سلطنة عُمان
وزارة التقنية والاتصالات
Sultanate of Oman
Ministry of Technology and Communications

مكتب الوزيرة
Office of the minister

عمان الرقمية
e.oman

تعميم رقم (٣ / ٢٠٢٠)
معايير أساسية لأمن قواعد البيانات لوحدات الجهاز الإداري للدولة

بناءً على ما تم إصداره من سياسات وأطر وإرشادات تتعلق بالممارسات والسياسات الأمنية في مختلف وحدات الجهاز الإداري للدولة وتأكيداً على أهمية الحفاظ على أمن المعلومات لهذه الوحدات بما فيها قواعد البيانات، تود وزارة التقنية والإتصالات التنويه على ضرورة إلتزام جميع وحدات الجهاز الإداري للدولة بتطبيق المعايير الأمنية الخاصة بقواعد البيانات لضمان حمايتها من التهديدات المحتملة ويمكن الإسترشاد بالمستند المرفق الذي يلخص الحد الأدنى من الإجراءات الواجب إتباعها حيال ذلك.

للمزيد من التوضيح والإستفسارات يمكن للمختصين التواصل مع المعنيين في الوزارة عبر البريد الالكتروني NOC.Services@mtc.gov.om أو على هاتف (٢٤١٦٦٨٨٨).

وتفضلوا بقبول فائق الإحترام والتقدير،،،

سلطنة عُمان
وزارة التقنية والاتصالات
Sultanate of Oman
Ministry of Technology and Communications

المهندسة/ عزة بنت سليمان الإسماعيلية
وزيرة التقنية والإتصالات

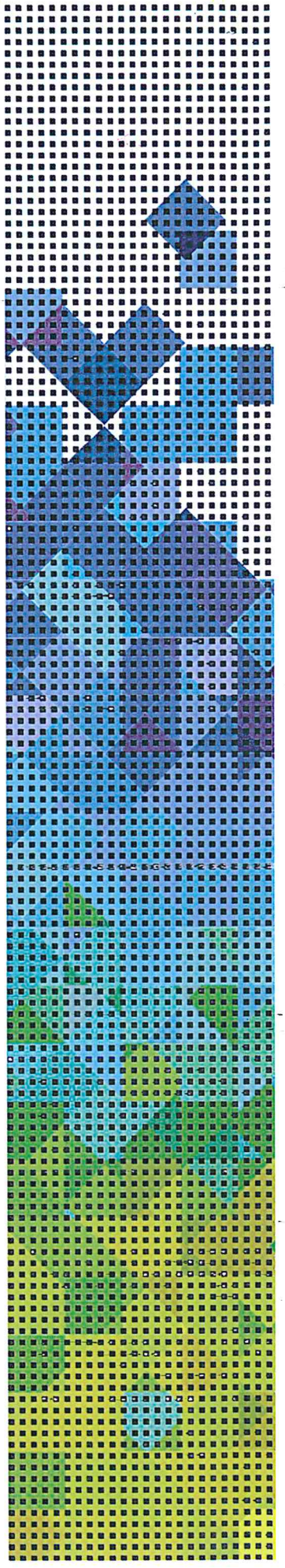
صدر في: ١١ شعبان ١٤٤١هـ
الموافق: ٥ أبريل ٢٠٢٠م

ص.ب: ١٨٠٧، الرمز البريدي: ١٣٠ العذيبة، سلطنة عُمان، هاتف: ٢٤١٦٦٦٠٠ (٠٠٩٦٨)، فاكس: ٢٤١٦٦٦٠٤ (٠٠٩٦٨)
P.O. Box: 1807, Postal Code: 130 Al Athaiba, Sultanate of Oman, Tel.: (00968) 24166600, Fax: (00968) 24166604

مرفق التعميم رقم (٣ /2020)

المعايير الاساسية لأمنْ قواعد البيانات لوحدات الجهاز الإداري للدولة

وزارة التقنية والإتصالات



التوثيق والتوزيع

	الجهة	البريد الالكتروني
صادر من	وزارة التقنية والإتصالات (قطاع أمن المعلومات)	NOC.Services@mtc.gov.om
تدقيق	وزارة التقنية والإتصالات (قطاع الحوكمة والإلتزام)	standards@mtc.gov.om

