



سياسة تصنيف البيانات بمحافظة مسندم

الإصدار	التاريخ	الإعداد	مستوى الخصوصية	الإعتماد
1.0	أغسطس 2024	دائرة تقنية المعلومات	عام	محافظ مسندم

قائمة المحتويات:

2	تعريفات.....
3	مقدمة
3	النطاق
4	المبادئ الرئيسة لتصنيف البيانات
5	المستويات الرئيسة لتصنيف البيانات.....
6	ضوابط تصنيف البيانات.....
9	خطوات تصنيف البيانات.....
12	الأدوار والمسؤوليات داخل المحافظة



تعريفات

المحافظة: محافظة مسندم

الإدارة العليا: محافظ مسندم

التقسيمات التابعة: التنظيمية جميع الوحدات الإدارية التابعة لمكتب محافظة مسندم

أصول البيانات: البيانات التي تنتجها وتملكها وتخزنها المحافظة

البيانات: الأرقام والخصائص الوصفية المتعلقة بمحافظة مسندم وخدماتها أو نشاطاتها، وقد تكون بيانات فردية أو مجموعة من البيانات الفردية أو ما تصدره الجهات الحكومية والخاصة المرتبطة بأعمال المحافظة من توثيق لأعمالها المختلفة على شكل أرقام بيانية، وقد يتم الاستفادة من تلك البيانات بعد معالجتها في عمليات دعم اتخاذ القرار .

البيانات الورقية: السجلات الورقية التي تدون فيها البيانات أو المعلومات المرتبطة فيها البيانات أو المعلومات المرتبطة بالمحافظة

البيانات الشخصية: كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة المستخدم على وجه التحديد، أو يجعله قابل للتعرف عليه بصفة مباشرة أو غير مباشرة، ويشمل ذلك الاسماء، وأرقام الهويات الشخصية، وأرقام والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم، وغير ذلك من البيانات ذات الطابع الشخصي .

بيانات الخدمات: البيانات المرتبطة بأعمال تقديم خدمات ونشاطات المحافظة، مثال البيانات المرتبطة بأعمال متابعة الشكاوى أو خدمات المراجعين الخ. حيث يتم استخدام هذه البيانات من قبل التقسيمات و الإدارات المختلفة بالمحافظة

البيانات الوصفية: هي مجموعة بيانات تصف الخصائص وتوفر المعلومات عن البيانات المتاحة لتسهيل عملية فهمها واستخدامها بشكل نظامي .

مالك البيانات: يقصد بمالك البيانات الوحدة التنظيمية التي تقوم بإنتاج البيانات، حيث تعتبر الجهة المالكة للبيانات المرجع النهائي بما يخص الاعمال والتصنيفات المرتبطة بالبيانات

مستخدم البيانات: أي شخص يطلع أو يتعامل أو يستفيد أو يدير البيانات سواء كان منسوباً للمحافظة أو لجهة أخرى خارجها.

مقدمة

تهدف هذه السياسة إلى وضع إطار موحد لتصنيف البيانات إلى أربعة مستويات (سري للغاية ، سري ، مقيد، عام) وذلك بناء على نتائج تقييم الأثر المترتب على الإفصاح غير المصرح به نظاماً أو الوصول غير المصرح به نظاماً عن البيانات أو عن محتواها ، بحيث يحدد هذا الإطار آلية الاطلاع على البيانات والتعامل معها وفقاً لمستوى تصنيفها.

النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها المحافظة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، الاجتماعات، و الاتصالات عبر وسائل التواصل والتطبيقات، ورسائل البريد الإلكتروني، والبيانات المخزنة على وسائط إلكترونية، وأشرطة الصوت أو الفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، وأي شكل آخر من أشكال البيانات المسجلة.

المبادئ الرئيسية لتصنيف البيانات

➤ الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتضي طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي الأمني) ما لم تقتضي طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية

➤ الضرورة والتناسب

يتم تصنيف البيانات إلى مستويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.

➤ التصنيف في الوقت المناسب

يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خال فترة زمنية محددة.

➤ المستوى الأعلى من الحماية

يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات تصنيف مختلفة.

➤ فصل المهام

يتم الفصل بين مهام ومسؤوليات العاملين - فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتالفها - بطريقة تحول دون تداخل الاختصاص وتتألف تشيت المسؤولية.

➤ الحاجة إلى المعرفة

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، وأقل عدد ممكن من العاملين.

