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 أمن قواعد البيانات

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.

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 <١,٠>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بأنظمة إدارة قواعد البيانات (Database Management System "DBMS") الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية الناتجة من التهديدات الداخلية والخارجية.

تمت موائمة هذا المعيار مع سياسة أمن قواعد البيانات والضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول التقنية والمعلوماتية (شاملة أنظمة إدارة قواعد البيانات) الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	مراجعة الإعدادات والتحصين (Secure Hardening Configuration)
الهدف	تحديد متطلبات حماية نظام إدارة قواعد البيانات (DBMS) الأساسية لضمان تصميم نظام إدارة قواعد البيانات (DBMS) وإعداده وتشغيله بطريقة آمنة.
المخاطر المحتملة	تعتبر الأخطاء في إعداد نظام إدارة قواعد البيانات (DBMS) والتصاميم الضعيفة من أبرز الأسباب التي تؤدي إلى وجود ثغرات أمنية يمكن استغلالها لتهديد سرية بيانات <اسم الجهة> وسلامتها وتوافرها.
الإجراءات المطلوبة	
١-١	أن تكون طريقة التسمية بين خوادم نظام إدارة قواعد البيانات (DBMS) في بيئة الإنتاج والبيئات الأخرى مختلفة ليتم تمييزها.
١-٢	تخصيص خوادم نظام إدارة قواعد البيانات (DBMS) وعدم استضافة أي وظائف أخرى مثل "مستوى الويب أو التطبيق" (Web or Application Tier) أو "خدمات النطاق" (Domain Services).
١-٣	إعادة تسمية جميع قواعد البيانات الافتراضية.
١-٤	استخدام الإجراءات المخزّنة المتوفّرة للتطبيق فقط لإجراء التعاملات أو الاستعلامات من قواعد البيانات.
١-٥	عدم تحديد روابط خوادم نظام إدارة قواعد البيانات (DBMS) (مثل إنشاء اتصالات أو واجهات) بين أنظمة إدارة قواعد البيانات (DBMS) الإنتاجية وغير الإنتاجية.

١-٦	استخدام خاصية التحقّق من صحة وسلامة البيانات المدخلة لضمان سلامة البيانات المخزّنة.
١-٧	تقييد حقول قاعدة البيانات بمجالات محدّدة من المدخلات واستخدام المدخلات الثنائية أو طرق التحقّق الأخرى من المدخلات والاستعلامات، مثل التحقّق من الحدود (Boundary Checking)، أو التحقق من المحتوى وتصفية روابط مواقع الإنترنت (Content Inspection/URL Filtering)، للحد من العمليات مثل: • البيانات المفقودة أو غير المكتملة أو كلاهما. • القيم خارج النطاق. • البيانات غير المصرّح بها أو غير المتسقة. • الأحرف والأرقام غير الصحيحة في حقول البيانات. • تجاوز حدود قيمة الحد الأعلى أو الأدنى للتاريخ.
١-٨	تقييد الوصول إلى ملفات إعدادات نظام إدارة قواعد البيانات (DBMS) والشفرة المصدرية (Source Code) للتطبيقات والبرمجيات المخزّنة في قاعدة البيانات ومراقبتها.
١-٩	حفظ قائمة جرد دقيقة لكافة قواعد البيانات ومحتوياتها وتحديثها دوريًا.
١-١٠	ترميز البيانات المخزّنة في قواعد البيانات باستخدام أنواع ترميز آمنة محدّدة مسبقًا وفقًا للسياسات والإجراءات والضوابط ذات العلاقة في <اسم الجهة>.
٢	سجلات التدقيق (Audit Logs)
الهدف	إصدار سجلات نظام إدارة قواعد البيانات (DBMS) للأحداث الأمنية الرئيسية والحرجة وتسجيلها وتأمينها على نظام إدارة قواعد البيانات (DBMS) للمساعدة في التحقيق والتتبع والتحقّق في المستقبل.
المخاطر المحتملة	تَحُد سجلات التدقيق غير الوافية من قدرة <اسم الجهة> على كشف الانتهاكات والحوادث والمسائل الأمنية وتتبُّعِها في نظام إدارة قواعد البيانات (DBMS)، وتُقيّد إمكانية تحديد سبب الانتهاكات الأمنية. كما يؤدي عدم تأمين سجلات التدقيق على نظام إدارة قواعد البيانات (DBMS) بالشكل المناسب إلى العبث بالسجلات مما يؤثّر في سلامتها.
الإجراءات المطلوبة	
٢-١	مزامنة أوقات جميع أنظمة إدارة قواعد البيانات (DBMS) مركزيًا مع خادم بروتوكول وقت الشبكة (Network Time Protocol).
٢-٢	إرفاق السجلات بسجلات نظام التشغيل أو أن تكون مستقلّة ضمن نظام إدارة قواعد البيانات (DBMS).

