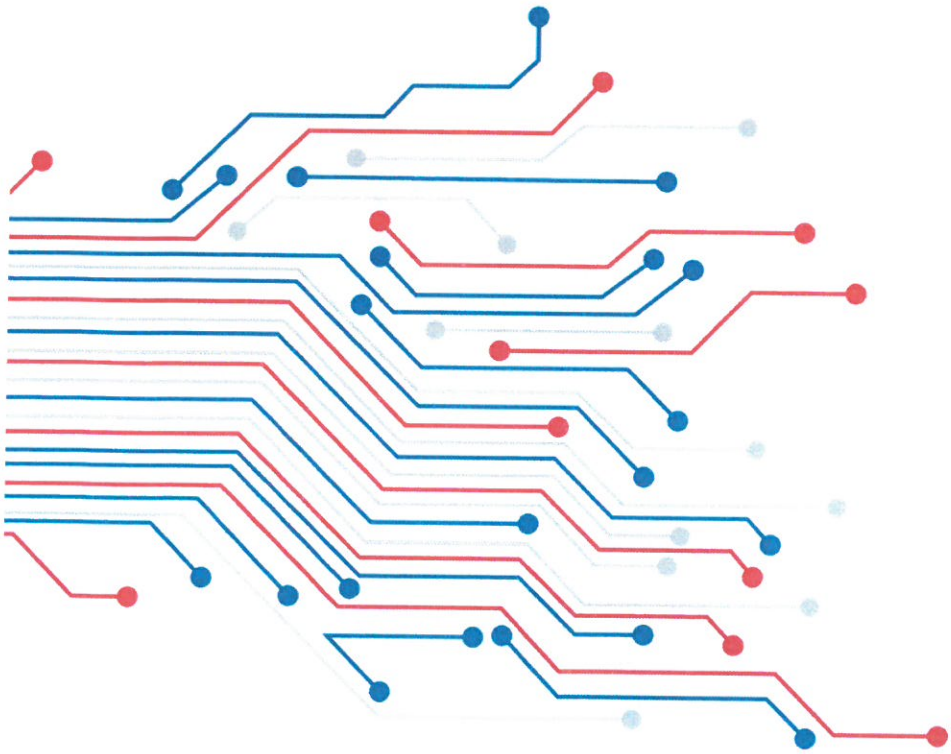
فريق الاستجابة للحوادث
السيبرانية للقطاع المالي
والمصرفي
Jo-FinCERT

Jo-FinCERT

البنك المركزي الأردني
CENTRAL BANK OF JORDAN

دليل ضوابط الأمن السيبراني
لمؤسسات القطاع المالي غير البنكي

الإصدار	١,٠
اعتماد المحافظ	



الفهرس

المقدمة

تعد سلامة المؤسسات المالية غير البنكية **(NBFIs)**، والتي تشمل شركات مقدمي خدمات الدفع وشركات التمويل وشركات التأمين وشركات الصرافة ضرورةً أساسية لضمان عملها في بيئة آمنة. وبالتالي، يجب إدارة معالجة ونقل المعلومات بطريقة تضمن سرية المعلومات وسلامتها وتوافرها، لتجنب الخسائر المالية ومخاطر السمعة.

ونظراً لاعتماد المؤسسات المالية على تكنولوجيا المعلومات والاتصالات **(ICT)** لتشغيل أعمالها، وارتفاع وتيرة الهجمات والتهديدات السيبرانية التي تستهدف هذه المؤسسات، أصبح من الضروري تطبيق إجراءات الأمن السيبراني للتخفيف من آثار تلك المخاطر.

مع انتشار التهديدات السيبرانية مثل برامج الفدية وهجمات التصيّد المستهدفة وتهديدات ال (**APT**)، أصبح من الضروري أن تعزز المؤسسات المالية مرونتها السيبرانية وتتخذ خطوات استباقية لحماية معلوماتها الحساسة، وضمان سلامة أنظمتها. حيث يُعبر مفهوم "المرونة السيبرانية" عن قدرة المؤسسة على الحفاظ على عملياتها الطبيعية على الرغم من كافة التهديدات السيبرانية والمخاطر المحتملة التي تواجهها.

الأهداف

يُحدد هذا الدليل المتطلبات الأساسية الواجب على مؤسسات المالية غير البنكية (NBFIs) الالتزام بها عند تطوير وتنفيذ الاستراتيجيات، والسياسات، والإجراءات والأنشطة المرتبطة بها لغايات تخفيف المخاطر السيبرانية.

الغرض من هذا الدليل يتمثل ب:

- إنشاء بيئة إلكترونية أكثر أماناً، تدعم أمن أنظمة المعلومات، وتعزز استقرار قطاع المؤسسات المالية غير البنكية.
- المساهمة في منع ومكافحة الجرائم الإلكترونية في قطاع المؤسسات المالية غير البنكية.
- تعزيز الثقة العامة في قطاع المؤسسات المالية غير البنكية وتعزيزها.
- تعزيز ثقافة الوعي بالأمن السيبراني من خلال تنمية القدرات وتطوير المهارات بشكل مستمر

النطاق

هذا الدليل مُصمم خصيصاً للمؤسسات المالية غير البنكية في المملكة الأردنية الهاشمية، بما في ذلك مقدمي خدمات الدفع، وشركات التمويل، وشركات التأمين، وشركات الصرافة (المؤسسات الخاضعة لرقابة البنك المركزي الأردني)، بهدف تطبيق أفضل الممارسات لتطوير وتعزيز الأمن السيبراني لدى لهذه المؤسسات.

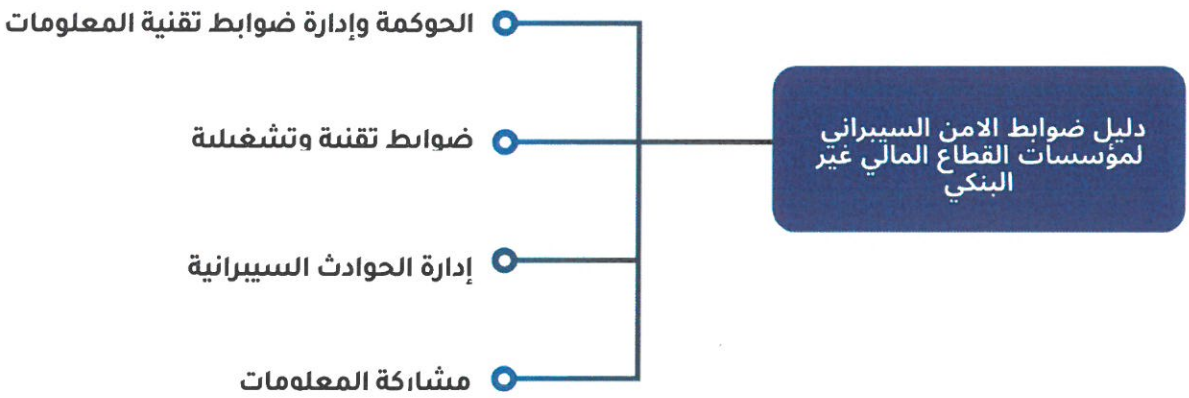
هيكل الدليل

يقدم هذا الدليل نهجًا قائمًا على إدارة مخاطر الأمن السيبراني .ويوضح الدليل الحدود الدنيا للمتطلبات الأمنية السيبرانية التي يجب على مؤسسات القطاع المالي غير البنكي تطبيقها (إن أمكن) لتحسين الوضع الأمني السيبراني لدى القطاع.

