DAMA SAUDI

تصنيف البيانات

يجب تصنيف كافة المعلومات ضمن إحدى فئات السرية كما هو موضح أدناه

فئـــــة	وصـــــف	تأثير الإفصاح غير المصرح به	أمثلـــــة
عام	معلومات غير حساسة متاحة للنشر الخارجي.	لا شيء / يمكن إهماله.	• كتيبات التسويق. • الإلكتروني العام. • الإعلان. • التقارير السنوية. • كتيبات المنتجات والخدمات.
داخلي	المعلومات التي تعتبر حساسة فقط خارج المنشأة وتكون متاحة بشكل عام للموظفين وغير الموظفين المعتمدين	تأثير سلبي محدود.	• المحتوى الموجود على الشبكة الداخلية التنظيمية. • الهواتف الداخلية. • سياسات المؤسسة والسياسات والإجراءات الوظيفية.
سري	المعلومات الحساسة داخل المنشأة , وهي المعلومات المتعلقة بالمنشأة والموظفين والمساهمين والعملاء. وهي مخصصة للاستخدام التجاري فقط من قبل مجموعات محددة من الموظفين .	• تأثير سلبي كبير • قد يترتب عليه التزامات مالية أو قانونية أو تتعلق بالصورة. • قد يؤثر سلبًا على المنشأة أو موظفيه أو عملائه أو خط العمل. • قد يساعد المنافس. • قد يؤدي انعدام الثقة في المنشأة .	• المنافسة. • أفراد الأمن. • بيانات الرواتب أو النتائج المالية أو أي معلومات مالية أخرى. • معلومات العميل.
سري للغاية	معلومات حساسة للغاية داخل المنشأة .	• تأثير سلبي كبير للغاية: • تحمل مسؤوليات مالية أو قانونية أو تتعلق بالصورة. • التأثير سلبًا على المنشأة أو موظفيه أو عملائه. • انعدام الثقة في المنشأة	• النتائج المالية الحساسة أو أي معلومات مالية حساسة أخرى. • خطط زيادة رأس مال المنشأة. • أية معلومات تتعلق بالاندماجيات أو الاستحواذ أو حالة الأوراق المالية.

تصنيفات سلامة المعلومات وتقييم أصول المعلومات

لتحديد الحماية المناسبة للأصول، من الضروري تقييم قيمتها النوعية من حيث أهميتها بالنسبة للمنشأة .

يتم تقييم الأصول على أساس السرية والنزاهة والتوافر

- السرية: هي الخاصية التي تجعل المعلومات غير متاحة أو يتم الكشف عنها لأفراد أو كيانات غير مصرح لها.
- النزاهة: خاصية حماية دقة واكتمال الأصول.
- التوفر: خاصية إمكانية الوصول والاستخدام عند الطلب من قبل جهة معتمدة.

تقييمات السرية و النزاهة و التوافر

يقوم مالكو أصول المعلومات بتقييم الأصول بناءً على تأثير فقدان السرية والنزاهة والتوافر.
تُستخدم الإرشادات التالية لتقييم سرية وسلامة وتوافر أصول المعلومات.

التوفـــــر يحدد المستوى المناسب بناءً على التأثير في حالة عدم توفر الأصل	النزاهـــــة يحدد المستوى المناسب بناءً على التأثير في حالة التعديل غير المصرح به للأصل.	السريـــــة يحدد المستوى المناسب بناءً على التأثير في حالة الكشف غير المصرح به عن الأصل.	الأساس / تقييم الخطر
تأثير كبير في حالة عدم توفر الأصل. الحد الأقصى المسموح به لوقت التوقف هو 24 ساعة أو أقل	التأثير المالي المباشر، التأثير السلبي على صورة العلامة التجارية، الغرامات أو الإجراءات القانونية أو التنظيمية أو التعاقدية.	التأثير المالي المباشر، التأثير السلبي على صورة العلامة التجارية، الغرامات أو الإجراءات القانونية أو التنظيمية أو التعاقدية.	**عالية (5)**
قد يكون هناك بعض التأثير على المنظمة في حالة عدم توفر الأصول. الحد الأقصى المسموح به لوقت التوقف هو ما بين 24 ساعة وأسبوع واحد داخلي	بعض التأثير على المنظمة، عادةً بعض الخسائر التجارية أو المالية غير المباشرة.	بعض التأثير على المنظمة، عادةً بعض الخسائر التجارية أو المالية غير المباشرة.	**متوسط (3)**
لا يوجد تأثير أو تأثير ضئيل على المنظمة في حالة عدم توفر الأصول. الحد الأقصى المسموح به للتوقف هو أسبوع واحد أو أكثر	لا يوجد تأثير أو تأثير ضئيل على المنظمة..	لا يوجد تأثير أو تأثير ضئيل على المنظمة.	**منخفض (1)**

تقييـــــم الأصـــــــول

تمثل قيمة الأصول لغرض تقييم مخاطر أمن المعلومات تصـنيف أهميـة الأصـول. ويعتبـر تصـنيف أهميـة الأصول أعلى قيمة لتصنيفات السرية والنزاهة والتوافر

A=1g C=5, I=3

ثم يتم حساب القيمة النهائية للأصول على أنها أعلى قيمة.

