواضح والشامل لضوابط الأمن المادي في مختلف الغرف بشكل يناسب مستوى الأمن المطلوب لاستخدام غرفة.

أما المواقع ذات الأهمية القصوى، مثل مواقع معالجة البيانات، ومكاتب كبار المسؤولين، ومراكز البيانات، فيجب أن تخضع لحماية مادية أعلى مستوى. وعلى المؤسسة أن تقرر فيما إذا كان من المناسب توفير محيط وحواجز إضافية لضبط الدخول المادي إلى المواقع التي تتطلب مستوى عاليا من الأمن داخل الموقع. ويجب الالتزام بمعايير دولية مثل **BS EN 1143** بالنسبة للأبواب والنوافذ ونقاط الدخول المادي الأخرى أجل ردع الدخول غير المصرح به. ذلك يشمل المواقع التي يُحتمل أن يكون بها نقاط ضعف مادي، مثل الجدار الخفيف والمغالق.

أما إذا كانت مجموعة من الغرف تُستخدم لنفس الغرض، مثل أماكن استلام المواد ومعالجتها، فقد تحتاج إلى احتوائها ضمن نطاق محدد، أو إلى حاجز أمن مادي داخلي متواصل، وذلك لفصل وحماية أجزاء مختلفة في الموقع.

وإذا أظهرت عملية تقييم المخاطر أن هناك حاجة لتأمين موقع أو تقييد الدخول إليه، وفقا للسياسة **١(ب) – إدارة المخاطر**، فإن طرق انتقاء الضوابط لحماية الغرف أو الحاويات ستشمل النقاط التالية، على سبيل المثال لا الحصر:

- محيط مادي متين للحاويات والمواقع، يحيط بها جدران وحواجز صلبة البناء.
- ضوابط كقضبان وأقفال وأجهزة إنذار توضع على كافة الأبواب الخارجية للحاويات أو الغرف.
- ضوابط كقضبان، وأقفال، وأجهزة إنذار توضع على النوافذ، وبشكل خاص نوافذ المواقع الآمنة.
- ضوابط بيومترية للتحكم بالدخول إلى المواقع الآمنة.
- أنظمة مناسبة لكشف الدخلاء، وخاصة في المواقع التي لا يتواجد فيها موظفون بشكل مستمر.

٢-٢ تشييد المباني والغرف

☑ **المتطلب ب. أخذ مواد وطرق التشييد بعين الاعتبار.** تتطلب مواد البناء والطرق التي ستستخدم في تشييد المباني والغرف الآمنة دراسة متأنية لضمان أنها ستفي بالغايات المرجوة منها.

إن بناء غرفة أو مبنى جديد، أو تحديث ما هو موجود منها، بسبب ازدياد الحاجة لضبط الدخول إليها أو لرفع مستوى الحماية، يتطلب عناية خاصة ونهجا مدروسا. ويمكن أن يشمل ذلك أية أعمال يُراد منها تغيير أو تحسين أو زيادة مقاومة أبواب دخول الأفراد، والنوافذ، والتغليف والشبك والمغالق الخارجية للمباني.
ولضمان ألا يتسلل أي دخلاء إلى الموقع، وألا تُترك فيه أية قطعة معدات أثناء عملية البناء، يجب أيضا وضع حماية لمحيط الموقع كما لو كان الموقع مكتملا ويؤدي عمله الذي يتطلب درجة عالية من الأمن.
يُضاف إلى ذلك ضرورة اختيار الموارد والمتعهدين الذين تم التعاقد معهم لتنفيذ أعمال الترميم والبناء الفعلي من خلال إجراءات مضمونة، وفق ما تناولته السياسة **٢(ج) – إدارة الموارد**. ومن ضمن عملية تقييم المخاطر التي تُجرى من أجل تشييد المبنى، ينبغي إدخال ضوابط مادية مثل قوة المبنى وتصميمه بحيث يعيق تسلل الدخلاء. المعايير **BS EN 1143** و **BS EN 1627** و **PAS 24** تعطي مزيدا من التفاصيل عن الأساليب المضمونة لإعاقة الدخلاء. ولمزيد من التفاصيل عن تقييم المخاطر، انظر السياسة **١(ب) – إدارة المخاطر**. ولدى الانتهاء من تشييد المبنى، يُنصح بتفحص الضوابط الأمنية التقنية والمادية، وفق ما تناولته السياسة **٤(أ) – أمن المعلومات**.