➤ الحد الأدنى من الامتيازات

يتم تقييد إدارة صالحيات العاملين على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة بهم.



المستويات الرئيسية لتصنيف البيانات

مستوى التصنيف	درجة الأثر	الوصف	أمثلة
سري للغاية 	عالي	- يشمل البيانات الحساسة جدًا - التي إذا تم الوصول غير المصرح به إليها أو الإفصاح عنها، قد يتسبب في ضرر جسيم واستثنائي للمصلحة الوطنية.	- معلومات تمس سيادة الدولة. - المعلومات المتعلقة بآليات ومفاتيح التشفير المستخدمة للبنى التحتية الوطنية. - خطط وتفاصيل العمليات العسكرية أو أي معلومات ذات عالقة بها
سري 	متوسط	يشمل البيانات ذات الأهمية الكبيرة للمصلحة الوطنية، مثل العلاقات الدبلوماسية والأمن القومي.	- معلومات عن مواقع تخزين المواد اللوجستية أو المخازن الاقتصادية. - مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو اقتصادية استراتيجية بالمحافظة.
مقيّد 	منخفض	يشمل البيانات ذات الأهمية المتوسطة، مثل المعلومات الإدارية والتشغيلية.	- معلومات تضر بسمعة أي شخصية عامة. - معلومات رواتب الموظفين. - عقود موردين وعروض أسعارهم.
عام 	لا يوجد	يشمل البيانات العامة وغير الحساسة	- الإحصاءات الوطنية حول عدد السكان والبيئة والأعمال وغيرها . - إجراءات الحكومة وسياساتها. - معلومات متعلقة بالخدمات العامة التي تقدمها الحكومة للمواطنين . - جهات الاتصال في المؤسسات



ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم الجهات بتحديد وتطبيق الضوابط الأمنية الملائمة لحماية البيانات، بما يضمن التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن. وفي حال عدم تصنيف البيانات عند إنشائها أو استلامها وفقاً لمعايير التصنيف، يتم اعتبارها "مقيدة" إلى أن يتم تصنيفها بشكل صحيح. كما يجب تصنيف البيانات التي لم يتم تصنيفها عند إصدار هذه السياسة خلال فترة زمنية محددة. ندرج في هذا المستند الضوابط التي يمكن استخدامها عند تصنيف البيانات:

علامات الحماية	
تُوضع علامات الحماية النصية على الوثائق الورقية والإلكترونية، بما في ذلك رسائل البريد الإلكتروني، وفقاً لكل مستوى من مستويات التصنيف.	
الوصول	
يتم منح الوصول إلى البيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة". ويجب منع حق الوصول إلى البيانات فور انتهاء أو إنهاء الخدمة المهنية للموظفين في المحافظة.	
الاستخدام	
تُستخدم البيانات المصنفة وفقاً لمتطلبات مستويات التصنيف. على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" في مواقع محددة، سواء كانت مادية مثل المكاتب، أو افتراضية باستخدام ترميز الأجهزة أو تطبيقات خاصة.	
التخزين	
- لا يجوز ترك البيانات المصنفة "سرية للغاية"، "سرية"، و"مقيدة"، وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات، دون مراقبة. - يجب حماية البيانات المصنفة "سرية للغاية"، "سرية"، و"مقيدة" غير المراقبة أثناء تخزينها مادياً أو إلكترونياً باستخدام إحدى طرق التشفير المعتمدة من قبل المركز الوطني للسلامة المعلوماتية.	
مشاركة البيانات	
تقوم الجهات بتحديد و الإتفاق على الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة و الامتثال لأنظمة مشاركة البيانات.	



الاحتفاظ بالبيانات	
	يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات بناءً على المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات الصلة. تتم مراجعة هذا الجدول الزمني دوريًا - سنويًا أو عند حدوث تغييرات في المتطلبات ذات العلاقة.
التخلص من البيانات	
	• يتم التخلص من جميع البيانات بشكل آمن وفقًا للجدول الزمني للاحتفاظ بالبيانات، بعد الحصول على موافقة ممثل بيانات الأعمال. • يتم التخلص من البيانات المصنفة "سرية للغاية" و"سرية" التي يتم التحكم بها إلكترونيًا باستخدام أحدث طرق التخلص من الوسائط الإلكترونية. • يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق. • يتم إعداد سجل مفصل يتضمن جميع البيانات التي تم التخلص منها.
الأرشفة	
	• تتم أرشفة البيانات في مواقع تخزين آمنة وفقًا للطريقة التي يوصي بها ممثل بيانات الأعمال. • يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة. • تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و"سري" باستخدام إحدى طرق التشفير المعتمدة من قبل المركز الوطني للسلامة المعلوماتية. • يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.
إلغاء التصنيف (رفع السرية)	
	• يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى لا للتصنيف . • في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب . • يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمن هذه العوامل ما يلي:



- فترة زمنية محددة بعد إنشاء البيانات أو تلقيها على سبيل المثال: عامين بعد الإنشاء
- فترة زمنية محددة بعد اتخاذ آخر إجراء على البيانات على سبيل المثال: ستة أشهر من تاريخ آخر استخدام
- بعد انقضاء تاريخ محدد على سبيل المثال، من المقرر مراجعتها في 1 يناير 2025
- بعد ظروف أو أحداث معينة تأثيراً مباشراً مباشر إحداه تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية
- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.



خطوات تصنيف البيانات

الخطوة 1: تحديد جميع بيانات الجهة

جرد وتحديد جميع البيانات التي تمتلكها المحافظة.

الخطوة 2: تعيين مسؤول تصنيف البيانات

تقوم المحافظة بتخصيص شخص مسؤول عن تصنيف البيانات يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات ينبغي على المسؤول أن يفهم طبيعة البيانات وقيمتها داخل المحافظة، كما يجب أن يتحمل المسؤولية حيال إجراء التصنيف الأولي، ونظراً إلى وجود أكثر من مسؤول بيانات داخل المحافظة، فقد يوجد أكثر من شخص مسؤول عن تصنيف البيانات.

الخطوة 3: إجراء عملية تقييم الأثر

يقوم مسؤول تصنيف البيانات بتقييم الأثر المترتب على التالي:

- الوصول غير المصرح به للبيانات
 - تعديل البيانات أو إتالها أو كليهما
 - عدم الوصول إلى هذه البيانات في الوقت المناسب
- تتم عملية التقييم أخذاً بالإعتبار مبدأ: الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتضي طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي الأمني) ما لم تقتضي طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية

يقوم السؤول أولاً بتحديد الفئة الرئيسة والفرعية للأثر المحتمل من الفئات التالية:

- المصلحة الوطنية
- أنشطة الجهات
- صحة أو سلامة الأفراد
- الموارد البيئية

ثانياً يحدد لكل أثر محتمل مستوى معين، حيث يعتمد تحديد المستوى على الآتي:

- مدة الأثر وصعوبة السيطرة على الضرر
- المدة الزمنية لإصلاح الأضرار بعد وقوعها
- حجم الأثر المترتب على مستوى وطني، مناطقي، عدة جهات، جهة واحدة، عدة أفراد ... إلخ
- و عليه يتم تحديد مستويات الأثر الأربعة



- **عالي:** يمكن أن يؤدي الوصول إلى البيانات إلى أضرار جسيمة أو خطيرة على المدى الطويل، والتي يصعب تداركها أو إصلاحها.
 - **متوسط:** يؤدي الوصول إلى البيانات إلى حدوث أضرار كبيرة أو خطيرة يصعب السيطرة عليها
 - **منخفض:** يؤدي الوصول إلى البيانات إلى أضرار محدودة يمكن السيطرة عليها أو أضرار متقطعة على المدى القصير يمكن السيطرة عليها
 - **لا يوجد أثر:** لا يؤدي الوصول إلى البيانات إلى أي ضرر على المدى الطويل أو القصير .
- يتم الاعتماد على أدلة واضحة في تحديد الأضرار و آثارها و الحد من التقديرات الشخصية للمسؤول.
- يحدد مسؤول البيانات مستوى تصنيف البيانات بناء على الآثار المحددة ومستوياتها :
- **عال:** تصنف البيانات باعتبارها **سرية للغاية**
 - **متوسط:** تصنف البيانات على أنها **سرية**
 - **منخفض:** يلزم إجراء مزيد من التقييمات (يرجى الاطلاع على الخطوة 4 و 5)
 - **لا يوجد أثر:** تصنف البيانات على أنها **بيانات عامة**

الخطوة 4: تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفضاً)

ينبغي القيام بأكثر عدد من التقييمات في حالة كان مستوى الأثر المحدد "منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنها بيانات "عامة" إلى الحد الأقصى.

يقوم مسؤول تصنيف البيانات بدراسة ما اذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة السلطنة فحينها يجب تصنيف البيانات على أنها بيانات "مقيدة"، عدى ذلك يجب الإنتقال للخطوة 5.