٢-٣	إصدار سجلات التدقيق التي تحتوي على معلومات تفصيلية لتحديد هوية أي مستخدم أو عملية ذات علاقة بالحدث المعني.
٢-٤	تسجيل نشاطات نظام إدارة قواعد البيانات (DBMS) التالية بحدّ أدنى، وزمن وقوعها (DBMS) تسجيل نشاطات نظام إدارة قواعد البيانات: • جميع حالات الإنذار أو الأخطاء التي ظهرت في النظام. • التشغيل. • الإغلاق. • إنشاء أو تعديل أو حذف (استبعاد) قواعد البيانات وأي هيكل تخزين لقواعد البيانات وأي جداول لقواعد البيانات وفهارس وحسابات ومصادر. • تفعيل وظيفة التدقيق وإلغاء تفعيلها. • منح الامتيازات والصلاحيات وإلغائها على مستوى نظام إدارة قواعد البيانات (DBMS). • أي إجراء يُسبِّب ظهور رسالة خطأ لعدم وجود المصدر الذي يتم البحث عنه. • أي إجراء يؤدي إلى إعادة تسمية مصدر على نظام إدارة قواعد البيانات (DBMS). • أي إجراء يمنح أو يلغي امتيازات وصلاحيات استخدام المصدر من دور أو حساب نظام إدارة قواعد البيانات (DBMS). • كافة التعديلات على دليل البيانات أو إعدادات نظام إدارة قواعد البيانات (DBMS). • تدقيق جميع حالات فشل الاتصال بنظام إدارة قواعد البيانات (DBMS) حيثما أمكن، ويضمن مدير قاعدة البيانات تدقيق محاولات الاتصال الناجحة وغير الناجحة. • تحديد عدد وإرسال التنبيه لمحاولات تسجيل الدخول غير الناجحة، وأقفال كلمات المرور. • محاولات إضافة أو تعديل أو حذف الامتيازات والصلاحيات أو التصاريح. • حذف فئات من المعلومات (مثل مستويات التصنيف أو مستويات الأمن). • أمر غير عادي (أمر يطلب أمرًا آخر وهكذا). • إلغاء تفعيل سجلات نظام إدارة قواعد البيانات (DBMS) أو تعديلها.
٢-٥	توفير تنبيه فوري ومباشر من أجل تقديم الدعم المناسب للأشخاص في جميع أحداث فشل التدقيق التي تتطلّب إجراءات مباشرة.
٢-٦	حماية خصائص التدقيق في نظام إدارة قواعد البيانات (DBMS) من عمليات الحذف غير المصرّح بها.

٢-٧	ضبط إعدادات أنظمة إدارة قواعد البيانات (DBMS) لإرسال سجلات الأحداث إلى نظام التسجيل والمراقبة المركزية وفقًا لمعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمد لدى <اسم الجهة>.
٣	معايير أخرى (Other Standards)
الهدف	تطبيق جميع المعايير والمتطلبات الأمنية لقواعد البيانات لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق جميع المعايير والمتطلبات الأمنية يعرض <اسم الجهة> إلى زيادة في المخاطر الأمنية لقواعد البيانات.
الإجراءات المطلوبة	
١-٣	تطبيق المعايير التالية: ١- معيار إدارة هويات الدخول والصلاحيات. ٢- معيار التعافي من الكوارث والنسخ الاحتياطية. ٣- معيار التشفير. ٤- معيار أمن الخوادم. ٥- معيار الأمن المادي.

الأدوار والمسؤوليات

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

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

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

٤- **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 في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

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

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

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