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 سياسة 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

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بحماية قواعد البيانات (Database) الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية ب<اسم الجهة> من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية (شاملة أنظمة قواعد البيانات) الخاصة ب<اسم الجهة>، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

بنود السياسة

١- البنود العامة

١-١ يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل <اسم الجهة>.

٢-١ يجب توفير بيئة آمنة مناسبة لحماية أنظمة قواعد البيانات من المخاطر البيئية والتشغيلية بما يتناسب مع تصنيف قواعد البيانات.

٣-١ يجب تطوير واعتماد معايير تقنية أمنية لأنظمة قواعد البيانات داخل <اسم الجهة> وتطبيقها من قبل مشرفي قواعد البيانات.

٤-١ يجب منع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات، فيما عدا مشرفي قواعد البيانات (Database Administrators) ويتم ذلك من خلال التطبيقات فقط، وبناءً على الصلاحيات المخوّل بها مع مراعاة تطبيق حلول أمنية تحد أو تمنع اطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data)، وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

٥-١ يجب منح حق الوصول أو الاطلاع أو التعديل على قواعد البيانات وفقًا لسياسة إدارة هويات الدخول والصلاحيات المعتمدة لدى <اسم الجهة>.

٦-١ يجب تطبيق متطلبات جميع السياسات ذات العلاقة بأمن الإعدادات والتحصين المعتمدة لدى <اسم الجهة> ويشمل ذلك على سبيل المثال لا الحصر السياسات التالية:

١-٦-١ سياسة حماية الخوادم المعتمدة لدى <اسم الجهة>.
٢-٦-١ سياسة الحماية من البرمجيات الضارة المعتمدة لدى <اسم الجهة>.

٣-٦-١ سياسة الأمن المادي المعتمدة لدى <اسم الجهة>.

١-٧ يجب منع نسخ أو نقل بيانات قواعد البيانات الخاصة بالأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة اخرى إلا بعد إجراء الاختبارات اللازمة.

١-٨ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية قواعد البيانات.

٢- الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات

٢-١ يجب تحديد متطلبات استمرارية الأعمال والتعافي من الكوارث الخاصة بقواعد البيانات المستضافة في العقود المعنية مع مزوّد الخدمة السحابية، والتي تتضمّن الأدوار والمسؤوليات المتبادلة من حيث الخطط والاختبارات للنسخ الاحتياطي والاستجابة للحوادث والتعافي من الكوارث وغيرها.

٢-٢ يجب توفير العزل المنطقي والعزل المادي بين قواعد البيانات الخاصة ب<اسم الجهة> وقواعد البيانات المستضافة الأخرى خاصة لقواعد البيانات الحساسة بما يتناسب مع تصنيف قواعد البيانات.

٢-٣ يجب إجراء مراجعة دورية للإعدادات والتحصين (Secure Configuration and Hardening) الخاصة بقواعد البيانات في <اسم الجهة> مرة واحدة كل سنة على الأقل.

٢-٤ يجب تقييد صلاحية الوصول الإداري إلى قواعد البيانات باستخدام وسيلة تشفير مُحكَمة مثل بروتوكول النقل الأمن (SSH)، أو الشبكات الخاصة الافتراضية (VPN)، أو طبقة المنافذ الآمنة (SSL)/أمن طبقة النقل (TLS)، أو استخدام آلية التحقق من الهوية متعدد العناصر (MFA)، وذلك وفقًا لسياسة التشفير المعتمدة في <اسم الجهة>.

٣- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

٣-١ يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقًا لعملية إدارة التغيير المعتمدة في <اسم الجهة>.

٣-٢ يجب تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في <اسم الجهة>.

٣-٣ يجب التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة عند التحديث أو التغيير.

٣-٤ يجب التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات ومراجعتها واختبارها سنويًا.

٣-٥ يجب توقيع اتفاقية مستوى الخدمة (SLAs) للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

٣-٦ يجب تطبيق التجزئة والتشفير على قواعد البيانات اثناء النقل والتخزين وفقًا لسياسة التصنيف وسياسة التشفير المعتمدة في <اسم الجهة>.

٤- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

٤-١ يجب تفعيل وحفظ سجلات الأحداث الخاصة بأنظمة قواعد البيانات وفقًا لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في <اسم الجهة>.

٤-٢ يجب على <الإدارة المعنية بالأمن السيبراني> مراقبة سجلات الأحداث المتعلقة بقواعد البيانات ومراقبة سلوك المستخدمين باستمرار.

٣-٤ يجب على <الإدارة المعنية بالأمن السيبراني> مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات باستمرار ومراقبة سلوكهم ومراجعتها كل ستة أشهر على الأقل.

٥- المتطلبات التشغيلية

١-٥ يجب على <الإدارة المعنية بتقنية المعلومات> مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه، وأخذ نسخ احتياطية خاصة لقواعد البيانات.

٢-٥ يجب مزامنة التوقيت (Clock Synchronization) مركزيًا لجميع أنظمة قواعد البيانات.

٣-٥ يجب تطبيق متطلبات سياسة النسخ الاحتياطية المعتمدة لدى <اسم الجهة>.

الأدوار والمسؤوليات

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

٢- **مراجعة السياسة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ السياسة وتطبيقها:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

٤- **قياس الالتزام بالسياسة:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

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

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذه السياسة.

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