يتكون هذا الدليل مما يلي:

٤ مجالات رئيسية

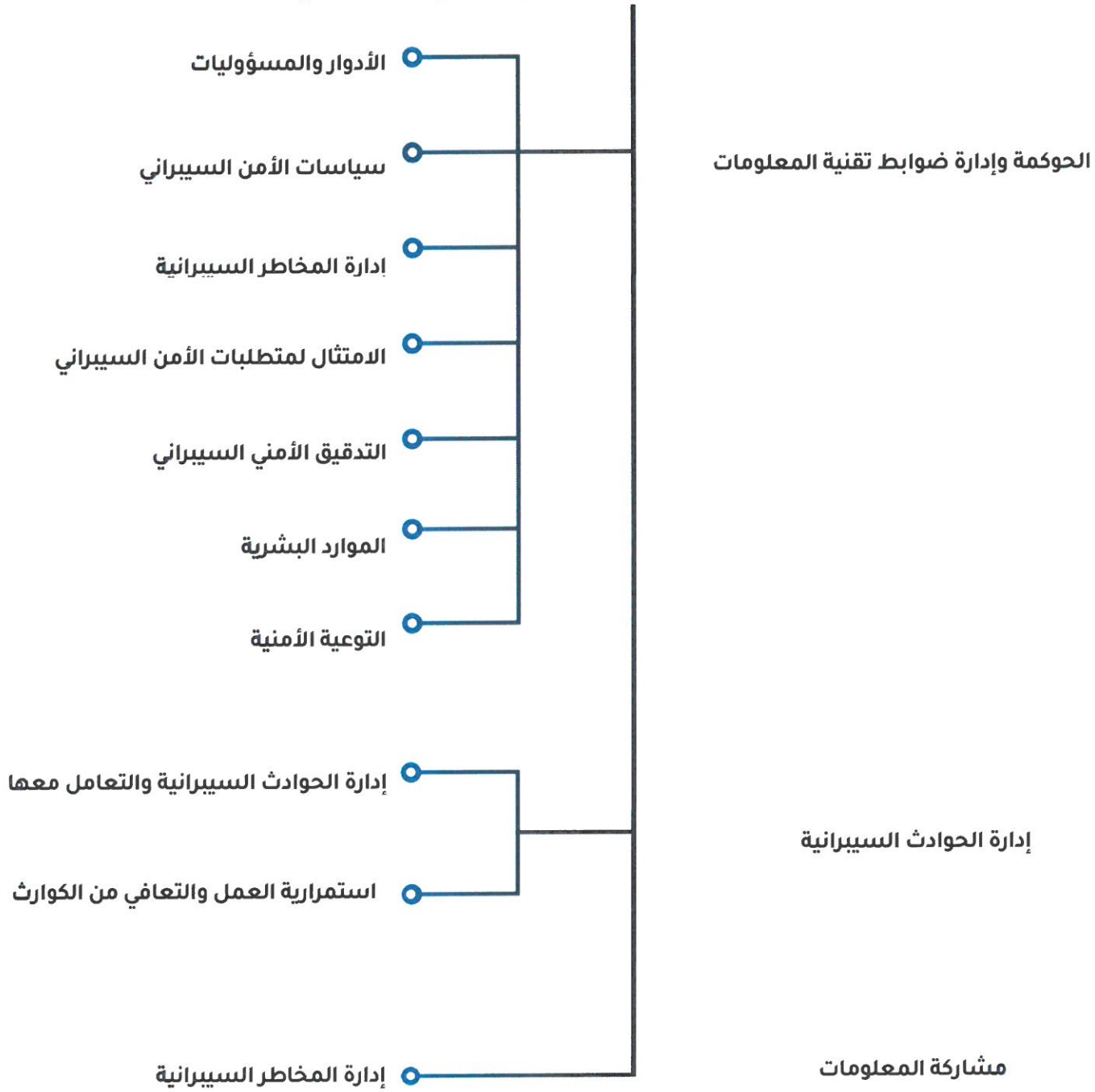
٢٧ مجالاً فرعياً



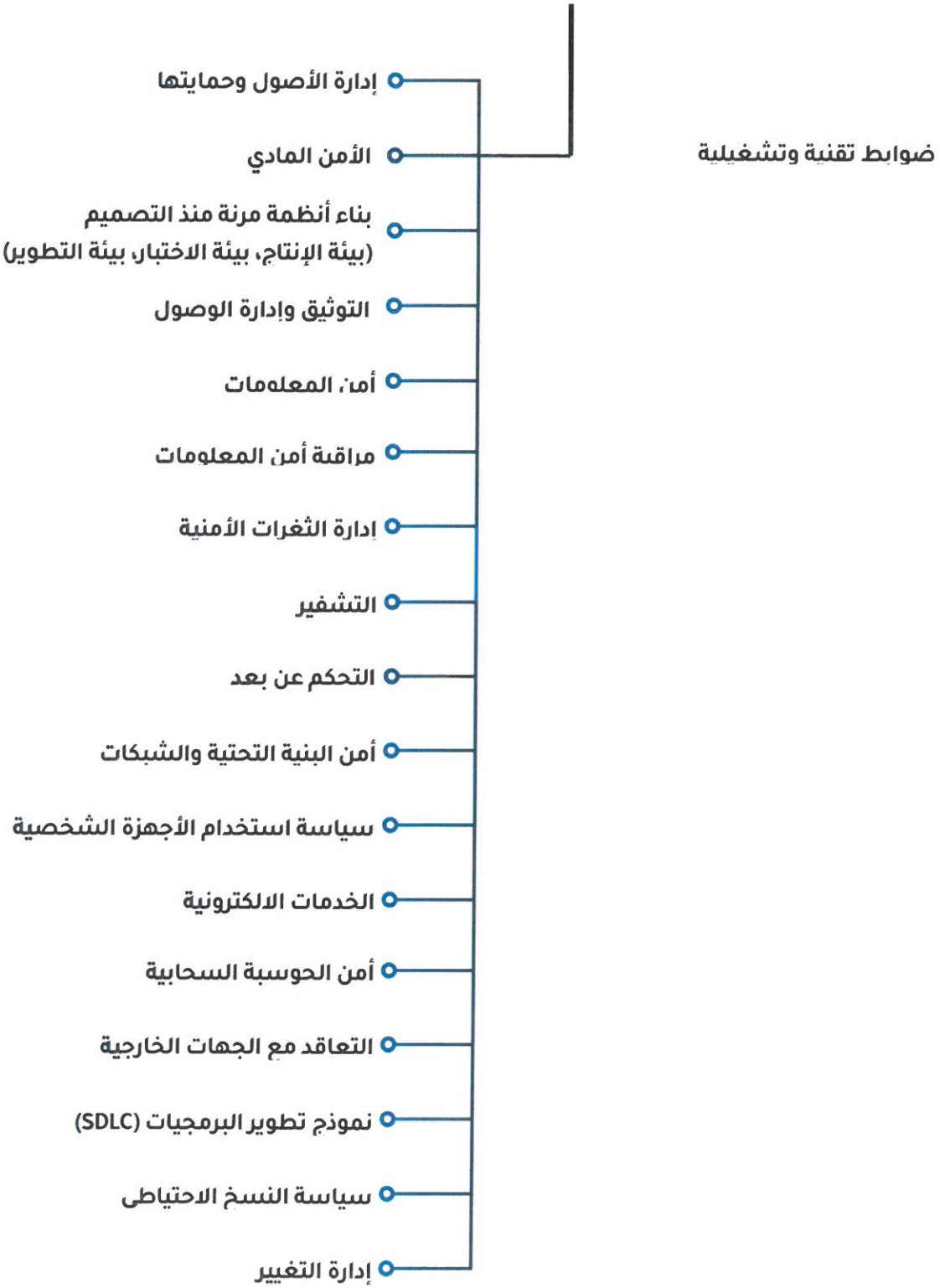
كل مجال رئيسي يتضمن عدة مجالات فرعية تنظم مواضيع الأمن السيبراني المختلفة. ويوضح كل موضوع الغرض والتوقعات الواجب تحقيقها كجزء من برنامج إدارة المخاطر الشاملة.

كلمة" **يجب** "في سياق تحديد الضوابط تشير إلى اعتبار الضابط إلزاميًا لتحقيقه وتنفيذه، أما كلمة" **ينبغي** "في سياق تحديد الضوابط تشير إلى اعتبار الضابط توصية ما لم يُفرض بموجب أطر أو سياسات أخرى للقطاع.

دليل الأمن السيبراني لمؤسسات القطاع المالي غير البنكي



دليل الأمن السيبراني لمؤسسات القطاع المالي غير البنكي



١. الحوكمة وإدارة ضوابط تقنية المعلومات

١,١ الأدوار والمسؤوليات

على جميع المؤسسات المالية غير البنكية في المملكة الأردنية الهاشمية اعتماد نموذج حوكمة ضمن هيكلها التنظيمي لتنفيذ وإدارة برنامج الأمن السيبراني، ويتضمن ذلك مراعاة الأدوار والمسؤوليات التالية:

١,١,١ الإدارة العليا

الإدارة العليا (مجلس الإدارة إن وجد) مسؤولة عن الأمن السيبراني في المؤسسة، وهي بشكل رئيسي مسؤولة عن:

- الإشراف والمسؤولية العامة عن برنامج الأمن السيبراني.
- ضمان تكامل الأمن السيبراني مع الوظائف التجارية، وإدارته بشكل جيد عبر المؤسسة.
- الموافقة على مستوى قبول مخاطر الأمن السيبراني. وذلك لضمان أن المخاطر السيبرانية الإجمالية ضمن النطاق المقبول.
- الموافقة على برنامج الأمن السيبراني، وعملية إدارة المخاطر السيبرانية، والسياسات التي تدير المخاطر السيبرانية.
- دعم وتعزيز ثقافة الوعي بالأمن السيبراني في المؤسسة.
- تخصيص ميزانية وموارد كافية لتلبية متطلبات الأمن السيبراني.