تصنيف أهمية الأصول على أعلى القيم السرية و النزاهة و التوافر	
المعلومات حيوية و/أو استراتيجية وتتطلب ضوابط أمنية صارمة. إن التغيير غير المصرح به أو تدمير أو الكشف عن المعلومات من شأنه أن يسبب ضرراً كبيراً للمنظمة.	**عالية (5)**
المعلومات مهمة, لكنها ليست استراتيجية ويجب حمايتها من أفعال مثل التدمير الخبيث أو الكشف عنها. إن التغيير غير المصرح به أو التدمير أو الكشف عن المعلومات من شأنه أن يخلف تأثيراً معتدلاً على المنظمة	**متوسط (3)**
المعلومات ذات أهمية محدودة والتهديدات ضئيلة. إن التغيير غير المصرح به أو التدمير أو الكشف عن المعلومات من شأنه أن يسبب تأثيراً ضئيلاً أو غير مهم	**منخفض (1)**

سيساعد تصنيف أهمية الأصول في تحديد أولويات الأصول المدرجة في سجل مخاطر الأصول المعلوماتية.
يتم النظر في الأصول التي تبلغ قيمتها المتوسطة (3) أو المرتفعة (5) فقط لأداء الخطوات التالية, بما في ذلك تحديد التهديدات والثغرات الأمنية.

خطـــــــوات الإجـــــــــراء

1. **نهـــــج التصنيـــــف**

يجب على فريق حوكمة العمليات والبيانات التأكد من تصنيف جميع بيانات النظام ضمن إحدى هذه الفئات الأربع: سرية للغاية, وسرية للغاية, وداخلية, وعامة.

2. **تحديد نظام الشركة**

يجب معرفة كافة المعلومات المتعلقة بهذا النظام مثل قاموس البيانات واسم قاعدة البيانات واسم المضيف واسم المخطط. يقع على عاتق مالكي البيانات وأمناء التطبيقات ومسؤولي قواعد البيانات والموردين مسؤولية توفير هذه المعلومات.

3. **مراجعة مجموعة البيانات**

يجب على فريق حوكمة البيانات والتحكم فيها مراجعة البيانات بشكل صحيح وتوضيح جميع جوانبها .

4. **تصنيف البيانات**

في هذه الخطوة يقوم فريق حوكمة البيانات والتحكم بتصنيف حساسية البيانات بناءً على نهج التصنيف المتبع في الخطوة 1.

5. **التحقق من صحة المعلومات الأمنية**

يجب على قسم أمن المعلومات التحقق من صحة التصنيف وإذا كان صحيحًا فسيتم اتخاذ الخطوة التالية, وإذا لم يكن كذلك, العودة إلى الخطوة السابقة

