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

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

قائمة المحتويات

الأهداف

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

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة إدارة قواعد البيانات (DBMS) الخاصة بـ<اسم الجهة>، وينطبق على جميع العاملين في <اسم الجهة>.

المعايير

1	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	
1-1	مراجعة الجوانب الأمنية لتصميم تقنيات نظام إدارة قواعد البيانات (DBMS) الجديدة واعتمادها من قبل الطرف المعني المصرّح له قبل التثبيت. The security aspects of the design of new DBMS technologies shall be reviewed and approved by the respective authorized party prior to deployment.
2-1	توثيق كافة الخدمات والتطبيقات والأدوات التي يمكنها الوصول إلى قواعد البيانات وحفظها، على أن تشمل الوثائق وصفاً موجزاً لاحتياجات العمل.

All services, applications and tools that access databases shall be documented and maintained, and the documents shall include a brief description of business needs.	
وضع المكونات المادية للخوادم التي تستضيف نظام إدارة قواعد البيانات (DBMS) في بيئة آمنة ومغلقة ومراقبة. Physical components of the servers that host the DBMS shall be located in a secure, locked and monitored environment.	3-1
وضع خوادم نظام إدارة قواعد البيانات (DBMS) وراء جدار حماية لمراقبة الحركة من وإلى خادم قاعدة البيانات. DBMS servers shall be located behind a firewall to control traffic to and from the database server.	4-1
يجب أن تسمح قواعد جدار الحماية بالوصول الى تطبيقات أو خوادم ويب محدّدة فقط وتمنع ما دون ذلك. كما يجب منع الوصول المباشر إلى خوادم أنظمة إدارة قواعد البيانات (DBMS) الموجودة على الشبكات الداخلية الخاصة بـ<اسم الجهة>، ومنع كافة أنواع الاتصال الأخرى. Firewall rules shall allow access only to specific applications or web servers. Direct connection to the DBMS servers on <entity name>'s internal networks shall not be allowed, and all other traffic shall be denied.	5-1
تقييد الوصول عن طريق الشبكة إلى خوادم نظام إدارة قواعد البيانات (DBMS) وحصره على مصادر شبكة محدودة مثل خوادم الويب وخوادم التطبيقات وشبكات منطقة التخزين. Network access to DBMS servers shall be restricted to strictly defined network resources such as web servers, application servers and storage area networks.	6-1
العزل المادي أو المنطقي لقواعد البيانات في بيئة الإنتاج عن قواعد البيانات في البيئات الأخرى مثل بيئة الاختبار وبيئة التطوير. Production databases shall be physically or logically isolated from other environments such as development or test environments.	7-1

8-1	عدم استخدام البيانات الموجودة في قواعد بيانات الإنتاج عند اختبار أو تطوير بيئات قواعد البيانات، مع التأكيد على تطبيق ضوابط أمن سيبراني مثل التعتيم (mask) أو مزج (scramble) البيانات الحسّاسة قبل استخدامها في بيئتي الاختبار أو التطوير. Data in production databases shall not be used when testing or developing databases environments, emphasis on applying cybersecurity controls such as masking or scrambling sensitive data before being used in the testing or development environments.
9-1	تمييز طريقة التسمية بين خوادم نظام إدارة قواعد البيانات (DBMS) الإنتاجية وغير الإنتاجية. Naming conventions shall be distinguished between production and non-production servers.
10-1	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). DBMS servers shall be dedicated and shall not host any other functionality such as “Web or Application Tier” or “Domain Services”.
11-1	يجب إعادة تسمية جداول قواعد البيانات الافتراضية. Default database table names shall be changed.
12-1	تحصين كافة أنظمة التشغيل التي تستضيف قاعدة (أو قواعد) البيانات، وذلك وفقاً لمعيار أمن الخوادم. All operating systems that host the database(s) shall be hardened in accordance with the Server Security Standard.
13-1	استخدام الإجراءات المخزّنة المتوفّرة للتطبيق فقط لإجراء التعاملات أو الاستفسارات من قواعد البيانات. Only stored and available procedures for the application shall be used to make transactions or queries from the database.
14-1	عدم تحديد روابط خوادم نظام إدارة قواعد البيانات (DBMS) (مثل إنشاء اتصالات أو واجهات) بين أنظمة إدارة قواعد البيانات (DBMS) الإنتاجية وغير الإنتاجية.