١,١,٢ إدارة أمن المعلومات والأمن السيبراني

يجب على المؤسسة إنشاء وظيفة للأمن السيبراني بطريقة تضمن مستوى مناسبًا من الاستقلالية عن أي دور آخر قد يتعارض مع برنامج الأمن السيبراني وأهدافه. تشمل مسؤوليات وظيفة الأمن السيبراني ما يلي:

١. الحفاظ على عمليات إدارة المخاطر السيبرانية وتطويرها، بالإضافة إلى السياسات والمعايير والإجراءات والمبادئ التوجيهية والمؤشرات الرئيسية للمخاطر والمؤشرات الأداء الخاصة ببرنامج الأمن السيبراني.
٢. مسؤول عن تنفيذ سياسات ومعايير الأمن السيبراني، وتقييم المخاطر وتحديد مسؤوليات الأمن السيبراني

٣. تقديم تقارير دورية إلى الإدارة العليا حول الحالة العامة للأمن السيبراني، وحالة المخاطر السيبرانية / الوضع العام للمؤسسة.

٤. تقييم وإدارة المخاطر التي يتسبب بها مقدمو الخدمات (التعاقدات والجهات الخارجية).

٥. ضمان وجود عمليات فعالة لمراقبة أنظمة تقنية المعلومات، للكشف عن أحداث وحوادث الأمن السيبراني في الوقت المناسب.

٦. ضمان وضوح وتوثيق وتوجيه الأدوار المتعلقة بإدارة المخاطر السيبرانية للموظفين المعنيين.

٧. تقييم فاعلية الضوابط والموافقة على الاستثناءات، مع مراعاة مستوى قبول مخاطر الأمن السيبراني (cyber Risk Appetite).

٨. إبلاغ وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي (Jo-FinCERT)بحوادث الأمن السيبراني، والإشراف على إجراءات الاستجابة للحوادث والتعامل معها وتصعيدها.

٩. تنفيذ تدريبات وتمارين للتوعية بالأمن السيبراني.

١٠. تعيين ضابط للارتباط مع وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي Jo-FinCERT.

١١. إنشاء منصب إداري مسؤول بصلاحيات تنفيذية على مستوى الإدارة العليا (CISO)، أو على مستوى الإدارة الوسطى (مدير) حسب حجم المؤسسة ليكون مسؤولاً عن وظيفة الأمن السيبراني. (سيتم تحديد حجم المؤسسات في تعليمات لاحقة).

١٢. يتمتع بصلاحيات كافية، ويتبع مباشرة للإدارة العليا دون تعارض مع المناصب الأخرى. يجب أن يستوفي الشروط أدناه:

12.1 حاصل على جنسية أردنية.

١٢,٢ تعيين بدوام كامل.

١٢,٣ المؤهلات:

- خبرة لا تقل عن ٨ سنوات في مجال تقنية المعلومات ذي الصلة، منها ٤ سنوات في مجال أمن المعلومات.
- درجة بكالوريوس في تخصص ذي صلة.
- حاصل على شهادة واحدة معتمدة على الأقل في إدارة أمن المعلومات من الشهادات العالمية مثل CISM أو شهادة لـ ISO 27001 Lead Implementer.

١,٢ سياسات الأمن السيبراني

١. يجب تحديد سياسة واضحة للأمن السيبراني، والموافقة عليها من قبل الإدارة العليا، وتعميمها على جميع الموظفين.

٢. يجب مراجعة وتحديث السياسة كل عامين على الأقل، أو عند حدوث تغييرات كبيرة على مستوى التعرض لمخاطر الأمن السيبراني للمؤسسة في ضوء التقنيات الناشئة.

٣. يجب أن تتوافق السياسة مع نُهج الأعمال والتكنولوجيا، لمواجهة مخاطر الأمن السيبراني وتحديد جميع أدوار ومسؤوليات الأمن السيبراني بوضوح.

٤. يجب أن تنقل السياسة بوضوح نية الإدارة ونهج المؤسسة لتحقيق أهدافها في مجال الأمن السيبراني.

١,٣ إدارة المخاطر السيبرانية

١. يجب تحديد عملية إدارة مخاطر الأمن السيبراني والموافقة عليها من قبل الإدارة العليا وتنفيذها.

٢. يجب على المؤسسة دمج إدارة مخاطر الأمن السيبراني مع إدارة المخاطر العامة لضمان إدارة متسقة للمخاطر عبر المؤسسة.

٣. يجب أن يستند برنامج إدارة مخاطر الأمن السيبراني إلى فهم التهديدات والثغرات والمستوى العام للمخاطر ومستوى قبول المخاطر للمؤسسة.

٤. يجب تحديد مستوى المقبول من مخاطر الأمن السيبراني والموافقة عليه من قبل الإدارة العليا.

٥. يجب أن تدعم الإدارة العليا عملية إدارة مخاطر الأمن السيبراني والمشاركة فيها، من خلال ضمان توفير الموارد والقدرات، وتحديد أدوار الموظفين بشكل صحيح في إدارة المخاطر.

٦. يجب أن تشتمل إدارة مخاطر الأمن السيبراني على الأنشطة الأساسية الأربعة التالية:

- تقييم المخاطر (Risk Assessment)
- قياس المخاطر (Risk Measurement)
- التخفيف من المخاطر / معالجتها ((Risk mitigation / treatment)
- مراقبة وإعداد التقارير الخاصة بالمخاطر (Risk monitoring and reporting)

٧. ينبغي تحديث تقييمات مخاطر الأمن السيبراني بانتظام، لمعالجة التغييرات، أو إدخال تقنيات، أو منتجات جديدة وما إلى ذلك قبل النشر، لضمان قياس المخاطر بدقة.

٨. ينبغي اختيار خيارات معالجة المخاطر مثل تخفيف المخاطر، وتجنب المخاطر، ونقل المخاطر، وكيفية معالجة المخاطر المتبقية بناءً على نتائج تقييم المخاطر.

٩. يجب مراقبة نتائج عملية التقييم باستمرار والإبلاغ عنها بانتظام للإدارة العليا.

١٠. ينبغي على المؤسسة تطوير مؤشرات المخاطر الرئيسية (KRIs) لتوفير إنذار مبكر عند زيادة مستوى التعرض للمخاطر، والجوانب المحتملة التي تتسبب في المخاطر. يجب أن تكون مؤشرات المخاطر الرئيسية متوافقة مع المستوى المقبول للمخاطر السيبرانية.

١١. ينبغي بناء برنامج إدارة مخاطر الأمن السيبراني استناداً إلى أفضل الممارسات والمعايير الدولية مثل NIST، وإرشادات ISACA مثلCOBIT و ISO.

١,٤ الامتثال لمتطلبات الأمن السيبراني

١. يجب على المؤسسات ضمان الامتثال للوائح التنظيمية المنشورة المتعلقة بالأمن السيبراني، وما ينشر لاحقًا من قبل البنك المركزي الأردني والتشريعات الوطنية.

٢. يجب على المؤسسة تعيين دور مستقل يكون مسؤول عن مراجعة برامج وعمليات الأمن السيبراني، لضمان الالتزام بالمبادئ التوجيهية والمنشورات بالخصوص.

١,٥ التدقيق الأمني السيبراني

يجب تدقيق نطاق الأمن السيبراني وتكنولوجيا المعلومات من قبل جهة مستقلة داخلية / خارجية، ويجب إجراء التدقيق مرة واحدة على الأقل كل عامين.

١,٦ الموارد البشرية

١. يجب على المؤسسة إجراء فحص أمني قبل توظيف أية موظفين جدد، أو موظفين مؤقتين، أو متعهدين.

٢. يجب على المؤسسة وضع وتطبيق سياسة لاستخدام أصول المعلومات.

٣. ينبغي على المؤسسة ضمان تناوب الوظائف والمسؤوليات، من خلال حصول الموظفين على إجازة/عطلة إلزامية، للحد من فرص التواطؤ والأنشطة الاحتيالية ومخاطر الموظفين (Key-man Risk).

