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

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

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

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط ١-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بـ<اسم الجهة>، وتنطبق على جميع العاملين في <اسم الجهة>.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل <اسم الجهة> والعمل على توفير البيئة المناسبة لحمايتها من المخاطر البيئية والتشغيلية.

2-1 يجب تطوير واعتماد معايير التقنية الأمنية لأنظمة قواعد البيانات داخل <اسم الجهة> وتطبيقها من قبل مشرفي قواعد البيانات.

3-1 فيما عدا مشرفي قواعد البيانات، يمنع الوصول أو التعامل المباشر مع قواعد البيانات الخاصة بالأنظمة الحساسة، ويتم ذلك من خلال التطبيقات فقط. (CSCC-2-2-1-8)

4-1 يتم منح حق الوصول إلى قواعد البيانات وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

5-1 يمنع نسخ أو نقل قواعد البيانات الخاصة بالأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة اخرى. (CSCC-2-6-1-5)

2- الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات

1-2 التحديد الواضح لمتطلبات استمرارية الأعمال والتعافي من الكوارث الخاصة بقواعد البيانات المستضافة في العقود المعنية مع مزوّد الخدمة السحابية، والتي تتضمّن الأدوار والمسؤوليات المتبادلة من حيث النسخ الاحتياطية والاستجابة للحوادث وخطة التعافي من الكوارث وغيرها.

2-2 توفير العزل المنطقي بين قواعد البيانات الخاصة بـ<اسم الجهة> وقواعد البيانات المستضافة الأخرى.

3-2 يجب أن يكون موقع الاستضافة الخاص بالخدمات السحابية موجوداً ضمن النطاق الجغرافي للمملكة العربية السعودية. (ECC-3-3-2-4)

4-2 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)، وذلك وفقاً لسياسة التشفير المعتمدة في <اسم الجهة>.

3- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

1-3 يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقاً لعملية إدارة التغيير المعتمدة في <اسم الجهة>.

2-3 يتم تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في <اسم الجهة>.

3-3 التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة.

4-3 التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات.

5-3 يجب على <اسم الجهة> توقيع اتفاقية مستوى الخدمة للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

6-3 تطبيق التجزئة والتشفير على قواعد البيانات المخزنة وفقاً لسياسة التصنيف وسياسة التشفير المعتمدة في <اسم الجهة>.

4- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

1-4 تفعيل وحفظ سجلات الأحداث الخاصة بنظام قواعد البيانات وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في <اسم الجهة>.

2-4 يجب على <الإدارة المعنية بالأمن السيبراني> مراقبة سجلات الأحداث المتعلقة بقواعد البيانات الخاصة بالأنظمة الحساسة، ومراقبة سلوك المستخدمين.

3-4 يجب على <الإدارة المعنية بالأمن السيبراني> مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات ومراقبة سلوكهم ومراجعتها دورياً.

5- المتطلبات التشغيلية

1-5 توفير المتطلبات اللازمة لتشغيل قواعد البيانات بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة، وتقييد الوصول المادي إلى الأنظمة والسماح بذلك للعاملين المصرح لهم فقط.

2-5 يجب على <الإدارة المعنية بتقنية المعلومات> مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه.

3-5 مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أنظمة قواعد البيانات. (ECC-2-3-3-4)

6- متطلبات أخرى

1-6 استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لنظام إدارة قواعد البيانات.

2-6 مراجعة متطلبات الأمن السيبراني الخاصة بإدارة قواعد البيانات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

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

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

الالتزام بالسياسة

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> ضمان التزام <اسم الجهة> بهذه السياسة دورياً.

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

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