DBMS servers links (such as creating connections or interfaces) shall not be defined between production and non-production DBMS(s).	
استخدام خاصية التحقّق من البيانات لضمان سلامة البيانات المخزّنة. Data validation shall be used to ensure the integrity of stored data.	15-1
تقييد حقول قاعدة البيانات بمجالات محدّدة من المدخلات واستخدام المدخلات الثنائية أو طرق التحقّق الأخرى من المدخلات، مثل التحقّق من الحدود (Boundary Checking)، أو التحقق من المحتوى وتصفية روابط مواقع الإنترنت (Content Inspection/URL Filtering)، لمنع أو الحد من العمليات التالية: • 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 Database fields shall be limited to specific ranges of input. In addition, dual input or other input checks (such as Boundary Checking and Content Inspection/URL Filtering) shall be used to limit transactions such as: • Missing and/or incomplete data • Out of range values • Unauthorized or inconsistent data • Invalid characters in data fields • Exceeding upper or lower date volume limits	16-1
تقييد الوصول إلى ملفات إعدادات نظام إدارة قواعد البيانات (DBMS) والشفرة المصدرية (Source Code) للتطبيقات والبرمجيات المخزّنة في قاعدة البيانات ومراقبتها. Access to all DBMS configuration files, as well as to the source code of applications/scripts stored in the database, shall be controlled and monitored.	17-1
استخدام البرمجيات المرخّصة فقط والتي تم التحقّق من صحتها من المورّد في خوادم قواعد البيانات.	18-1

Only licensed software whose authenticity has been verified by the vendor shall be used on the database servers.	
استخدام إصدارات نظام إدارة قواعد البيانات (DBMS) التي يدعمها المورّد فقط. DBMS versions that are supported by the vendor shall be used only.	19-1
تطبيق كافة التحديثات والإصلاحات الأمنية المناسبة قبل تثبيت نظام إدارة قواعد البيانات (DBMS) في الخدمة، وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات. All appropriate security patches shall be applied prior to DBMS deployment into service and as per the Patch Management Policy.	20-1
إلغاء تفعيل البرمجة النصية (Scripting) من طرف الخادم على كافة قواعد البيانات إن لم تكن ضرورية. Server-side scripting on all databases shall be disabled if unrequired.	21-1
إلغاء تفعيل أو تقييد الوصول إلى البرامج والملفات التنفيذية الخارجية. Access to external executables shall be disabled or restricted.	22-1
حذف الرموز والملفات والأوامر الافتراضية وغيرها التي لم تعد ضرورية بعد تثبيت نظام إدارة قواعد البيانات (DBMS). Default code, files, objects, etc. that are no longer required after DBMS installation shall be deleted.	23-1
إلغاء تفعيل كافة الخدمات أو المنافذ غير الضرورية أو حذفها من خوادم قواعد البيانات. All unnecessary services or ports shall be disabled or removed from the database servers.	24-1
ضبط إعدادات قواعد البيانات لاستقبال اتصالات الشبكة على الواجهات (Interfaces) المصرّح بها فقط. Databases shall be configured to listen to network connections on authorized interfaces only.	25-1
يجب التأكد من سلامة حزم تحديثات وإصلاحات برمجيات قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في < اسم الجهة>.	26-1