٤. يجب على المؤسسة تضمين أدوار ومسؤوليات الأمن السيبراني في الوصف الوظيفي للوظائف الخاصة بالدرجات الوظيفية ذات الصلة.

٥. يجب على المؤسسة مراجعة جميع صلاحيات الوصول المادي والرقمي الممنوحة لأي موظف بعد تغيير المهام، وتعديل الصلاحيات بناءً على احتياجات العمل الجديدة.

٦. يجب على المؤسسة إلغاء جميع صلاحيات الوصول المادي والرقمي الممنوحة لأي موظف انتهت خدمته على الفور.

١,٧ التوعية الأمنية

١. يجب على المؤسسة تطوير برنامج للتوعية والتدريب على الأمن السيبراني والحصول على موافقة الإدارة العليا.

٢. يجب على المؤسسة عقد جلسات توعية منتظمة لجميع الموظفين والموظفين، المؤقتين، والمتعهدين، على أن تتناول على الأقل:

- استخدام سياسات كلمات المرور الفعالة.
- تحديد رسائل البريد الإلكتروني والروابط الخبيثة.
- الاستخدام المقبول لأصول المعلومات وسياسة المكتب النظيف.
- التهديدات الأمنية السيبرانية في قطاع الخدمات المالية.
- كيفية الإبلاغ عن أي أنشطة وحوادث غير اعتيادية.

٣. ينبغي على المؤسسة إجراء جلسات توعية مخصصة للإدارة العليا والمديرين التنفيذيين لضمان امتلاكهم الفهم المطلوب لتهديدات الأمن السيبراني والثغرات وأدوات التحكم ذات الصلة بأدوارهم.

٤. يجب على المؤسسة تنفيذ برنامج توعية لعملائها بشكل منتظم من خلال قنوات فعالة والتي تشمل وسائل التواصل الاجتماعي والرسائل والنشرات وغيرها.

٥. ينبغي على المؤسسة تنفيذ برامج تدريب متخصصة لموظفي الأمن السيبراني وتكنولوجيا المعلومات. ينبغي أن تتضمن البرامج تدريبًا على المنتجات والخدمات المتعلقة بالأمن السيبراني، بالإضافة إلى شهادات احترافية في الأمن السيبراني بناءً على أدوار الموظفين والمستوى المطلوب.

٦. ينبغي على المؤسسة إجراء عملية تقييم لقياس فاعلية جلسات وبرامج التوعية. يمكن إجراء عملية التقييم من خلال اختبارات هجمات محاكاة للهندسة الاجتماعية (على سبيل المثال، رسائل تصيد مزيفة).

٢. ضوابط تقنية وتشغيلية

٢,١ إدارة الأصول وحمايتها

١. يجب على المؤسسة تطوير عملية شاملة لإدارة الأصول.

٢. يجب على المؤسسة الحفاظ على جرد محدث لجميع الأصول، بما في ذلك الأجهزة والبرامج.

٣. يجب أن تتضمن عملية إدارة الأصول:

- تحديد وتصنيف الموارد المختلفة، بما في ذلك البرامج والأجهزة وموارد الشبكة.

- تحديد ملكية كل أصل ومسؤولية الحفاظ عليه.
- تنفيذ إجراءات التصنيف وآلية التعامل معها.
- فرض ضوابط وتدابير أمنية لضمان حماية البيانات والمعلومات.

٤. ينبغي تصنيف أصول المعلومات وفقًا للسرية والتكامل والتوافر (Availability , Integrity.Confidentiality).

٥. ينبغي على المؤسسة تطوير مخططات لتدفق البيانات عالية المستوى ومنخفضة المستوى وتحديثها بانتظام.

٦. يجب على المؤسسة التأكد من تسجيل جميع الانظمة القديمة (Legacy Systems) التي لا تزال قيد الاستخدام (سواء كانت مهمة أم غير مهمة). يجب تحديد الثغرات المرتبطة بها على الفور وتطبيق ضوابط تعويضية.

٧. يجب على المؤسسة مراجعة وتحديث سجل الأصول بانتظام.

٢,٢ الأمن المادي

١. يجب على المؤسسة تحديد المناطق والمواقع الآمنة التي تحتوي على معلومات وأصول حساسة. ويشمل ذلك على سبيل المثال لا الحصر: مراكز البيانات والمكاتب والغرف وأجهزة الشبكة.

٢. يجب على المؤسسة تحديد قائمة محدثة بالأفراد المخول لهم الوصول إلى المواقع والمناطق الآمنة.

٣. يجب على المؤسسة حماية المناطق والمواقع الآمنة من خلال ضوابط مادية تسمح فقط للموظفين المخولين بالدخول بناءً على احتياجات العمل. ينبغي مراجعة قوائم التحكم في الوصول المادي على الأقل سنويًا.

٤. يجب التحكم في الوصول المادي إلى مراكز البيانات والشبكات. ويجب استخدام اقفال للأبواب لضمان عدم الوصول إليها إلا من قبل الموظفين المصرح لهم.

٥. ينبغي على المؤسسة تنفيذ ضوابط الكشف والحماية للمناطق الآمنة ومواقع المهام الحرجة ضد المخاطر البيئية بما في ذلك - على سبيل المثال لا الحصر - انقطاعات التيار الكهربائي الحرائق، التقلبات في درجة الحرارة، والرطوبة، وتسرب المياه.

٦. ينبغي على المؤسسة الاحتفاظ بسجلات دخول المنشأة وأي مناطق أو مواقع آمنة محددة. وهذا ينطبق على جميع الموظفين المؤقتين والزوار والضيوف.

٧. يجب على المؤسسة مراقبة الوصول إلى المواقع الآمنة باستخدام كاميرات الفيديو وكشف الحركة. يجب أن يتم الاحتفاظ بمقاطع الفيديو المسجلة وفقاً للتشريعات المحلية.

٨. يجب مراقبة جميع الزوار الذين يُسمح لهم بدخول المواقع الآمنة.

٢,٣ بناء أنظمة مرنة منذ التصميم (بيئة الإنتاج، بيئة الاختبار، بيئة التطوير)

١. يجب على المؤسسة فصل بيئات التطوير والاختبار والإنتاج على مستوى كل من الشبكة والوصول الرقمي.

٢. يجب ان تمر التطورات والإصدارات الجديدة بشكل شامل في بيئة الاختبار.

٣. ينبغي ألا يتمكن المطورون من الوصول إلى بيئة الإنتاج.

٤. ينبغي على المؤسسة مراقبة أنشطة المطورين، سواء كانوا موظفين أو عمالًا مؤقتين.

٥. يجب إزالة أي بيانات الاختبار أو النصوص البرمجية المصدرية (source Code) في النظام قبل تشغيل النظام في بيئة الإنتاج، ويجب توفير النص البرمجي المعالج (compiled Code) فقط على أنظمة الإنتاج.

٦. يجب على المؤسسة عدم استخدام بيانات الإنتاج لأغراض الاختبار أو التطوير ما لم يتم تفويض ذلك صراحةً من قبل الإدارة ولأغراض العمل.

٧. لا يجوز استخدام بيئة الإنتاج كبيئة اختبار تحت أي ظرف من الظروف.

٨. يجب على المؤسسة التأكد من أن مستوى أمان بيئة الاختبار تتطابق مع تلك في بيئة الإنتاج قبل نقل أي بيانات ومعلومات مصنفة.

٢,٤ التوثيق وإدارة الوصول

١. يجب أن تمتلك كل مؤسسة اسم نطاق فريد يكون بمثابة معرّفها المميز عبر الإنترنت.

٢. يجب مصادقة المستخدمين باستخدام معرف فريد وكلمة مرور مخصصة لهم للوصول إلى جميع الأنظمة.

٣. يجب أن يستند تفويض المستخدم على مبدأي: الحاجة للمعرفة والحد الأدنى المطلوب للوصول (Need-to-Know , Least Privilege)

٤. يجب وضع ضوابط مناسبة لتقسيم المهام، لتقليل مخاطر إساءة استخدام النظام بشكل غير مقصود و/أو عمداً.

٥. يجب اعتماد جميع طلبات وصول المستخدمين قبل منح الصلاحيات.

٦. يجب على المؤسسة تعديل صلاحيات الوصول عند تغيير المسؤوليات. على سبيل المثال، يجب تغيير صلاحيات الوصول الخاصة بأي موظف يتم نقله الى قسم آخر

٧. ينبغي مراجعة صلاحيات الوصول بشكل دوري (على الأقل سنويًا).

