هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار الأمن السيبراني للبيانات

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <1.0>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بحماية البيانات الخاصة بـ<اسم الجهة>. ويهدف هذا المعيار إلى تحديد مجموعة من ضوابط الأمن السيبراني للتأكد من حماية البيانات الخاصة بالأصول المعلوماتية الخاصة بـ<اسم الجهة>.

تمت مواءمة هذا المعيار مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وضوابط الأمن السيبراني للبيانات (DCC-1:2022) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

ينطبق هذا المعيار على جميع الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان توفير الوصول المنطقي لأصول البيانات بهدف منع الوصول غير المصرح به والسماح فقط بوصول المصرح لهم.
المخاطر المحتملة	قد تتسبب الإدارة غير السليمة للبيانات في وصول الأشخاص غير المصرح لهم إلى البيانات الحساسة، مما قد يؤدي إلى تلف البيانات أو فقدانها أو سرقتها.
الإجراءات المطلوبة	
1-1	أن تستند صلاحيات المستخدمين إلى مبادئ ضوابط الهويات وصلاحيات الوصول، والتي تتمثل بما يلي: • الحاجة إلى المعرفة • الحاجة إلى الاستخدام • الحد الأدنى من الصلاحيات • فصل المهام.
2-1	ضبط جميع عمليات الوصول إلى البيانات باستخدام آليات التعرّف والتحقق. ويجب أن يستوفي الضابط الخاص بالوصول ما يلي: 1. تخصيص الصلاحيات للأفراد بناءً على تصنيفهم الوظيفي وإداراتهم. 2. تقييد الصلاحيات للحد الأدنى المطلوب للأفراد أو الخدمات لأداء وظائفهم. 3. حجب جميع أشكال الوصول غير المصرح به. 4. إزالة كافة أشكال الوصول غير المطلوب إلى النظام.

	5. مراجعة هويات المستخدمين وحقوق الوصول دوريًا.
3-1	تعيين حسابات الأجهزة والخدمات والتطبيقات لصاحب الحساب، ويجب ألا يستخدمها الأفراد للوصول إلى الأجهزة والخدمات والتطبيقات ذات العلاقة. ويجب إدارة هذه الحسابات وكلمات المرور المرتبطة بها من خلال أداة إدارة الحسابات ذات الصلاحيات في الجهة.
4-1	مراجعة جميع الحسابات عند إجراء تغييرات في دور المستخدم سنويًا على الأقل لحسابات المستخدمين أو مجموعات المستخدمين التي تتعامل مع البيانات العامة والسرية. أما الحسابات والخدمات ذات الصلاحيات، أو الحسابات التي تتعامل مع مستويات البيانات السرية والسرية للغاية، فيجب مراجعتها كل 6 أشهر.
2	خصوصية البيانات والمعلومات (Data and Information Privacy)
الهدف	ضمان تطبيق متطلبات خصوصية البيانات والمعلومات.
المخاطر المحتملة	قد تؤدي عدم كفاية أو غياب إجراءات خصوصية البيانات إلى الوصول غير المصرح به إلى البيانات السرية، مما قد يترتب عليه تسرب البيانات أو فقدانها.
المعايير المطلوبة	
1-2	أن تراعي <اسم الجهة> تدابير الخصوصية في مراحل التصميم الأولية وطوال عملية التطوير الكاملة للأنظمة أو التطبيقات أو قواعد البيانات أو المنتجات أو العمليات أو الخدمات الجديدة التي تتضمن معالجة معلومات التعريف الشخصية (PII).
2-2	تضمين مبدأ "الخصوصية حسب التصميم" في تصميم ومعمارية أنظمة تقنية المعلومات التي تعالج معلومات التعريف الشخصية (PII) للتأكد من أن التغييرات الحالية أو الجديدة أو التغييرات التي تطرأ على الأنظمة التي تجمع معلومات التعريف الشخصية (PII) أو تعالجها تستوفي المتطلبات.
3-2	عند الحاجة، يجب أن تطبق <اسم الجهة> تقنيات إخفاء هوية البيانات لتلبية متطلبات الخصوصية وفقًا لمبدأ "الخصوصية حسب التصميم".
4-2	أن تلائم إعدادات النظام الافتراضية تدابير الخصوصية على أفضل وجه (مبدأ الحدّ الأدنى من البيانات)، إذا تضمن النظام أو الخدمة اختيارات لموضوعات البيانات حول مقدار معلومات التعريف الشخصية (PII) التي تتم مشاركتها.
5-2	أن تطبق <اسم الجهة> التدابير الفنية والتنظيمية الملائمة لضمان معالجة معلومات التعريف الشخصية (PII) الضرورية فقط بشكل افتراضي.