	Database software patches and updates shall be checked for integrity as per <entity name>'s Patch Management Policy.
27-1	حفظ قائمة جرد دقيقة لكافة قواعد البيانات ومحتوياتها وتحديثها دورياً. An accurate inventory of all databases and their contents shall be maintained and regularly updated.
28-1	ترميز البيانات المخزّنة في قواعد البيانات باستخدام أنواع ترميز آمنة محدّدة مسبقاً وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>. Data stored in databases shall be labeled using predefined types of security labels as per <entity name>'s relevant policies and procedures.
2	تأمين الوصول (Secure Access)
الهدف	تطبيق ضوابط التحقّق والتصريح ذات العلاقة والمحدّدة لضمان منح حق الوصول إلى نظام إدارة قواعد البيانات (DBMS) وصلاحيات استخدامه بناءً على الحاجة إلى المعرفة والحاجة إلى التنفيذ.
المخاطر المحتملة	يمكن أن يؤدي الوصول غير المصرّح به إلى نظام إدارة قواعد البيانات (DBMS) أو صلاحيات استخدامه غير الضرورية إلى إفصاح غير مصرّح به أو تغييرات غير معتمدة على بيانات <اسم الجهة> وتعطيل سير العمل.
الإجراءات المطلوبة	
1-2	استخدام آليات آمنة فقط للتحقّق من هويات المستخدمين للوصول إلى قواعد البيانات مثل التحقق من الهوية متعدد العناصر والذي يتضمن مجموعة من عناصر التحقق مثل: • المعرفة (ما يعرفه المستخدم فقط "مثل كلمة المرور") • الحيازة (ما يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول") • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع") Only secure authentication mechanisms, such as mutli-factor authentication, shall be used to access databases. This may include a combination of: • Knowledge (something only the user knows, such as a password)

	• Possession (something owned by the user only, such as a program or a device generating random numbers, or SMSs for login records) • Inherent characteristics (a characteristic of the user only, such as fingerprints)
2-2	استخدام أنظمة التحكّم في الوصول لإدارة الوصول إلى نظام إدارة قواعد البيانات (DBMS). Central access control systems shall be used to manage access to DBMS.
3-2	التحقّق من هوية المستخدم أو التطبيق الذي يطلب الوصول إلى نظام إدارة قواعد البيانات (DBMS) قبل منحه حق الوصول. User or application requesting access to DBMS shall be authenticated prior to granting the requested access.
4-2	تغيير كلمات المرور الافتراضية للحسابات والخدمات (مثل "SA" و"Listener") قبل تثبيتها. Default passwords for accounts and services (such as SA and Listener) shall be changed prior to being deployed.
5-2	عدم السماح للحسابات الافتراضية (مثل "SA" و"PUBLIC") بالبقاء نشطة، حيث يجب أن تخضع هذه الحسابات إلى الإجراءات التالية: • تغيير اسمها أو حذفها أو إلغاء تفعيلها (حسب الحاجة). • عدم منح الحسابات الافتراضية التي يمكن حذفها (أو إلغاء تفعيلها) امتيازات وصلاحيات لاستخدام نظام إدارة قواعد البيانات (DBMS) إلا إذا اشترط المورّد ذلك مباشرةً. • في حال عدم التمكّن من تغيير اسم الحساب الافتراضي أو حذفه أو إلغاء تفعيله، يجب تقييد الوصول له وفقاً لسياسة إدارة الوصول. • منع الوصول المباشر إلى هذه الحسابات/الوظائف (التي لا يمكن تغيير اسمها أو حذفها أو إلغاء تفعيلها) والطلب من المستخدم تسجيل الدخول من خلال حسابه الخاص ذي الامتيازات والصلاحيات الإدارية. Default accounts (such as SA and PUBLIC) shall not be permitted to remain active. The following MUST be maintained with regards to these accounts:

• Rename, delete or disable default accounts (as appropriate). • Do not grant DBMS/object privileges to default accounts which cannot be removed (or otherwise disabled) unless there is an explicit vendor requirement to do so. • In case default accounts cannot be renamed, deleted or disabled, restrict and control access to them as per the Access Management Policy. • Prevent direct access to such accounts/functions (which cannot be renamed, deleted or disabled) and require the user to logon with their individual account with administration privileges.	
تطبيق سياسات التحكّم في الوصول التقديرية (Discretionary Access Control)، على النحو الذي حدّده مالك البيانات، على المستخدمين والأوامر المحدّدة (Subjects and Objects). Discretionary Access Control policies, as defined by the data owner, shall be enforced over specified subjects and objects.	6-2
الحفاظ على الفصل بين المهام في جميع أنظمة إدارة قواعد البيانات (DBMS)، وعدم استخدام مشرفي قواعد البيانات (DBA) حسابات المديرين/حسابات المستخدمين عالية الامتيازات (Admins/Super User Accounts) في الأنشطة اليومية. Segregation of duties shall be maintained across all DBMS. Admins/Super User accounts shall not be used by DBA for day-to-day activities.	7-2
تقييد الوصول إلى الحسابات ذات الإمكانات الإدارية وحصره على عددٍ قليل من الأفراد المصرّح لهم حسبما هو مطلوب لإدارة نظام إدارة قواعد البيانات (DBMS) والتطبيقات. Access to accounts with administration capabilities shall be limited to a few authorized individuals as needed to manage the DBMS and applications.	8-2
تطبيق مبدأ الحد الأدنى من الصلاحيات على الوصول إلى نظام إدارة قواعد البيانات (DBMS) وتقييد التصاريح اللازمة لأداء الوظائف في قاعدة البيانات بناءً على الأدوار والمسؤوليات الوظيفية، وإدارة التصاريح من خلال الأدوار أو المجموعات وليس من خلال التصاريح المباشرة الممنوحة إلى هويات المستخدم. Least privilege principle shall be applied on DBMS access, and the permissions required for performing the job function in	9-2

the database shall be limited based on the job role and responsibilities. In addition, permissions shall be managed through roles or groups and not by direct grants to user IDs.	
تقييد قدرة مستخدمي قواعد البيانات على الوصول إلى محتويات قواعد البيانات أو إدراجها أو تعديلها أو حذفها بناءً على مهامهم في العمل. Database users' ability to access, insert, modify or remove content in databases shall be restricted based on their work duties.	10-2
تجنب تشغيل خدمات نظام إدارة قواعد البيانات (DBMS) على نظام التشغيل الخاص بالمستضيف من خلال حسابات ذات امتيازات وصلاحيات. Running DBMS services on the underlying host operating system through privileged accounts shall be avoided.	11-2
يجب على مديري قواعد البيانات (DBA) استخدام حسابات فردية لأداء المهام الإدارية وعدم استخدام حساب مشترك أو جماعي. Database administrators (DBAs) shall use individual accounts to perform administrative duties. Shared individual/group accounts shall not be used.	12-2
تطبيق أدوار الوصول على الجداول الافتراضية (Views) وقواعد البيانات، لتجنّب المخاوف المتعلّقة بمجموع أو تجميع بيانات منفصلة ضمن قواعد البيانات والتي يمكن أن تتيح للمستخدم تحديد المعلومات الحسّاسة أو المصنّفة. Access roles shall be applied on views and databases to avoid concerns related to the sum or aggregation of separate pieces of data within the databases, which could allow users to determine more sensitive or classified information.	13-2
عدم إعداد قواعد البيانات بكلمات مرور فارغة. Databases shall not be configured with blank passwords.	14-2
استخدام كلمات مرور قوية لكافة أنظمة التشغيل وحسابات قاعدة البيانات الخاصة بمدير قاعدة البيانات وتغييرها عند ترك المشرفين أو المتعاقدين مناصبهم حسب ما تنص عليه سياسة إدارة هويات الدخول والصلاحيات. Strong passwords for all DBA operating system and database accounts shall be used. In addition, passwords shall be changed when administrators/contractors leave their positions	15-2

اختر التصنيف

	as per the statements of the Identity and Access Management Policy.
16-2	حذف الملفات المؤقّتة (من عملية التثبيت) والتي يمكن أن تحتوي على كلمات مرور. Temporary files (from the installation process) that may contain passwords shall be removed.
17-2	تقييد الوصول إلى ملفات قواعد البيانات وحصره على العمليات ذات العلاقة والمستخدمين الإداريين المصرّح لهم. Access to database files shall be restricted to the relevant processes and the authorized administrative users.
18-2	إغلاق جلسة المستخدم تلقائياً بعد تلبية الشروط المحدّدة مثل انتهاء مهلة الجلسة. User session shall be terminated automatically after meeting defined conditions, such as session timeout.
3	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	
1-3	مزامنة أوقات جميع أنظمة إدارة قواعد البيانات (DBMS) مع خادم بروتوكول وقت الشبكة (Network Time Protocol) المركزي. All DBMS clocks shall be synchronized with the centralized Network Time Protocol (NTP) server.
2-3	يمكن إرفاق السجلات بسجلات نظام التشغيل أو أن تكون مستقلّة ضمن نظام إدارة قواعد البيانات (DBMS). Logs may be appended to the operating system logs or be self-contained within the DBMS.