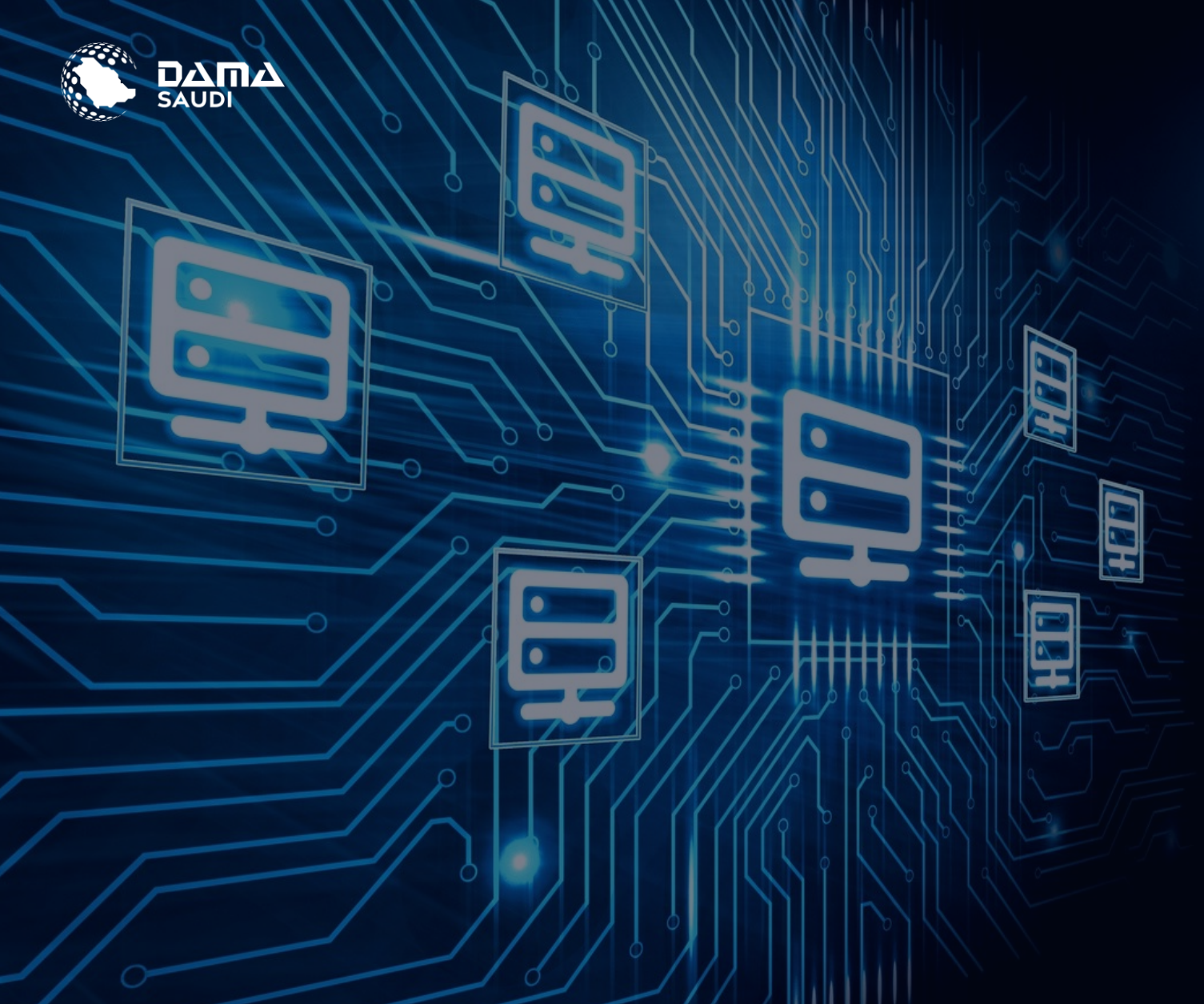
6. **تشفير ووضع العلامات على أمن المعلومات**

إذا كانت البيانات تحتاج إلى تشفير ووضع علامات, فسوف يتولى قسم أمن المعلومات عملية التشفير ووضع العلامات. ويقوم قسم أمن المعلومات بتحليل المدخلات وتنفيذ عناصر التحكم في الحماية المناسبة.

7. **التحقق من مالك البيانات**

بعد التحقق من أمان المعلومات, يجب على مالك البيانات أيضًا الموافقة على التصنيف, وإذا كان التصنيف صالحًا, فسيتم إنهاء العملية الامنية


نهج التصنيف
يجب على فريق حوكمة العمليات والبيانات التأكد من تصنيف جميع بيانات النظام ضمن إحدى هذه الفئات الأربع: سرية للغاية, وسرية للغاية, وداخلية, وعامة.
تحديد نظام الشركة
يجب معرفة كافة المعلومات المتعلقة بهذا النظام مثل قاموس البيانات واسم قاعدة البيانات واسم المضيف واسم المخطط. يقع على عاتق مالكي البيانات وأمناء التطبيقات ومسؤولي قواعد البيانات والموردين مسؤولية توفير هذه المعلومات.
مراجعة مجموعة البيانات
يجب على فريق حوكمة البيانات والتحكم فيها مراجعة البيانات بشكل صحيح وتوضيح جميع جوانبها .
تصنيف البيانات
في هذه الخطوة يقوم فريق حوكمة البيانات والتحكم بتصنيف حساسية البيانات بناءً على نهج التصنيف المتبع في الخطوة 1.
التحقق من صحة المعلومات الأمنية
يجب على قسم أمن المعلومات التحقق من صحة التصنيف وإذا كان صحيحًا فسيتم اتخاذ الخطوة التالية, وإذا لم يكن كذلك, العودة إلى الخطوة السابقة.
تشفير ووضع العلامات على أمن المعلومات
إذا كانت البيانات تحتاج إلى تشفير ووضع علامات, فسوف يتولى قسم أمن المعلومات عملية التشفير ووضع العلامات. ويقوم قسم أمن المعلومات بتحليل المدخلات وتنفيذ عناصر التحكم في الحماية المناسبة.
التحقق من مالك البيانات
بعد التحقق من أمان المعلومات, يجب على مالك البيانات أيضًا الموافقة على التصنيف, وإذا كان التصنيف صالحًا, فسيتم إنهاء العملية.



شكـــــــــراً

المراجـــــع

ISO/IEC 27001
NIST Special Publication 800-60
GDPR