هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. والبنود الملونة باللون الأخضر هي أمثلة يجب حذفها. ويجب حذف التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار النسخ الاحتياطية

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.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجعك اضغط هنا لإضافة نص

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.

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

قائمة المحتويات

الغرض 4
النطاق 4
المعايير 4
الأدوار والمسؤوليات 10
التحديث والمراجعة 10
الالتزام بالمعيار 10

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بالنسخ الاحتياطية لجميع المعلومات والأصول التقنية في <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية وذلك لتحقيق الأهداف الرئيسية للحماية وهي: سرية المعلومات، وسلامة أنظمة المعلومات، وتوافرها.

تمت موائمة هذا المعيار مع سياسة النسخ الاحتياطية الخاصة ب<اسم الجهة> والضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية (مثل: الأنظمة والبيانات والمعلومات) الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	عمليات إدارة النسخ الاحتياطية (Data backup and recovery processes)
الهدف	تحديد آلية النسخ الاحتياطي لكل نظام من أنظمة تقنية المعلومات الذي تستخدمه <اسم الجهة>.
المخاطر المحتملة	قد يؤدي عدم وجود نسخ احتياطية إلى فقدان البيانات والمعلومات في حالة حدوث خطأ في النظام أو إيقاف التشغيل غير المخطط له أو حدوث انتهاك أمني، ومن الممكن أن يؤدي عدم وجود عملية نسخ احتياطي للنظام إلى عدم استعادة نظام تقنية المعلومات إلى نقطة زمنية محددة وحالة معروفة، مما يؤثر سلبًا على العمليات التشغيلية ويُعرض <اسم الجهة> لانتهاك الالتزامات التشريعية أو التنظيمية.
الإجراءات المطلوبة	
1-1	تحديد عمليات وإجراءات النسخ الاحتياطي للبيانات لجميع أنظمة تقنية المعلومات، بما في ذلك الحوسبة السحابية والوصول عن بُعد والعمل عن بُعد والأنظمة الحساسة، والتي تستخدمها <اسم الجهة> بما في ذلك الأنظمة المستضافة لدى طرف خارجي وفقًا لمعيار تصنيف البيانات الخاص ب <اسم الجهة>.
2-1	إجراء تقييم التأثير على الاعمال من قبل مالك النظام (المسؤول عن النظام) ووحدة الاعمال لتحديد وتيرة ونوع النسخ الاحتياطي المطلوب.

اختر التصنيف

الإصدار <1.0>

3-1	يجب تحديد وقت التعافي وأهداف نقطة التعافي من قبل مسؤول ومستخدمي النظام حسب نتائج تقييم التأثير على الأعمال.
4-1	يتولى مالك النظام مسؤولية تحديد عمليات وإجراءات النسخ الاحتياطي للبيانات للأنظمة التي يتولون مسؤوليتها. يجب أن تتضمن عمليات وإجراءات النسخ الاحتياطي للبيانات المتطلبات التالية كحد أدنى: أ) أسماء الموظفين المصرح لهم الذين يمكنهم الوصول إلى النسخ الاحتياطية ووسائط النسخ الاحتياطي ب) الإجراءات التشغيلية ج) إجراءات تسجيل النسخ الاحتياطي د) وتيرة النسخ الاحتياطي (مثل: يوميًا أو أسبوعيًا أو شهريًا) لتحقيق تحليل التأثير على الأعمال ووقت التعافي وأهداف نقاط التعافي ه) سجل من ملفات النظام والتطبيقات المطلوب إعداد نسخ احتياطية لها (مثل: نظام التشغيل، أو ملفات التطبيق القابلة للتنفيذ) و) سجل بالبيانات والمعلومات المطلوب إعداد نسخ احتياطية لها (مثل: البيانات الثابتة أو ملفات العملاء أو سجلات المعاملات) ز) نوع النسخ الاحتياطي (مثل: إضافية أو كاملة) ح) الوسيط (مثل: شريط، قرص، سحابة) ط) التخزين (مثل: في الموقع، خارج الموقع، التعاقب(Rotating)) ي) سجلات النسخ الاحتياطي (مثل: التاريخ، وسائط وموقع التخزين) ك) فترات الاحتفاظ بالنسخ الاحتياطية ل) إجراءات مراقبة السجل ومعالجة الأخطاء (مثل: إعادة تشغيل نسخة احتياطية لم يتم تشغيلها بنجاح، وذلك ضمن إطار زمني محدد) م) إجراءات الاختبار (مثل: التحقق من النسخ الاحتياطي) ن) إجراءات استعادة البيانات وجداولها الزمنية س) متطلبات تشفير البيانات
5-1	استخدام الوسائط الشخصية القابلة للإزالة من أي نوع (مثل: أجهزة التخزين الخارجية USB) كوسيلة احتياطية يجب حظرها.
2	حماية وسائط النسخ الاحتياطي Protection of backup media
الهدف	حماية وسائط النسخ الاحتياطي.