الخطوة 5: لموازنة بين مزايا الإفصاح عن البيانات و الآثار السلبية (فقط إذا كانت الإجابة على الخطوة 4 "لا")

بعد ضمان أن مستوى الأثر منخفض و أن الإفصاح لن يكون انتهاكاً لأي نظام نافذ، يجب تقييم المزايا المحتملة للإفصاح و الأكّد من أن المزايا تفوق الآثار السلبية، و تكون المزايا عن طريق زيادة شفافية العمليات الحكومية أو زيادة مشاركة الأفراد مع الحكومة .

- المزايا أكبر من الآثار السلبية، تصنف البيانات على أنها **عامة**
- المزايا أقل من الآثار السلبية، تصنف البيانات على أنها **مقيدة**



الخطوة 6: مراجعة مستوى التصنيف

يتم مراجعة التصنيف من قبل المسؤول المباشر للوحدات المعنية للتأكد من صحة التصنيف المقدم من المسؤول

الخطوة 7: تطبيق الضوابط المناسبة

حماية جميع البيانات وفقاً لمستوى التصنيف عن طريق تطبيق ضوابط تصنيف البيانات

بعد الإنتهاء من جمع و تصنيف البيانات الخاصة بالمحافظة يتم التحقق و تطبيق الضوابط ذات الصلة، بعدها يمكن مشاركتها مع جهات أخرى، أو إتاحتها ونشرها بصفتها بيانات مفتوحة عند تصنيفها بيانات عامة.

الأدوار والمسؤوليات داخل المحافظة

يجب أن يتم تحديد أشخاص لتولي مسؤولية القيام بكل دور من الأدوار المرتبطة بعملية تصنيف البيانات وشروط حمايتها كالآتي:

مسؤول تصنيف البيانات

و هو الشخص المسؤول عن البيانات التي تجمعها المحافظة أو تحتفظ بها، و يكون مسؤول عن الأعمال التالية:

1. جميع البيانات: جمع البيانات من مختلف التقسيمات التابعة للمحافظة
2. تصنيف البيانات: تصنيف البيانات التي تجمعها المحافظة بكافة التقسيمات التابعة لها
3. تنظيم تبادل البيانات: إدارة عملية تبادل البيانات بين التقسيمات لضمان أن تكون متناسقة
4. اتباع ضوابط تصنيف البيانات (بالتنسيق مع مختصي البيانات في المحافظة): التأكد من أن البيانات محمية وفقاً للضوابط المحددة.

مراجع تصنيف البيانات

الشخص المسؤول عن مراجعة واعتماد مستويات تصنيف البيانات التي يحددها مسؤول تصنيف البيانات.

مختص البيانات

مختص البيانات عضو من دائرة تقنية المعلومات أو أمن المعلومات أو كليهما، ويتحمل مسؤولية حماية البيانات عن طريق تطبيق الضوابط المعتمدة المحددة في قسم "ضوابط تصنيف البيانات" بالإضافة إلى الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها. و تحدد مسؤولية مختص البيانات بالآتي:

1. التحكم في الوصول: التأكد من تطبيق ضوابط الوصول و مراجعتها وفقاً لمستويات تصنيف البيانات التي يحددها مسؤول تصنيف البيانات
2. إعداد تقارير المراجعة الدورية: إرسال تقرير سنوي إلى مسؤولي البيانات يتناول توافر البيانات المصنفة وسلامتها وسريتها
3. النسخ الاحتياطي للبيانات: إجراء نسخ احتياطي منتظمة للبيانات
4. التحقق من صحة البيانات: التحقق من صحة البيانات بشكل دوري
5. استعادة البيانات: استعادة البيانات من وسائط النسخ الاحتياطي
6. مراقبة البيانات : مراقبة الأنشطة التي تتم على البيانات وتسجيلها
7. اتباع ضوابط تصنيف البيانات (بالتنسيق مع مسؤول تصنيف البيانات في المحافظة) التأكد من أن البيانات محمية وفقاً للضوابط المحددة.

مستخدم البيانات



جميع الموظفين في المحافظة و الذي يقتضي عملهم التعامل مع البيانات أو الوصول إليها أو استخدامها أو تحديثها بغرض أداء مهمة بتحويل من مسؤول تصنيف البيانات، و يجب من المستخدمين الإمتثال لهذه السياسة وجميع السياسات المتعلقة باستخدام البيانات في السلطنة.