٨. يجب تطوير وتنفيذ سياسة قوية لكلمات المرور.

٩. يجب حظر الوصول المشترك إلى الموارد من خلال مشاركة كلمات المرور.

١٠. يجب تقييد الوصول إلى مستوى (Admin level) على الأشخاص المصرح لهم فقط.

١١. ينبغي تقسيم كلمات مرور المسؤول، مثل مسؤول النظام (المستخدم ذو الامتيازات العالية)، بين مستخدمين اثنين، واستخدامها فقط عند الحاجة إلى الامتيازات الإضافية للحسابات الامتيازات العالية.

١٢. ينبغي استخدام مصادقة المتعددة (MFA) لمسؤولي الوصول إلى الأنظمة الحرجة.

١٣. يجب تعطيل تعريفات تسجيل الدخول وكلمات المرور للموظفين فور إنهاء خدماتهم او ايقافها.

٢,٥ أمن المعلومات

١. يجب على المؤسسة الحفاظ على تدابير تقنية وتنظيمية مناسبة لحماية البيانات أثناء تخزينها أو نقلها

٢. يجب تقييد الوصول إلى البيانات الحساسة ليقتصر فقط على الأشخاص المصرح لهم.

٣. يجب إدارة المعلومات الحساسة المخزنة على الأصول (الرقمية او المادية) طوال عملية الإزالة والنقل والإتلاف.

٤. ينبغي على المؤسسة تنفيذ تدابير لمنع فقدان البيانات ولمراقبة عمليات نقل البيانات.

٥. ينبغي على المؤسسة وضع سياسة احتفاظ بالبيانات تحدد مدة الاحتفاظ بالبيانات وإتلافها عند عدم الحاجة إليها بعد ذلك.

٦. يجب إتلاف المعلومات الحساسة باستخدام تقنيات تجعل من المستحيل استردادها.

٢,٦ مراقبة أمن المعلومات

١. يجب على المؤسسة تحديد ما يحتاج إلى مراقبة (الأنظمة، والتطبيقات، والشبكة، وقواعد البيانات، وما إلى ذلك) ومستوى المراقبة المطلوب لكل منها.

٢. ينبغي على المؤسسة تحديد البيانات المراد مراقبتها والأحداث الأمنية المطلوب تسجيلها.

٣. ينبغي على المؤسسة إنشاء آلية مراقبة في الوقت الفعلي لجمع وربط وتحديد أنشطة المستخدم والمسؤول والنظام والعمليات / الخدمات غير الطبيعية على النظام وقواعد البيانات والشبكة في الوقت المناسب مع التحقق من فعالية التدابير الأمنية الموضوعة.

٤. ينبغي على المؤسسة تنفيذ أدوات للمراقبة والكشف عن حالات الخرق الأمني المحتملة أو الأنشطة غير الطبيعية والتنبيه بها.

٥. يجب على المؤسسة تطبيق آلية مزامنة (time synchronization) لجميع مكونات تقنية المعلومات والأنظمة الأمنية.

٦. ينبغي جمع السجلات في مكان أمن منفصل عن مصادر جمع السجلات. وينبغي تنفيذ عملية لضمان سلامة السجلات المخزنة، والتأكد من عدم السماح لمسؤولي تقنية المعلومات بالتلاعب بها.

٧. يجب تأمين السجلات عن طريق تقييد الوصول للأفراد بحسب حاجة العمل لأداء وظائفهم.

٨. يجب وضع وتنفيذ إجراءات لمراجعة سجلات جميع الأنظمة للكشف عن أي تشوهات أو أنشطة مشبوهة.

٢,٧ إدارة الثغرات الأمنية

١. يجب على المؤسسة إنشاء عمليات لفحص الثغرات واختبارات الاختراق للأنظمة.

٢. يجب على المؤسسة تحديد نطاق فحص الثغرات الذي يتضمن على سبيل المثال لا الحصر (محطات العمل، أجهزة الشبكة، الخوادم، ... إلخ).

٣. يجب على المؤسسة تحديد نطاق اختبارات الاختراق، لتشمل الخدمات المتاحة عبر الإنترنت.

٤. يجب على المؤسسة تحديد دورية إجراء فحص الثغرات واختبار الاختراق وفقًا لأهمية الانظمة، بحسب أفضل الممارسات والتشريعات ذات الصلة.

٥. ينبغي على المؤسسة إجراء فحص للثغرات كل ستة أشهر على الأقل أو عند حدوث تغيير كبير (مثل تثبيت أنظمة أو أجهزة أو تطبيقات جديدة وما إلى ذلك) في البنية التحتية للمؤسسة أو عند اكتشاف الثغرات جديدة.

٦. ينبغي على المؤسسة إجراء اختبار اختراق على الأقل سنويًا، أو عند حدوث تغيير كبير في الخدمات المتاحة عبر الإنترنت.

٧. يجب على المؤسسة تطبيق التحديثات لمعالجة الثغرات المعروفة. ويجب ضمان التنفيذ في الوقت المناسب لتقليل التعرض للمخاطر السيبرانية.

٨. يجب فحص التحديثات على بيئة الاختبار قبل تنفيذها في بيئة الإنتاج.

٢,٨ التشفير

١. يجب تخزين مفاتيح التشفير السرية في أماكن آمنة.

٢. يجب تقييد الوصول إلى مفاتيح التشفير على الموظفين المصرح لهم.

٣. ينبغي وضع إجراءات لضمان إمكانية اعتماد طلبات مفاتيح التشفير بشكل مناسب، وتوفيرها في الوقت المناسب، وتسجيلها بشكل صحيح.

٤. تجنب استخدام نفس المفتاح عبر بيئات التطوير والاختبار والإنتاج.

٥. يجب إدارة مفاتيح التشفير وحمايتها بشكل أمن طوال دورة حياتها. ويشمل ذلك الحماية من التعديل والفقدان والوصول/الاستخدام غير المصرح به أو التسريب.

٦. يجب أن تكون الخوارزميات ودرجة تعقيد مفاتيح التشفير موثوقة ومتوافقة مع أفضل الممارسات الأمنية.

٧. يجب حماية المعدات المستخدمة في إنشاء وتخزين وأرشفة المفاتيح بشكل مادي باستخدام ضوابط وصول آمنة ومناسبة.

٨. في حالة تعرض مفتاح تشفير للخطر، يجب إلغاء المفتاح الحالي، وإنشاء مفتاح جديد (أو زوج مفاتيح).

٩. يجب تحديد الفترة الزمنية لمفاتيح التشفير. ويجب وضع إجراء لاستبدال المفاتيح منتهية الصلاحية والحفاظ عليه.

تطبيق التشفير

١. يجب تنفيذ التشفير باستخدام طرق وتقنيات معتمدة.

٢. يجب تطبيق آليات لتشفير وسائط النسخ الاحتياطي ووسائط تخزين البيانات والمعلومات الحساسة، وتخزينها في موقع آمن مادياً.

٣. يجب تشفير البيانات الحساسة عند تخزينها.

٤. يجب نقل البيانات الحساسة عبر قناة آمنة (القناة الآمنة هي اتصال شبكة مشفر).

٥. عند نقل معلومات المؤسسة الحساسة خارج أنظمة الشركة الآمنة، يجب تشفيرها. قد يشمل التشفير استخدام تشفير ملف يتم إرساله عبر البريد الإلكتروني، أو تشفير قرص صلب محمول يتم استخدامه لنقل البيانات، أو من خلال استخدام بروتوكولات نقل مشفرة مثل TLS.

٦. ينبغي أن يكون لدى جميع أجهزة الشركة المملوكة آلية تشفير كامل للقرص.

٢,٩ التحكم عن بعد

١. يجب استخدام طرق مصادقة مركزية لإدارة وصول المستخدمين للأنظمة عن بعد.

٢. يجب تأمين طرق الوصول عن بعد باستخدام آليات ومعايير تشفير قوية.

٣. يجب أن يعتمد منح صلاحيات الوصول عن بعد وتحديد المدد الزمنية بناءً على احتياجات العمل.

٤. ينبغي على المؤسسة تعديل صلاحيات الوصول عن بعد مع تغير المسؤوليات. على سبيل المثال، إذا انتقل موظف إلى قسم آخر، يجب تغيير صلاحياته.

٥. يجب إعادة تسجيل الدخول لفترات الوصول عند مرور ٣٠ دقيقة بحد أقصى من عدم القيام بأي نشاط.