قائمة التوزيع	
١.	كافة الجهات الحكومية المعنية
٢.	الموقع الإلكتروني لوزارة التقنية والإتصالات

قائمة المحتويات

١- الغرض

الهدف من إصدار هذه الوثيقة هو التأكيد على إلتزام وحدات الجهاز الإداري في الدولة بالمعايير الأساسية لأمن قواعد البيانات وضرورة توفير الحماية اللازمة لقواعد البيانات لتفادي تعرضها إلى خطر التسريب أو التغيير الغير مصرح به أو أن يتم الإطلاع عليها من قبل الأشخاص الغير مصرح لهم .

٢- الفئة المستهدفة

تستهدف هذه الوثيقة جميع وحدات الجهاز الإداري للدولة ممثلة بالأقسام والموظفين المعنيين بالتعامل مع قواعد البيانات وإدارتها.

٣- ضوابط الأمن الأساسية

يجب على جميع وحدات الجهاز الإداري للدولة الالتزام بما يلي:

١- **تطبيق فصل الصلاحيات (Segregation of Duties)**

يلتزم مصمم ومطور ومدير النظم بتطبيق فصل الصلاحيات حيث يكون لكل موظف الصلاحيات التي تناسب طبيعة عمله والدور الذي يقوم به فقط. على سبيل المثال، يجب أن لا تتداخل صلاحيات مدير النظام مع صلاحيات مطور التطبيق/مدير قواعد البيانات وصلاحيات المستخدم.

٢- **تطبيق الحد الادنى للصلاحيات (Least Privilege)**

الالتزام بإعطاء الصلاحيات الضرورية للأشخاص المخولين في صورها الأدنى فقط حيث لا توجد ضرورة لإعطاء أشخاص صلاحيات أكثر من الحد اللازم لإتمام عملهم.

٣- قائمة صلاحيات المستخدمين **(List of User Permission)**

الالتزام بإعداد وتوثيق قائمة تتضمن صلاحيات المستخدمين والحرص على تحديثها بإستمرار، مثال على ذلك الجدول التوضيحي. ويتم تزويد مسؤول أمن المعلومات بهذه القائمه للقيام بعملية التدقيق الدوري بناءً عليها. كما توفر أنظمة قواعد البيانات عادةً خصائص لتنظيم الصلاحيات مما يساعد في عمليات التدقيق من خلال مقارنة الصلاحيات في القائمة بتلك المعتمدة في النظام. كما يجب تسجيل جميع حوادث الدخول إلى قواعد البيانات مباشرة بودن إستخدام التطبيق.

اسم الموظف	الوظيفة	مستوى الصلاحيات	وصف الصلاحيات	مخول من قبل	تاريخ منح وانتهاء الصلاحية الخ..
		مدير النظام الاول (Root Admin)	لديه كل الصلاحيات، إلا أن بيانات الدخول متحفظ عليها في خزنة محمية ولا تستخدم إلا في وقت الحاجة إليها فقط.	وفق قرار صادر من الإدارة العليا (مثل الوزير)	
		مدير النظام (Administrator) / مدير قواعد البيانات (Database Administrator)	صلاحيات التشغيل والتعديل وتغيير الإعدادات ومنح الصلاحيات بعد تحديدها من قبل الإدارة		
		مدقق (Auditor)	صلاحيات التدقيق فقط		
		مطور/ مبرمج (Developer / Programmer)	صلاحيات التطوير والبرمجه.		
		المستخدم (User)	الحد الادنى من الصلاحيات التي تمكنه من اداء المهام بناء على طبيعة عمله. قراءة وكتابة فقط		

جدول توضيحي: يمكن الاستعانة به.

٤- **تصنيف البيانات (Data Classification)**

الالتزام بتصنيف البيانات وفق قانون تصنيف وثائق الدولة وحمايتها وفق ذلك، والأخذ بعين الأعتبار تصنيف قواعد البيانات وفق آلية تساعد في فرز البيانات بطريقة تضمن تشفير حقول حساسة دون أخرى ودون التأثير على أداء النظام ومساحة التخزين.