6-2	أن تتواءم ضوابط الأمن الموضحة في هذه الوثيقة مع متطلبات الخصوصية. ويجب أن تمتلك <اسم الجهة> سياسة/ معيار/ متطلبات منفصلة معنية بخصوصية البيانات.
3	تشفير البيانات المنقولة (Data in Transit Encryption)
الهدف	تحديد متطلبات التشفير لبيانات معينة بناءً على تصنيفها، ونتائج تقييم مخاطرها، وحالة استخدامها.
المخاطر المحتملة	قد يؤدي عدم التشفير أو التشفير غير الوافي للبيانات إلى إرسال بيانات سرية -عن قصد أو بدون قصد- إلى شخص لا يمتلك حق الوصول إليها أو مشاركتها بشكل علني.
المعايير المطلوبة	
1-3	أن تستخدم <اسم الجهة> التشفير على جميع بيانات الأنظمة الحساسة أثناء نقلها (البيانات المنقولة)، باستخدام وسائل وخوارزميات ومفاتيح تشفير محدثة وآمنة وفقًا للمعايير الوطنية للتشفير ذات العلاقة.
2-3	استخدام التشفير في حال نقل معلومات التعريف الشخصية (PII) الإلكترونية (على سبيل المثال لا الحصر، من خلال البريد الإلكتروني، وبروتوكول النقل الآمن (SSH)، وخدمة الرسائل الفورية، والفاكس الإلكتروني، والاتصالات الهاتفية عبر الإنترنت (VOIP).
3-3	استخدام التشفير (نقطة الوصول المحمية للشبكة اللاسلكية (WPA) أو بروتوكول تشفير ذي مستوى أعلى) في حال الاتصال بالشبكة (الشبكات) الداخلية عبر شبكة لا سلكية.
4-3	استخدام التشفير في حالة الوصول عن بُعد إلى الشبكة (الشبكات) الداخلية أو الأجهزة الموصولة بشبكة مشتركة في <اسم الجهة> (مثل الإنترنت) أو شخصية (مثل تقنية بلوتوث Bluetooth والاتصال قريب المدى NFC). ولا ينطبق هذا على الوصول عن بُعد عبر نقطة مُدارة من <اسم الجهة> إلى نقطة اتصال مخصصة.
5-3	استخدام التشفير إذا تم نقل البيانات باستخدام موقع ويب عام و/أو خدمات ويب خاصة بـ<اسم الجهة>، ويجب استخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) بدلاً من بروتوكول نقل النص التشعبي (HTTP) حيثما كان ذلك ممكنًا من الناحية الفنية. يجب أن تستخدم مواقع الويب العامة آلية أمن النقل الصارم ببروتوكول نقل النص التشعبي (HTTP)، وتعيد توجيه طلبات بروتوكول نقل النص التشعبي (HTTP) تلقائيًا إلى مواقع الويب التي تستخدم بروتوكول نقل النص التشعبي الآمن (HTTPS) حيثما كان ذلك ممكنًا من الناحية الفنية.
6-3	أن تستخدم <اسم الجهة> طرق التشفير المناسبة للبيانات أثناء النقل، بما في ذلك على سبيل المثال لا الحصر، أمان طبقة النقل 1.2 (TLS) أو أحدث، وبروتوكول النقل الآمن (SSHv2) أو أحدث، وبروتوكول الوصول المحمي للشبكات اللاسلكية (WPA)