٦. يجب على المؤسسة تطبيق آليات مصادقة ثنائية على الأقل للتحقق هوية المستخدمين قبل الوصول إلى أصول الموارد والمعلومات الداخلية.

٧. يجب على المؤسسة مراقبة اتصالات الوصول عن بعد غير المصرح بها والأنشطة الأخرى المشبوهة.

٨. ينبغي تسجيل جميع فترات الوصول عن بعد ومراقبتها.

٩. يجب منح موظفي الجهات الخارجية حق الوصول عن بعد على أساس مؤقت ومقتصر على احتياجات العمل الفعلية. كما يجب تسجيل ومراقبة جلسات الوصول عن بعد.

١٠. ينبغي حظر نسخ ونقل وتخزين البيانات والمعلومات الحساسة على الأقراص الصلبة و الوسائط الإلكترونية القابلة للإزالة، إلا إذا تم تفويض ذلك صراحةً لحاجة تشغيلية محددة.

١١. يجب مراجعة أذونات الوصول عن بعد بشكل دوري.

٢,١٠ أمن البنية التحتية والشبكات

١. يجب حصر جميع أجهزة ومكونات الشبكة ومراقبتها وإدارتها بشكل مناسب لتحديد قابلية التأثر بالمخاطر أو الثغرات ومستوى الحماية المطلوب للالتزام بالسياسات والمعايير.

٢. ينبغي تطبيق ضوابط أمنية متعددة لأمن الشبكة لضمان عدم تقييد الشبكة عند فشل مكون واحد.

٣. يجب ضبط إعدادات جميع أجهزة الشبكة وفقًا لمعايير أمن ضبط الشبكات.

٤. يجب حظر البروتوكولات غير الآمنة (مثل FTP و TELNET، وما إلى ذلك).

٥. يجب على المؤسسة تجزئة الشبكة لشبكات أصغر (Network Segmentation) لتقليل التأثير المحتمل لاختراق الأمان

٦. يجب على المؤسسة فرض تحكم بالوصول بين أجزاء الشبكة من خلال جدار حماية الشبكة (firewall).

٧. يجب على المؤسسة تنفيذ مناطق (DMZ) معزولة عن مناطق الشبكة الموثوقة للخدمات المتاحة للجمهور، وتقييد حركة البيانات الواردة إلى عناوين IP وبروتوكولات ومنافذ محددة.

٨. يجب على المؤسسة استخدام جدران الحماية، ونظام اكتشاف التسلل / (IDS) و نظام منع التسلل (IPS)لمراقبة والتحكم في حركة البيانات الواردة والصادرة على الشبكة.

٩. يجب على المؤسسة مراجعة وتحديث إعدادات جدار الحماية بانتظام لتعكس سياسات أمن المؤسسة.

١٠. ينبغي حماية جميع أجهزة الشبكة ضمن منطقة آمنة مادياً.

١١. ينبغي إمداد معدات الشبكة الأساسية بمصدر طاقة (UPS) ومولدات مصممة بشكل مناسب.

١٢. يجب على المؤسسة تنفيذ ضوابط وصول قوية بناءً على مبدأ الحد الأدنى المطلوب (Least Privilege).

١٣. ينبغي التحكم في الوصول إلى أجهزة الشبكة من خلال قوائم الوصول لتقييد إمكانية الوصول إلى المعدات بحيث تقتصر على عدد محدود من المواقع.

١٤. يجب على المؤسسة تطوير وتنفيذ عملية إدارة التحديثات لضمان تحديث جميع البرامج وأنظمة التشغيل بأحدث تحديثات الأمان.

١٥. يجب ضبط إعدادات جميع مكونات الشبكة لتوفير سجلات تدقيق لمراقبة الأمن الضرورية والمستمرة.

١٦. ينبغي على المؤسسة تنفيذ خدمات للحد من هجوم حجب الخدمة(DoS) ، والهجمات الموزعة لحجب الخدمة(DDoS) ، لحماية الخدمات المنشورة الحرجة عبر الإنترنت

١٧. يجب ضبط إعدادات جميع الأنظمة والتطبيقات وفقًا لأفضل الممارسات الأمنية. يمكن تجاوز هذه الإعدادات في حال وجود متطلبات خاصة بالتطبيق لضمان تشغيلها.

١٨. يجب على المؤسسة استخدام حلول مكافحة الفيروسات والبرامج الضارة على جميع الاجهزة والخوادم.

١٩. يجب على المؤسسة تأمين الشبكات اللاسلكية باستخدام تشفير قوي (مثل WPA3).

٢٠. ينبغي على المؤسسة إجراء تدقيق دوري لإعدادات الشبكة اللاسلكية.

٢١. يجب على المؤسسة تفعيل خاصية جمع السجلات الأمنية لمكونات البنية التحتية الحساسة للمراقبة.

أمن البريد الإلكتروني

١. ينبغي على المؤسسة الرجوع إلى دليل "Securing the Financial Sectors Email Ecosystem"

٢,١١ سياسة استخدام الأجهزة الشخصية

١. يجب على المؤسسة التأكد من أن جميع الأجهزة المحمولة تملك كلمات مرور للوصول إلى النظام، وأنها مقفلة عند عدم استخدامها.

٢. يجب على المؤسسة منع وصول الأجهزة التي تم عمل "root" أو "jailbreak" لها إلى التطبيقات والخدمات.

٣. لا يجوز السماح بتثبيت تطبيقات من مصادر غير موثوقة و / أو متاجر تابعة لجهة خارجية على الأجهزة المحمولة (الهاتف، الأجهزة اللوحية) إلا بعد موافقة صريحة.

٤. يجب على المؤسسة تحديث برامج مكافحة الفيروسات ونظام التشغيل والبرامج الأخرى بانتظام.

٥. ينبغي أن تكون المؤسسة قادرة على مسح البيانات عن بُعد للجهاز المفقود أو المسروق لمنع سرقة البيانات.

٦. يجب ألا يتمكن المستخدمون من تثبيت البرامج والتطبيقات على الأجهزة المحمولة دون موافقة صريحة.

٧. ينبغي تطبيق ضوابط مثل تشفير القرص.

٨. ينبغي إجراء فحص أمني للأجهزة المحمولة قبل منح حق الوصول إلى شبكة المؤسسة.

٩. يجب تعطيل منفذ USB والقرص المضغوط / قرص DVD ما لم يكن مطلوبًا بشكل صريح لاحتياجات العمل.

١٠. ينبغي على المؤسسة استخدام برنامج إدارة الأجهزة المحمولة (MDM) على الأجهزة المحمولة الخاصة بالمؤسسة.

١١. ينبغي تسجيل ومراقبة أنشطة وصول الأجهزة المحمولة.

١٢. ينبغي إجراء توعية أمنية لمستخدمي الأجهزة المحمولة والاتصال بشبكةWi-Fi .

٢,١٢ الخدمات الإلكترونية

١. يجب تحديد رقم مرجعي فريد لجميع المعاملات والمراسلات المالية لتتبعها.

٢. ينبغي على المؤسسة تنفيذ ضوابط عمل لكشف ومنع أنشطة الدفع والتحويل المشبوهة.

٣. مراقبة الحركات التجارية للعملاء على مدار اليوم بما في ذلك حدود الحركات من حيث القيم ودورية هذه الحركات.

٤. ينبغي إنهاء جلسة المستخدم بعد ٥ دقائق على أقصى تقدير من عدم النشاط.

٥. يجب على المؤسسة استخدام تقنيات الاتصال لتجنب هجمات"Man-in-The-Middle" .

٦. يجب على المؤسسة استخدام آليات المصادقة متعددة العوامل"MFA".

٧. ينبغي على المؤسسة منع تثبيت التطبيق الخاصة بالمؤسسة (Mobile Application) على الأجهزة التي تم عمل "root" أو "jailbreak" لها.

٨. ينبغي على المؤسسة تطبيق حلول أمنية لحماية العلامة التجارية والخدمات عبر الإنترنت، بما في ذلك وسائل التواصل الاجتماعي.

٢,١٣ أمن الحوسبة السحابية

١. يجب توقيع اتفاقية خدمات الحوسبة السحابية وتحديد شروط اتفاقيات مستوى الخدمة (SLA) بشكل واضح، لتشمل حماية البيانات وتدميرها، واستمرارية العمل وتوافر الخدمة، والأدوار والمسؤوليات والشروط القانونية.