٥- **تشفير البيانات الحساسة (Data Encryption)**

الالتزام بتشفير البيانات عن طريق التطبيق قبل حفظها في قواعد البيانات. تعتبر هذه الخاصية من أفضل الطرق وأأمنها من حيث الحفاظ على سرية المعلومات بحيث يتعذر حتى على من لديهم صلاحيات الدخول للنظام الوصول للبيانات وقرائتها أوالاستفادة منها بأي شكل من الأشكال إلا بعد فك تشفيرها من قبل الشخص المخول، على أن تتم عملية التشفير في مرحلة ما قبل وصول المعلومات لقاعدة البيانات. الجدير بالذكر أنه قد يتعين على فريق البرمجة القيام ببعض التغييرات على مستوى البرمجة.

٦- **التحكم بالوصول للبيانات (Access Control)**

الالتزام بضبط الوصول والدخول إلى البيانات بناءً على تصريح وتخويل من الإدارة بحيث يحدد التخويل ماهية البيانات التي يمكن للموظف الإطلاع عليها حسب طبيعة عمله وتصنيف البيانات (سري للغاية، سري، محدود، إلخ..)، وبالتالي التأكد من أن البيانات لا يتم الإطلاع عليها إلا من قبل المصرح لهم فقط.

٧- **إدارة التغيير (Change Management)**

الالتزام بتنفيذ اجراءات وخطوات إدارة التغيير وفق معايير وإجراءات محددة والتي بدورها تضمن فاعلية وشرعية التغيير وعدم تأثيره على سرية وأصالة وتوفر البيانات والخدمات.

٨- **التحديثات والترقيات الدورية والمستمرة لأنظمة قواعد البيانات والأنظمة المرتبطة بها (Update and Upgrade)**

الالتزام بتحديث وترقية أنظمة التشغيل وأنظمة قواعد البيانات والأنظمة المرتبطه بها بشكل دوري ومستمر حيث أنها تعالج الثغرات وتعزز الأمان لتفادي التعرض للإختراق أو التأثر بالبرمجيات الخبيثة المعروفة وتعمل على تصحيح الأخطاء وتحسين وظائف الأنظمة.

٩- **مراقبة ومتابعة أعمال إدارة قواعد البيانات بشكل مستمر عن طريق مهام التدقيق (Audit Trails)**

الالتزام بمراقبة الملفات الأرشيفية وتوثيق المراقبة بشكل دوري ومستمر لاكتشاف أي أعمال إدارية مشبوهة مثل استخلاص بيانات معينة أو تغييرها أو إتلافها.

١٠- **التوعية المستمرة للموظفين (Awareness Sessions)**

التزام مكتب أمن المعلومات بتوفير برامج التوعية اللازمة والمستمرة للموظفين فيما يتعلق بالبيانات وتصنيفها وكيفية التعامل مع الحوادث المتعلقة بها وطرق الإبلاغ عن اشتباه لتسرب البيانات أو عند العثور على بيانات سرية، وغيرها من المواضيع التوعوية التي تصب في مصلحة المحافظة على سرية وأصالة وتوفر البيانات.

٤- الوثائق المتعلقة

تم استخدام هذه الوثيقة وفقا لقائمة الوثائق المبينة أدناه :

- دليل إرشادات تصنيف البيانات ونظم أمن المعلومات
(Data and Information Systems Security Classification Mapping Guidelines)

- الدليل الإرشادي الخاص بالضوابط الاساسية لأمن المعلومات
(Basic Security Controls)

- إطار التصاميم والإعدادات الأمنية للأجهزة الطرفية والأجهزة الذكية
(End Point and Smart Devices Security Architecture and Configuration Framework)

- إطار التصاميم الأمنية للتطبيقات والخدمات الإلكترونية الحكومية
(Government Application and E-Services Security Architecture Framework)

- إطار التصاميم الأمنية للشبكات الحكومية
(Government Network Security Architecture Framework)

- ISO/IEC27001:2013