	الإصدار 2 أو أحدث (مع تعطيل الإعدادات اللاسلكية المحمية)، والشبكات الخاصة الافتراضية (VPN) على النحو المنصوص عليه من قبل الهيئة الوطنية للأمن السيبراني في المعايير الوطنية للتشفير (NCS-1: 2020). يجب ضبط إعدادات المكونات لدعم أقوى حزم التشفير الممكنة.
4	تشفير البيانات المخزّنة (Encryption in Data at rest)
الهدف	التأكد من تشفير البيانات بناءً على تصنيفها، ونتائج تقييم مخاطرها، وحالة استخدامها.
المخاطر المحتملة	قد يؤدي عدم تشفير البيانات أو تشفيرها بشكل غير صحيح إلى تسرب البيانات، والوصول غير المصرح به إليها، والكشف عن المعلومات السرية أمام العلن.
المعايير المطلوبة	
1-4	أن تقوم <اسم الجهة> بتشفير جميع بيانات الأنظمة الحساسة أثناء التخزين (البيانات المخزّنة) على مستوى الملفات أو قواعد البيانات او عمود مخصص في قاعدة البيانات، باستخدام طرق تشفير وخوارزميات ومفاتيح تشفير محدثة وآمنة وفقًا للمعايير الوطنية للتشفير ذات العلاقة.
2-4	استخدام التشفير في الأنظمة الواردة أدناه: • الحواسيب المكتبية التي تصل إلى معلومات التعريف الشخصية (PII) أو المعلومات الحساسة. • مخازن البيانات (بما في ذلك، على سبيل المثال لا الحصر، قواعد البيانات ومشاركات الملفات) التي تحتوي على معلومات التعريف الشخصية (PII) والمعلومات الحساسة. • جميع الأجهزة المحمولة، بغض النظر عمّا إذا كانت صادرة عن <اسم الجهة> أو جهة خارجية، والتي تصل إلى أو تحتوي على أي معلومات تخص <اسم الجهة> أو معلومات حساسة. • أجهزة التخزين المحمولة التي تحتوي على أي معلومات تخص <اسم الجهة> أو معلومات حساسة. • معلومات التعريف الشخصية (PII) المنقولة أو المخزّنة خارج مرافق <اسم الجهة> أو المعلومات الحساسة.
3-4	استخدام تشفير القرص الكامل لجميع أجهزة الحاسوب المحمولة التي تصل إلى معلومات <اسم الجهة> أو تحتوي عليها. ويجب أن تستخدم أدوات تشفير القرص الكامل إما مصادقة ما قبل التشغيل التي تستخدم وحدة النظام الأساسي الموثوقة (TPM) للجهاز، أو الواجهة الموحدة للبرنامج الثابت الممتد (UEFI).