٢. يجب على المؤسسة عدم توقيع اتفاقية مع مزود خدمات الحوسبة السحابية (CSP) قبل استكمال وتجاوز جميع متطلبات الأمان.

٣. ينبغي على المؤسسة التأكد من أن اتفاقيات مستوى الخدمة (SLAs) تعكس أعلى درجات التوافر للتطبيقات والبيانات في حالة حدوث انقطاعات أو توقف مخطط له أو غير مخطط له. مع سياسة استمرارية الأعمال والتعافي من الكوارث وآليات النسخ الاحتياطي والتكرار.

٤. يجب على المؤسسة توقيع اتفاقية عدم إفشاء المعلومات (NDA) مع مزود خدمات الحوسبة السحابية (CSP) قبل توفير أي خدمة.

٥. يجب على المؤسسة تقييم تأثير مبادرات الحوسبة السحابية على الامتثال للقوانين والتشريعات التي تفرض التزامات الخصوصية والأمان على المؤسسة. وعلى وجه التحديد، تلك المبادرات التي تتضمن موقع البيانات وضوابط الخصوصية والأمان وإدارة السجلات.

٦. يجب حماية بيانات المؤسسة وأصولها التي تقوم بتخزينها أو معالجتها من العبث المادي، والفقدان، والتلف.

٧. يجب حماية بيانات المؤسسة بشكل كافٍ من العبث والتنصت أثناء نقلها عبر الشبكات داخل وخارج خدمات الحوسبة السحابية. ينبغي تحقيق ذلك باستخدام مجموعة من التشفير ومصادقة الخدمة والحماية على مستوى الشبكة.

٨. يجب على المؤسسة أن تضمن ضمن العقد إخطارها "فورًا" بأي خرق مؤكد دون أي تأخير غير مبرر.

٩. يجب على المؤسسة التأكد من أن مزود خدمات الحوسبة السحابية (CSP) ينفذ أفضل ممارسات الأمان عند تثبيت وإعداد الخدمة.

١٠. يجب على المؤسسة مراقبة بيئة خدمات الحوسبة السحابية بحثًا عن التغييرات والأنشطة غير المصرح بها.

١١. يجب على المؤسسة مراقبة حالة أمان أنظمة المعلومات التي يتم استضافتها على خدمات الحوسبة السحابية.

٢,١٤ التعاقد مع الجهات الخارجية

١. يجب على المؤسسة الحفاظ على سجل محدث للخدمات التي يقدمها الباعة، المتعهدين، جهات خارجية ومصادر خارجية مع اتفاقية مستوى خدمة (SLA) سارٍ لكل منها.

٢. يجب على المؤسسة التأكد من أن الاتفاقية تتضمن بنود خاصة ب:

- الامتثال للسياسات والإجراءات التنظيمية والقوانين والتشريعات ذات الصلة.
- الأدوار والمسؤوليات.
- بند حق التدقيق.

- إخطار بأي خروقات أو حوادث أمنية.
- الإجراءات التي يجب اتخاذها إذا تجاهل الطرف الثالث متطلبات أمن المؤسسة.
- نطاق واضح لخدمات الاستعانة الخارجية.
- بند إنهاء الخطة وخطط المغادرة.

٣. يجب على الطرف الثالث الذي يُمنح حق الوصول إلى معلومات غير عامة توقيع اتفاقية عدم إفشاء (NDA)قبل منحه حق الوصول.

٤. يجب أن يكون الوصول إلى البيئة الداخلية والمعلومات غير العامة بناءً على أقل صلاحيات ممكنة.

٥. ينبغي إجراء تقييم المخاطر وفقًا لعملية إدارة المخاطر.

٦. يجب على المؤسسة أن تطلب من الأطراف الثالثة إخطارها بأي عمليات نقل أو إنهاء لأفراد العمل الذين يمتلكون بيانات المؤسسة و/أو بطاقات دخول، أو الذين لديهم صلاحيات على الأنظمة.

٧. يتم حماية الأنشطة الخارجية الحرجة، كحد أدنى، بنفس معيار الرعاية المطبق عليها كما لو كانت تُدار داخل المؤسسة.

٨. يجب على المؤسسة مراجعة ومراقبة جميع الاتصالات بشبكتها وأنشطتها.

٢,١٥ نموذج تطوير البرمجيات (SDLC)

١. يجب على المؤسسة تحديد عمليات لإدارة دورة حياة التطوير لضمان معالجة متطلبات الأمان خلال جميع مراحل دورة حياة تطوير البرامج أو الحصول على برامج جديدة.

٢. التأكد من دمج ضوابط الأمن السيبراني في جميع مراحل دورة حياة النظام / التطبيق.

٣. يجب أن تحدد وتوثق متطلبات العمل الخاصة باقتناء / تطوير النظم / التطبيقات متطلبات الأمان أيضًا. ويشمل ذلك على سبيل المثال لا الحصر التحكم في الوصول، وإدارة صلاحيات الوصول، والمصادقة، وتسجيل الأحداث، وسجل المراجعة، وإدارة جلسات المستخدم، وفصل الواجبات، وأقل امتياز وما إلى ذلك.

٤. يجب على المؤسسة التأكد من تطوير جميع التطبيقات الداخلية بما يتماشى مع ممارسات البرمجة الآمنة مثل (threat modeling, input validation, least privilege, fault deny, defense in-depth, and fail secure whilst mitigating against OWASP vulnerabilities)، (OWASP Secure Code Practices)

٥. يجب على المؤسسة تنفيذ تقنيات البرمجة الآمنة. يمكن للمؤسسة تبني إحدى أفضل الممارسات الدولية (مثل ممارسات برمجة OWASP الآمنة). ومن المتوقع أن توفير هذه الممارسات إجراءات مضادة وأن

تتناول على الأقل المخاطر والعيوب ونقاط الضعف المحددة في (OWASP Top Ten Security Risks and CWE/SANS TOP 25 Most Dangerous Software Errors).

٦. ، يجب إجراء تحليل للنص البرمجي (عبر مسح الثغرات واختبار الاختراق) خلال مرحلة / مراحل الاختبار والتحقق.

٧. يجب اختبار التطبيقات المطورة داخليًا بشكل شامل من قبل فريق من أخصائي اختبار البرامج المستقلين ومالكي الأعمال / التطبيقات.

٨. ينبغي مراجعة النص البرمجي قبل نشره في بيئة الإنتاج للتأكد من أن البرنامج يتوافق مع المبادئ والممارسات المعتمدة، وتحديد ومعالجة أي نقاط ضعف مكتشفة.

٩. سيتبع تعديل النص البرمجي أو التحديث الطارئ سياسة إدارة التغيير.

١٠. ينبغي على المؤسسة ترتيب اتفاقيات مع المورد لإدارة النص البرمجي للتطبيقات الحرجة المستضافة .

٢,١٦ سياسة النسخ الاحتياطي

١. يجب على المؤسسة إجراء نسخ احتياطي منتظم للبيانات والأنظمة الحرجة.

٢. يجب على المؤسسة اختبار عمليات النسخ الاحتياطي والاستعادة بانتظام لضمان فعاليتها.

٣. يجب على المؤسسة تخزين النسخ الاحتياطية في بيئات آمنة وخاضعة للرقابة.

٤. يجب على المؤسسة تحديد فترات احتفاظ لأنواع مختلفة من النسخ الاحتياطية.

٥. يجب على المؤسسة وضع إجراءات للتخلص الأمن من النسخ الاحتياطية التي لم تعد هناك حاجة إليها.

٢,١٧ إدارة التغيير

١. يجب وضع اجراءات لعملية إدارة التغيير والموافقة عليها وتنفيذها.

٢. يجب على المؤسسة تحديد المخاطر والتأثيرات في بداية التغيير مباشرة ووضع خطط التنفيذ والتراجع.

٣. يجب على المؤسسة فحص التغيير في بيئة اختبارية قبل تنفيذه على بيئة الانتاج.

٤. يجب الحصول على موافقة على التغيير قبل إصداره / نقله وتوثيق التغيير المُكتمل.

٥. ينبغي على المؤسسة تشكيل مجلس استشاري للتغيير(CAB) ، لمراجعة والموافقة على التغييرات المقترحة.

٦. التأكد من أن المجلس الاستشاري للتغيير (CAB) يضم ممثلين من الإدارات ذات الصلة، بما في ذلك أمن وتكنولوجيا المعلومات.

٧. يجب على المؤسسة مراقبة الأنظمة أثناء وبعد تنفيذ التغييرات لأي مشاكل متعلقة بالأمان.