٢-٣ الأثاث الآمن

☑ **المتطلب ج. تحديد مواقع الأثاث والمعدات.** يتعين على المؤسسة أن تدرس بعناية الموقع الذي ستختاره لتضع فيه الأثاث الآمن والأجهزة الآمنة، وذلك لضمان أن يظلوا محميين من أجل الحد من التهديدات التي قد تأتيه من محيطه، والأخطار، وفرص الدخول غير المصرح به.

يجب على المؤسسة توفير الحماية لأجهزتها وأصولها ووثائقها عن طريق استخدام أثاث آمن مضمون يمثل بحد بذاته أحد أشكال الردع لمنع حالات الدخول غير المصرح به، ولمنع تعرض المواد التي بداخله للتلف، حيثما كان مناسبا. وينبغي وضع ضوابط لمنع دخول أو إطّلاع غير المصرح لهم على أنشطة العمل والوثائق والأصول السرية. وفي بعض الحالات، قد تشمل وسائل الحماية ضوابط تقنية، مثل الدرع الكهرومغناطيسي، ومنع تسرب المعلومات من خلال الانبعاث الكهرومغناطيسي، إن أمكن ذلك. ويجب أن استخدام ذلك الأثاث الآمن بالشكل الذي تحدده عملية تقييم المخاطر، كما هو موضح في السياسة **١(ب) – إدارة المخاطر**.

الحرص واجب أيضا لتوفير الحماية للجوانب المادية من عملية توزيع المعلومات، كما في حالات استخدام خطوط الإرسال وأقراص الكمبيوتر وما شابه، حيث يجب تطبيق إجراءات منفصلة ومشددة لحماية الوثائق والأصول ذات التصنيف الأمني العالي، كما هو مبين في السياسة **٢(أ) – نظام العلامات الوقائية**.

يشمل الأثاث الآمن والواقي الذي يُستعمل لتخزين البيانات وإتلافها التجهيزات التالية، على سبيل المثال لا الحصر:

- خزائن صغيرة بأقفال لحفظ الوثائق وما شابه؛
- خزائن للمفاتيح (تُحفظ في مكان منفصل، أي بعيدا عن الأعين وخارج أماكن العمل الرئيسية)؛
- خزائن بأقفال للتمديدات الكهربائية والأسلاك وما شابه؛

- خزائن بأقفال لمركز البيانات، وأرفف لخادم الكمبيوتر؛
- أغطية واقية لخطوط الأسلاك/الألياف بين أقسام الموقع؛
- مراقبة الظروف البيئية لمنع تعرض المواد للتلف؛
- لضمان الإتلاف بأمان تحديدا، آلات تقطيع الأوراق بشكل متقاطع، ومطارق وفؤوس لإتلاف الأجهزة الالكترونية المحمولة؛

وعلى المؤسسة توفير الحماية الكافية لوحدات التخزين الآمن مثل الخزنات والأنواع الأخرى من الخزائن الآمنة. ويُنصح بشراء الوحدات التي تُطابق المعايير الدولية. لمزيد من المعلومات عن استخدام وحماية المفاتيح العادية وأقفال الأرقام السرية، انظر السياسة **٥(ج) – الدخول إلى الموقع**.

لمزيد من التفاصيل عن إتلاف الوثائق والأجهزة، انظر السياسة **٤(أ) – أمن المعلومات**.

٣ الاعتبارات الرئيسية

- يتعين على جميع الموظفين معرفة مسؤولياتهم فيما يتعلق بالمواقع والحاويات وحلول التخزين الآمنة، كأن يتأكدوا من تفعيل الأقفال واستخدامها، وأن يحافظوا على سرية شيفرة الدخول إلى المواقع، وأن يلتزموا باستمرار بتطبيق الإجراءات المتبعة بالنسبة للدخول إلى المواقع الآمنة.
- هناك أهمية بالغة لموقع مرافق حفظ المفاتيح ومراقبتها، رغم أنه يتم تجاهل هذه الأهمية أحيانا. وعلى المؤسسة أن تحتفظ بسجلات واضحة لتدوين الدخول إلى تلك المرافق لكشف التهديدات التي تأتي من داخل المؤسسة، حيث أن الدخول إلى المواقع الآمنة باستخدام مفتاح أو تصريح سليم لا يثير الشبهة عادة إلا بعد وقوع الحادث الأمني.
- يجب شراء وتركيب حلول التخزين وفقا لإجراءات المشتريات التي تتبعها الحكومة/الجيش. والأقفال بالذات ينبغي شراؤها فقط من مُورّد مُعتمد حكوميا.