4-4	إيقاف تشغيل أجهزة الحاسوب المحمولة وأيضًا أجهزة الكمبيوتر المحمولة التابعة لجهات خارجية التي تصل إلى أو تحتوي على معلومات التعريف الشخصية (PII) أو المعلومات الحساسة عندما تكون خارج مرافق <اسم الجهة>، (على سبيل المثال، إيقاف التشغيل أو وضع السكون) عندما لا تكون مستخدمة، للحدّ من الهجمات على مفاتيح التشفير.
5-4	أن يكون لدى <اسم الجهة> عملية مطبقة للتأكد من أن الأجهزة والوسائط المستخدمة قد تم تشفيرها بنجاح باستخدام آلية واحدة على الأقل مما يلي (مرتبة بحسب الآلية المفضلة): • إنفاذ السياسات آليًا • نظام جرد آلي • حفظ السجلات يدويًا
5	التخلص من الوسائط (Media Disposal)
الهدف	قد تتطلب أنظمة المعلومات التي تسجل المعلومات وتعالجها وتخزنها باستخدام مجموعة متنوعة من الوسائط، بما في ذلك الورق، إجراءات خاصة للتخلص منها من أجل التخفيف من حدة مخاطر الوصول غير المصرح به إلى البيانات ولضمان سريتها.
المخاطر المحتملة	يؤدي عدم كفاية أو غياب ممارسات تدقيق البيانات إلى تعريض <اسم الجهة> لمخاطر اختراق البيانات والكشف عنها والوصول غير المصرح به إلى المعلومات السرية.
المعايير المطلوبة	
1-5	أن تقوم <اسم الجهة> بإزالة البيانات بالكتابة فوقها كوسيلة للتطهير، وذلك في حال إعادة استخدام الوسائط وبقائها في حيازة <اسم الجهة> من أجل منع استرداد المعلومات عن طريق أدوات استرداد البيانات أو القرص أو الملفات.
2-5	أن تستخدم <اسم الجهة> عملية تنظف البيانات كوسيلة لتطهيرها إذا كان سيتم إعادة استخدام الوسائط ولن تكون في حيازة <اسم الجهة>، من أجل حماية سرية المعلومات ضد أي هجوم من خلال إزالة المغنطة أو المسح الآمن.
3-5	على <اسم الجهة> إتلاف البيانات ماديًا كوسيلة لتطهيرها، إذا كان لن يتم إعادة استخدام الوسائط مطلقًا من أجل إتلاف الوسائط بشكل كامل.
4-5	توثيق النقاط التالية: • وقت إتلاف البيانات • الشخص الذي قام بإتلاف البيانات

	• يجب تخزين الأدلة وفقًا لفترة الاحتفاظ بها المتفق عليها.
5-5	أن تقرر <اسم الجهة> عملية التطهير التي سيتم استخدامها، بناءً على التصنيف ومستوى السرية المرتبط بالمعلومات، وليس بناءً على نوع الوسائط. ويجب أن يوافق مالك البيانات على نوع التطهير.
6	ضوابط مكافحة المخاطر المالية ومخاطر المساس بالسمعة (Controls Against Financial and Reputational Risks)
الهدف	ضمان سرية وسلامة وتوافر بيانات <اسم الجهة> ومعلوماتها وفقًا للسياسات والإجراءات التنظيمية والقوانين واللوائح ذات الصلة، من أجل تجنب الإضرار المالي والمساس بالسمعة.
المخاطر المحتملة	يمكن أن تتسبب الوثائق المسروقة والمدعى أنها "أصلية" (بدون علامات مائية)، وتسرب البيانات، وسوء التعامل مع البيانات الحساسة والشخصية في وقوع مخاطر مالية ومخاطر المساس بالسمعة.
المعايير المطلوبة	
1-6	أن تستخدم <اسم الجهة> خاصية العلامات المائية لترميز الوثيقة بأكملها عند إعدادها أو تخزينها وطباعتها أو عرضها على الشاشة، مع التأكد من احتواء كل نسخة من الوثيقة على رقم يمكن تتبعه.
2-6	أن تستخدم <اسم الجهة> تقنيات منع فقدان البيانات.
3-6	أن تحظر <اسم الجهة> استخدام البيانات الحساسة والشخصية في أي بيئة أخرى غير بيئة الإنتاج. لا يُمنح الاستثناء إلا بعد تطبيق ضوابط صارمة لحماية بيانات <اسم الجهة> باستخدام التقنيات المناسبة، مثل: تقنيع البيانات أو تخليط البيانات.
7	المعايير الأخرى (Other Standards)
الهدف	يجب نشر حماية البيانات بشكل آمن واستخدامها بشكل ملائم عند الحاجة.
المخاطر المحتملة	يزيد الإخفاق في تلبية جميع معايير ومتطلبات الأمن من المخاطر الأمنية المتعلقة بحماية البيانات.
المعايير المطلوبة	

1-7	تطبيق المعايير التالية فيما يتعلق بحماية البيانات: 1. نموذج معيار التشفير 2. نموذج معيار أمن الشبكات 3. نموذج معيار الأمن المادي 4. نموذج معيار إدارة النسخ الاحتياطية والاسترجاع

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو عند حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.