المخاطر المحتملة	يمكن أن تتعرض وسائط النسخ الاحتياطي غير المحمية أو التي يتم تخزينها أو التعامل معها بشكل غير سليم للتلف أو الفقدان أو السرقة أو انتهاك أمني. وقد يؤثر تلف وسائط النسخ الاحتياطي سلبًا على استعادة نظام تقنية المعلومات أو البيانات والمعلومات المرتبطة به، وقد يعني فقدان الوسائط أو سرقتها عدم إمكانية تنفيذ عملية استعادة البيانات والمعلومات، واعتمادًا على البيانات والمعلومات المخزنة على وسائط النسخ الاحتياطي، قد يُعرّض <اسم الجهة> للتحقيقات والعقوبات القانونية أو التنظيمية.
الإجراءات المطلوبة	
1-2	تخزين وسائط النسخ الاحتياطي في مكان آمن ومقاوم للحريق عند عدم استخدامها وحمايتها من المخاطر البيئية (مثل: الفيضانات).
2-2	يجب ان تحفظ وسائط النسخ الاحتياطي بشكل منفصل عن الوسائط المباشرة (أي وسائط البث الحي) باستخدام وسائط التخزين عبر الإنترنت (مثل شبكة نسخ احتياطية مخصصة أو التقسيم المادي و/أو المنطقي للشبكة).
3-2	يكون الوصول إلى وسائط النسخ الاحتياطي مقتصرًا على الموظفين المصرح لهم ممن لديهم احتياجات عمل مناسبة.
4-2	تحديد وتوثيق الموظفين المصرح لهم بالوصول إلى وسائط النسخ الاحتياطي ومبررات الوصول.
5-2	نقل وسائط النسخ الاحتياطي المادية (مثل: الأقراص والأشرطة وغيرها) إلى موقع آمن ومعتمد لدى <اسم الجهة> مباشرة بعد الإنشاء أو الاستخدام.
6-2	نقل وسائط النسخ الاحتياطي المادية من مواقع خارجية وإليها باستخدام وسيلة نقل آمنة (مثل البريد السريع المخصص وصندوق الأمن).
7-2	تقتصر القدرة على استعادة وسائط النسخ الاحتياطي من خارج الموقع على الموظفين المصرح لهم.
8-2	تسجيل جميع طلبات استعادة البيانات الاحتياطية في موقع مركزي (أي سجل طلب النسخ الاحتياطي). يحتوي سجل طلبات النسخ الاحتياطي على الأقل على ما يلي: أ) وقت تقديم الطلب ب) هوية مقدم الطلب ج) سبب تقديم الطلب

	د) النسخ الاحتياطي المطلوب للنظام ه) هوية الشخص الذي يوافق على الطلب أو يرفضه (يجب أن يكون الرفض مصحوبًا بمبررات رفض الطلب).
9-2	تخزين سجل طلب النسخ الاحتياطي بطريقة آمنة، مع قصر الوصول على الموظفين المصرح لهم، باستخدام ضوابط الوصول المادي والمنطقي.
10-2	مراجعة وحصر جميع وسائط النسخ الاحتياطي المادية مرة واحدة سنويًا على الأقل.
11-2	استبدال وسائط النسخ الاحتياطي المادية قبل أن تصل إلى نهاية عمرها الافتراضي المعلن عنه من الشركة المصنعة.
3	اختبار النسخ الاحتياطي واستعادة النسخ الاحتياطية (Backup test and restore)
الهدف	اختبار بيانات النسخ الاحتياطي للتأكد من اكتمالها وإمكانية استعادتها.
المخاطر المحتملة	عدم القدرة على تحديد ضرر أو تلف وسائط النسخ الاحتياطي وفساد البيانات والمعلومات المخزنة على وسائط النسخ الاحتياطي، وقد يؤثر ذلك سلبًا على استعادة نظام تقنية المعلومات أو البيانات والمعلومات المرتبطة به.
الإجراءات المطلوبة	
1-3	اختبار جميع النسخ الاحتياطية والتحقق منها بعد تشغيلها لضمان نجاح إجراء النسخ الاحتياطي. على سبيل المثال، التحقق من حجم الملف باستخدام خاصية إجمالي حقول الملف أو تطبيق طرق أخرى للتحقق.
2-3	إجراء اختبار استعادة النسخ الاحتياطية بشكل دوري وفقًا لما يلي: • مرة واحدة سنويًا لجميع النسخ الاحتياطية. • مرة واحدة كل ثلاثة أشهر للنسخ الاحتياطية للأنظمة الحساسة. • مرة واحدة كل ستة أشهر للنسخ الاحتياطية لأنظمة العمل عن بعد.
3-3	مراجعة اختبار استعادة النسخ الاحتياطية للتحقق مما إذا كان قد حدث خلال فترات زمنية محددة أو ضمن نطاقه.
4	حماية النسخ الاحتياطية الإلكترونية (Protection of online backups)
الهدف	حماية النسخ الاحتياطية الإلكترونية.