٣. إدارة الحوادث السيبرانية

٣,١ إدارة الحوادث السيبرانية والتعامل معها

٣,١,١ عمليات إدارة الحوادث

١. يجب على المؤسسة إعداد خطة استجابة شاملة للحادث توضح عملية إدارة الحوادث بالكامل، بداية من تحديدها وحتى حلها.

٢. يجب على المؤسسة التأكد من تشكيل فريق محدد مسؤول عن إدارة حوادث الأمان، وموظفين مدربين ذوي كفاءة (بشكل مستمر).

٣. يجب على المؤسسة تنفيذ إجراء يتيح للموظفين الإبلاغ عن أي أنشطة مشبوهة أو حوادث محتملة على الفور.

٤. يجب على المؤسسة ضمان التوفر المستمر لعناصر الاستعداد للحادث المطلوبة مثل:

- جداول النسخ الاحتياطي للبيانات.
- تصاميم محدثة للبنى التحتية والنظام.
- أدوات جمع الحزم وتحليل البروتوكولات، بالإضافة إلى أدوات جمع الأدلة والتحقيق الجنائي الرقمي.

٥. ينبغي على المؤسسة توثيق جميع مراحل الاستجابة للحادث (response, containment, recovery and after action review)، من خلال مسؤول الحادث (Incident Manager).

٦. يجب على المؤسسة مشاركة جميع الحوادث ومعلومات استخبارات التهديدات المرتبطة بها مع وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي (Jo-FinCERT) خلال مراحل الاستجابة المختلفة للحوادث.

٣,١,٢ تصنيف شدة الحوادث

١. تقوم المؤسسة بتنفيذ تصنيف شدة الحوادث على مستوى المؤسسة لتحديد النقطة التي ينبغي عندها معالجة الحادث ككارثة، بالإضافة إلى تحديد إجراءات التصعيد، والموارد البشرية، ومدة الاسترداد.

٢. يجب على المؤسسة إخطار وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي (Jo-FinCERT) عن الحادث وفقًا للجدول الزمني التالي:

- بعد إغلاق الحادث بالنسبة للحوادث "منخفضة."
- خلال ساعتين من تأكيد الحادث بالنسبة للحوادث "متوسطة."

- إبلاغ (Jo-FinCERT)على الفور عند حدوث وتحديد حادث أمني مصنف على أنه "عالي الخطورة."

٣. ينبغي على المؤسسة استخدام مصفوفة فئة التأثير وتصنيف الشدة التالية.

Incident / Impact	Functional Impact	Information Impact				Recoverability Impact
	Service Disruption	Data Privacy Breach	Data Confidentiality Breach	Data Integrity Breach	Proprietary Breach	
Low	The entity can still provide all critical services to all users but with decreased efficiency	Personal Identifiable Information (PII) was accessed but not exfiltrated	low classified information was accessed or exfiltrated.	Unclassified information was accessed or altered	The monetarized impact of fraud or theft of property can be absorbed by the entity	Time to recover is predictable
Medium	The entity has lost the ability to provide a critical service to a subset of users	Personal Identifiable Information (PII) was accessed and exfiltrated, and impacting less than 3% of the customer based	Medium classified information was accessed or exfiltrated.	Low business impacting information was accessed or altered	The monetarized impact of fraud or theft of property is little higher than what the entity can absorb	Time to recover is unpredictable, where additional resources and outside assistance are needed
High	The entity is no longer able to provide some critical services to any user	Personal Identifiable Information (PII) was accessed and exfiltrated, and impacting more than 3% of the customer based	Sensitive classified information was accessed or exfiltrated.	High business impacting information was accessed or altered	The monetarized impact of fraud or theft of property is more higher than what the entity can absorb	Recovery from the incident is not possible (e.g. PII data exfiltrated and posted publicly).

٣,٢ استمرارية العمل والتعافي من الكوارث

١. يجب إنشاء خطة لاستمرارية الأعمال والتعافي من الكوارث (DR/BCP) ومراجعتها مع المؤسسة (أصحاب المصلحة) للتأكد من كفايتها وفعاليتها.

٢. ينبغي للمؤسسة تحديد مسبقًا أهداف توافر واسترداد وظائف الأعمال بناءً على الأهمية والحساسية (أي تحليل تأثير الأعمال .((BIA) يجب أن تتضمن الأهداف على الأقل:

- هدف مستوى الخدمة السنوي(SLO).
- أقصى انقطاع مقبول(MAO) ، وهدف وقت الاسترداد(RTO) ، وهدف نقطة الاسترداد(RPO).

٣. يجب على المؤسسة إنشاء موقع / مواقع بديلة لضمان استمرارية الأعمال الحرجة.

٤. يجب أن يقع الموقع/ المواقع البديلة بمكان أمن ماديا ومفصول عن الموقع الرئيسي، ويكون بنفس مستوى ضوابط الأمن السيبراني المطبقة في الموقع الرئيسي.

٥. يجب إجراء اختبارات استمرارية العمل والتعافي من الكوارث على الأقل سنويا، وعند حدوث تغييرات كبيرة للأنظمة والخدمات الحرجة.

٦. إذا اعتمدت المؤسسة على مزود خدمة طرف ثالث لخدمة / خدمات أو أعمال حرجة، يجب على المؤسسة التأكد من أن مزود الخدمة (مقدمي الخدمات) يحافظ على خطة استمرارية عمل تلبي أهداف استرداد المؤسسة.

٤. مشاركة المعلومات

٤,١ إدارة المخاطر السيبرانية

١. ينبغي وضع اجراءات لإدارة استخبارات التهديدات السيبرانية والموافقة عليها وتنفيذها.

٢. ينبغي أن تتضمن إجراءات إدارة استخبارات التهديدات السيبرانية ما يلي:

١. التحكم بالوصول، والسجلات الأمنية للتطبيقات والبنية التحتية، وأنظمة (IDS, IPS)، وأدوات الأمن، ونظام إدارة معلومات الأمان والفعاليات(SIEM) ، ووظائف الدعم (على سبيل المثال، الشؤون القانونية، والتدقيق، ومكتب مساعدة تقنية المعلومات، وإدارة الاحتيال، وإدارة المخاطر، والامتثال).

٢. استعمال مصادر خارجية موثوقة وذات صلة، مثل ISIAC, Jo-FinCERT .

٣. مشاركة استخبارات التهديدات مع Jo-FinCERT من خلال منصة المشاركة.

قياس مستوى النضج الأمني

يجب قياس وتقييم مستوى نضج الأمن السيبراني لكل مؤسسة بناءً على مدى توافق حالة الأمان الحالية مع المجالات التي يغطيها هذا الدليل. يتكون نموذج النضج من ستة مستويات، ويركز على الأشخاص والسياسات والإجراءات المعمول بها، بالإضافة إلى الحلول التقنية الموجودة.

Maturity Level	Definition and Criteria	Explanation
0	• No documentation • There is no awareness or attention for certain cyber security control.	• Cyber security controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such cyber security controls.
1	• Cyber security controls are not or partially defined. • Cyber security controls are performed in an inconsistent way. • Cyber security controls are not fully defined.	• Cyber security control design and execution varies by department or owner. • Cyber security control design may only partially mitigate the identified risk and execution may be inconsistent.
2	• The execution of the cyber security control is based on an informal and unwritten, though standardized, practice.	• Repeatable cyber security controls are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideration for a structured review or testing of a control.
3	• Cyber security controls are defined, approved and implemented in a structured and formalized way. • The implementation of cyber security controls can be demonstrated.	• Cyber security policies, standards and procedures are established. • Compliance with cyber security documentation i.e., policies, standards and procedures are monitored, • key performance indicators are defined, monitored and reported to evaluate the implementation.
4	• The effectiveness of the cyber security controls is periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of cyber security controls are measured and periodically evaluated. • key risk indicators and trend reporting are used to determine the effectiveness of the cyber security controls. • Results of measurement and evaluation are used to identify opportunities for improvement of the cyber security controls.
5	• Cyber security controls are subject to a continuous improvement plan.	• The enterprise-wide cyber security program focuses on continuous compliance, effectiveness and improvement of the cyber security controls. • Cyber security controls are integrated with enterprise risk management framework and practices. • Performance of cyber security controls are evaluated using peer and sector data.

سجل التعديلات

الاصدار	التاريخ	السبب
V 1.0	تموز ٢٠٢٤	الإصدار الاول