3-3	إصدار سجلات التدقيق التي تحتوي على معلومات كافية لتحديد هوية أي مستخدم أو عملية ذات علاقة بالحدث المعني. Audit records containing sufficient information shall be generated to establish the identity of any user/subject or process associated with the event.
4-3	تسجيل نشاطات نظام إدارة قواعد البيانات (DBMS) التالية بحدّ أدنى: • 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 يُسبّب 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). • الأختام الزمنية عند وقوع الأحداث. • 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. • محاولات 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 أمراً آخر وهكذا). • إلغاء تفعيل سجلات نظام إدارة قواعد البيانات (DBMS) أو تعديلها. The following DBMS activities shall be recorded and logged at minimum: • All raised system alarms or errors • Start up • Shutdown

	• The creation, alteration, or deletion (drop) of databases, and any database storage structures, tables, indexes, accounts and objects • Enabling and disabling of audit functionality • Granting and revoking of DBMS system level privileges • Any action that returns an error message because the object referenced does not exist • Any action that renames a DBMS object • Any action that grants or revokes object privileges from a DBMS role or account • Time stamps when the events occurred • All modifications to the data dictionary or DBMS system configuration • Audits of all DBMS connection failures where possible. DBA shall ensure that both successful and unsuccessful connection attempts are audited • Failed logon attempts, and password locks • Attempts to add, modify or delete privileges/permissions • Deletion of categories of information (such as classification levels/security levels) • Abnormal command (command calling another command, etc.) • Disabling or modifying DBMS's logs
5-3	توفير تنبيه فوري ومباشر من أجل تقديم الدعم المناسب للأشخاص في جميع أحداث فشل التدقيق التي تتطلّب إجراءات مباشرة. An immediate real-time alert shall be raised to appropriately support individuals with all audit failure events requiring real-time action(s).
6-3	حماية خصائص التدقيق في نظام إدارة قواعد البيانات (DBMS) من عمليات الحذف غير المصرّح بها. Audit features in the DBMS shall be protected against unauthorized removal.
4	التعافي من الكوارث والنسخ الاحتياطية (Disaster Recovery and Backup)

الهدف	تحديد متطلّبات عمل نسخ احتياطية لقواعد البيانات واختبارها (مثل النموذج والوتيرة والنوع) لضمان توافر البيانات المخزّنة في قاعدة البيانات بمستوى مقبول لدى <اسم الجهة> في حال حدوث عطل كبير.
المخاطر المحتملة	في حال حدوث عطل كبير في البنية التحتية الخاصة بـ<اسم الجهة>، بما في ذلك نظام إدارة قواعد البيانات (DBMS)، ولم تتوفر نسخ احتياطية سليمة، فإن <اسم الجهة> لن تكون قادرة على استئناف عملها بالصورة المطلوبة.
الإجراءات المطلوبة	
1-4	عمل نسخ احتياطية لقاعدة البيانات دورياً بناءً على احتياجات العمل ووفقاً لمتطلّبات خطة استمرارية الأعمال (BCP) وخطة التعافي من الكوارث (DRP). Databases shall be regularly backed up based on business needs and in line with Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) requirements.
2-4	اختبار البيانات المخزّنة والتي تم عمل نسخ احتياطية لها والتحقّق منها وتحديثها كل ثلاثة أشهر أو وفقاً لإجراءات اختبار خطة التعافي من الكوارث (DRP). Archived and backed up data shall be tested, verified and updated on a quarterly basis or as per the DRP testing requirements.
3-4	عمل نسخ من نظام إدارة قواعد البيانات (DBMS) (نسخ احتياطية تابعة) لجميع أنظمة قواعد البيانات المتواجدة خارج الموقع أو المستضافة على الخدمات السحابية (داخل المملكة العربية السعودية). DBMS (slave backups) shall be replicated for all database systems off site or on cloud (within KSA).
4-4	الاحتفاظ بالنسخ الاحتياطية من قاعدة البيانات لفترات زمنية معتمدة تكون كافية لتلبية متطلّبات استئناف العمل (كما ورد في الضوابط "ECC-2-9-2" و"CSCC-2-8-1" و"CSCC-2-8-2") وذلك لمدّة 12 شهراً لجميع قواعد البيانات و18 شهراً لقواعد البيانات للأنظمة الحساسة. Database backups shall be retained for an approved intervals sufficient to meet the business resumption requirements (as stated by "ECC-2-9-2", "CSCC-2-8-1" and "CSCC-2-8-2"). Backups of all databases shall be retained for 12 months, and 18 months for critical databases.