المخاطر المحتملة	قد تؤدي عدم حماية النسخ الاحتياطية الإلكترونية أو عدم حمايتها بشكل مناسب إلى الوصول غير المصرح به أو التعديل أو الحذف للبيانات والمعلومات الاحتياطية. وقد يؤثر ذلك سلبًا على استعادة نظام تقنية المعلومات أو البيانات والمعلومات المرتبطة به.
الإجراءات المطلوبة	
1-4	تقييد الوصول المادي والمنطقي إلى النسخ الاحتياطية الإلكترونية (مثل: وسائط التخزين المتصلة بالشبكة أو شبكات منطقة التخزين أو السحابة) وتحديده بالموظفين المصرح لهم.
2-4	تشفير التخزين الاحتياطي، سواء عبر الإنترنت أو خارجه، إما عن طريق تشفير ملفات النسخ الاحتياطي الفردية و/أو حجم التخزين.
3-4	تشفير ملفات النسخ الاحتياطي عند نقلها أو مشاركتها عبر الشبكات والمواقع المادية.
5	متطلبات النسخ الاحتياطي والاحتفاظ بالبيانات (Backup and data retention (requirements
الهدف	الاحتفاظ بالبيانات والنسخ الاحتياطية وإدارتها وفقًا للمتطلبات التشريعية والتنظيمية والسياسات.
المخاطر المحتملة	قد يؤدي الاحتفاظ بالبيانات والمعلومات لفترات زمنية غير صحيحة إلى مخالفة التشريعات والأنظمة والسياسات.
الإجراءات المطلوبة	
1-5	الاحتفاظ بالبيانات والنسخ الاحتياطية لفترات زمنية محددة كما هو مطلوب بموجب التشريعات واللوائح وسياسة الأعمال بالمواءمة مع معيار تصنيف الأصول وسياسة حماية البيانات في <اسم الجهة>.
2-5	مراجعة البيانات والنسخ الاحتياطية مرة واحدة سنويًا على الأقل لتحديد ما إذا تم تجاوز فترات الاحتفاظ المحددة، كما يجب توثيق نتائج المراجعة.
3-5	مراجعة البيانات والنسخ الاحتياطية التي تحتوي على معلومات شخصية مرة واحدة على الأقل كل ستة أشهر لتحديد ما إذا تم تجاوز فترات الاحتفاظ المحددة، كما يجب توثيق نتائج المراجعة.
4-5	يجب على مالك النظام تحديد عملية حذف البيانات والنسخ الاحتياطية عند الطلب وفقًا سياسة حماية البيانات المتبعة لدى <اسم الجهة>. يجب أن تتضمن العملية المتطلبات التالية كحد أدنى:

	أ) كيفية تقديم طلب حذف البيانات أو النسخ الاحتياطي (على سبيل المثال عبر البريد الإلكتروني) ب) مستلمو طلب الحذف (مثل: مالك النظام، ممثل <إدارة الشؤون القانونية>، مسؤول حماية البيانات) ج) الشخص المؤهل لطلب حذف البيانات/النسخ الاحتياطي (مثلاً موظفي <اسم الجهة>) د) من يمكنه التصريح بإصدار حذف البيانات أو النسخ الاحتياطي (مثل: <إدارة الشؤون القانونية>) ه) من يمكنه حذف البيانات أو النسخ الاحتياطية أو إنشاء نشاط حذف تلقائي (مثل: <إدارة تقنية المعلومات>) و) المدة التي يستغرقها طلب حذف البيانات أو النسخ الاحتياطي ز) ما الآلية التي يتم استخدامها لإثبات حدوث الحذف بشكل دائم ح) كيفية إتلاف مفاتيح التشفير (في حال استخدامها) ط) كيفية تسجيل الطلب والحذف بطريقة آمنة.
5-5	يجب تسجيل جميع طلبات حذف البيانات الاحتياطية في موقع مركزي (سجل حذف النسخ الاحتياطي). يحتوي سجل حذف النسخ الاحتياطي على الأقل على ما يلي: أ) وقت طلب الحذف ب) هوية مقدم طلب الحذف ج) أسباب الحاجة إلى الحذف د) النسخة الاحتياطية للنظام المطلوب حذفها ه) تاريخ ووقت الحذف الفعلي و) اسم الشخص/الموظف الذي قام بحذفه ز) هوية الشخص الذي يوافق على الطلب أو يرفضه (يجب أن يكون الرفض مصحوبًا بمبررات رفض الطلب).
6-5	تخزين سجل طلب النسخ الاحتياطي بطريقة آمنة، مع قصر الوصول إليه على الموظفين المصرح لهم، مع مراعاة ضوابط الوصول المادي والمنطقي.
7-5	يكون إتلاف وسائط النسخ الاحتياطي المادي متوافقًا مع معيار تصنيف الأصول ومعايير الأمن المادي المتبعة لدى <اسم الجهة>.

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 في حال 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 جميع 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>.