5	التشفير(Cryptography)
الهدف	تحديد متطلّبات تشفير نظام إدارة قواعد البيانات (DBMS) (بما في ذلك الاتصالات والتحقّق والتخزين) وتحديد متطلّبات البروتوكولات الآمنة وشهادات التشفير المعتمدة.
المخاطر المحتملة	قد يعرّض عدم استخدام نظام إدارة قواعد البيانات (DBMS) لآليات تشفير مُحكَمة <اسم الجهة> لإفصاح غير مصرّح به عن البيانات الحسّاسة.
الإجراءات المطلوبة	
1-5	تشفير قواعد البيانات وفقاً لسياسة التشفير لمنع التعديل غير المصرّح به على البيانات المصنّفة والخاصة المخزّنة. Databases shall be encrypted as per the Cryptography Policy to prevent unauthorized modification of classified and private data at rest.
2-5	تشفير قواعد البيانات وفقاً للمعايير والسياسات ذات العلاقة (يرجى الرجوع إلى سياسة تصنيف البيانات ومعيار التشفير المعتمد). Databases shall be encrypted as per the respective standards and polices (Refer to Data Classification Policy and Cryptography Standard).
3-5	نقل البيانات عبر الشبكة وبين الأنظمة باستخدام آليات تشفير قوية وكافية للحدّ من مخاطر انتهاك البيانات. Data shall be transmitted over the network and between systems using encryption mechanisms strong enough to minimize the risk of data exposure.
4-5	تشفير ملفات قاعدة البيانات، على مستوى قاعدة البيانات أو على مستوى الحقول، وفقاً للسياسات والإجراءات ذات العلاقة في <اسم الجهة>. Database files, on the database-level or field-level, shall be encrypted as per <entity name>'s relevant policies and procedures.
5-5	حماية مفاتيح التشفير وفقاً لسياسة التشفير. Encryption keys shall be protected as per the Cryptography Policy.

6-5	التحقّق من شهادات التشفير من المزوّد وهيئة منح الشهادات (CA) المعنية. All encryption certificates shall be verified from the provider and the Certificate Authority (CA).
7-5	تشفير أشرطة النسخ الاحتياطية التي تُخزّن النسخ الاحتياطية من قواعد البيانات وعدم تخزين مفتاح التشفير على نفس الأشرطة في حالة غير مشفرة. Backup tapes that store database backups shall be encrypted, and the encryption key shall not be stored in the same tapes in plain text.
8-5	تشفير كافة حركات (Traffic) المديرين أو المستخدمين أو التطبيقات من نظام إدارة قواعد البيانات (DBMS) وإليه. All administrator, user or application traffic to and from the DBMS shall be encrypted.
9-5	عدم استخدام بروتوكولات غير مشفّرة أو خدمات غير آمنة (مثل بروتوكول نقل النص التشعبي "HTTP"، وبروتوكول نقل الملفات "FTP"، وغيرها) واستخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وغيرها بدلاً منها. Unencrypted protocols or non-secure services (such as HTTP, FTP, etc.), shall not be used, and HTTPS, SFTP, etc. shall be used instead.
10-5	حساب القيمة المميزة (Hash) لعبارات المرور المخزّنة في قواعد البيانات باستخدام خوارزمية مُحكَمة وعشوائية بصورة فريدة (Uniquely Salted) لحساب النص المميز (Hash Function) بصورة فريدة. Hash passphrases stored in databases shall be calculated with a strong hashing algorithm that is uniquely salted.

الأدوار والمسؤوليات

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

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

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

الالتزام بالمعيار

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

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>.