الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

سياسة تصنيف البيانات الوطنية

[IAP-NAT-DCLS]

مايو
2023
إصدار – V3.0

نحو فضاء
سيبراني آمن

إخلاء المسؤولية
الحقوق القانونية

الوكالة الوطنية للأمن السيبراني، قامت بإعداد وإصدار هذا المنشور، «سياسة تصنيف البيانات الوطنية» النسخة الثالثة. لمساعدة المؤسسات على تصنيف البيانات الخاصة بهم.

إن الوكالة الوطنية للأمن السيبراني مسؤولة عن مراجعة وصيانة الوثيقة.

أي نسخ لهذه الوثيقة سواء جزئيًا أو كليًا وبغض النظر عن وسائل الاستنساخ ، يجب أن يقر بالوكالة الوطنية للأمن السيبراني كمصدر و مالك للوثيقة «سياسة تصنيف البيانات الوطنية»

أي نسخ بخصوص هذه الوثيقة بقصد تجاري يجب أن يطلب تفويضًا كتابيًا من الوكالة الوطنية للأمن السيبراني. تحتفظ الوكالة الوطنية للأمن السيبراني بالحق في تقييم فاعلية وقابلية تطبيق جميع النسخ المطورة لأغراض تجارية. لا يجوز تفسير التفويض من الوكالة الوطنية للأمن السيبراني على أنه تأييد للنسخة المطورة ولا يجوز للمطور بأي حال من الأحوال نشر أو إساءة تفسير ذلك على أي من وسائل الإعلام أو المناقشات الشخصية / الاجتماعية.

معلومات الوثيقة

تفاصيل الوثيقة

◄ **معرف الوثيقة**	IAP-NAT-DCLS
◄ **النسخة**	3.0
◄ **وسم التصنيف**	عام
◄ **نبذة**	تم إعداد هذه الوثيقة كسياسة لوضع أسس إدارة البيانات داخل الحكومة ومؤسسات القطاع الحيوي في قطر ، وكذلك لإنشاء مخطط موحد لتصنيف البيانات لتسهيل تبادل المعلومات داخل قطر

المراجعة / الاعتماد

الشخص	المسمى الوظيفي / الإدارة	المرجعة/الاعتماد	النسخة	التاريخ
مدير شؤون الحوكمة والضمان السيبراني الوطني	مدير شؤون الحوكمة والضمان السيبراني الوطني		**V3.0**	مايو 2023

تسلسل التحديثات والمراجعة

النسخة	المؤلف	وصف المراجعة	التاريخ
1.0	المجلس الأعلى للاتصالات وتكنولوجيا المعلومات	منشور	يناير 2010
2.0	وزارة المواصلات والاتصالات – إدارة حماية البنية التحتية للمعلومات الحيوية	منشور	فبراير 2014
3.0	الوكالة الوطنية للأمن السيبراني – شؤون الحوكمة والضمان السيبراني الوطني	منشور	مايو 2023

"التفويض القانوني"

استنادا إلى المرسوم الأميري رقم 1 لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، والتي تهدف بدورها إلى الحفاظ على الأمن السيبراني الوطني وتنظيمه وتعزيز وحماية المصالح الحيوية للدولة في مواجهة التهديدات السيبرانية ، تنص المادة رقم (3) من القرار أن تختص بتطوير وتحديث السياسات وآليات الحوكمة والمعايير والضوابط والإرشادات اللازمة لتعزيز الأمن السيبراني بالتنسيق مع الجهات المعنية، وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها.

وفي هذا السياق، تم تطوير هذا المعيار الوطني لتأمين المعلومات الذي يهدف إلى تنظيم وحوكمة أمن وتامين المعلومات في مؤسسات دولة قطر وتحديد المبدأ الأساسي في فهم حوكمة البيانات وتغطية الضوابط المهمة لحماية البيانات خلال دورة حياتها.

اعتماد وتنفيذ هذا المعيار هو المسؤولية الكاملة للمؤسسة. لا تتحمل أي مسؤولية عن أي أضرار تتعلق بقرار غير مستنير باعتماد وتنفيذ هذا المعيار أو خارج نطاق هذا المعيار.

تم إعداد هذا المستند بناءً على الإختصاصات الواردة للوكالة الوطنية للأمن السيبراني بموجب القرار الأميري رقم 1 لسنة 2021. في حالة حدوث تعارض بين هذه الوثيقة (أحكام أو بنود محددة) وقوانين قطر، فإن هذه الأخيرة (القانون)، تكون لها الأسبقية. أي مصطلح بهذه الوثيقة (أحكام أو بنود محددة) يتعارض مع قوانين ولوائح قطر، لا يتم العمل به، دون التأثير على الأحكام المتبقية. وعندئذ يلزم إجراء تعديلات في هذه الحالة لضمان الامتثال للقوانين المعمول بها ذات الصلة في دولة قطر.

جدول المحتويات

1. مقدمة

إن التحول الرقمي والتطور التقني في كافة المجالات، كان له الأثر الهائل والانعكاس الواضح على مختلف الخدمات التي تقوم بها المؤسسات والتي أصبحت أغلبها رقمية. تعد البيانات المحور الرئيسي في هذا التطور، والذي أصبح ذلك واضحاً في كم البيانات الهائلة، ونتج عن ذلك استخدام المؤسسات للتقنيات الحديثة مثل تقنيات البيانات الضخمة وتعلم الآلة والذكاء الاصطناعي، ليس فقط للتعامل مع البيانات وإنما لتحسين تجربة التحول الرقمي والاستفادة منها.

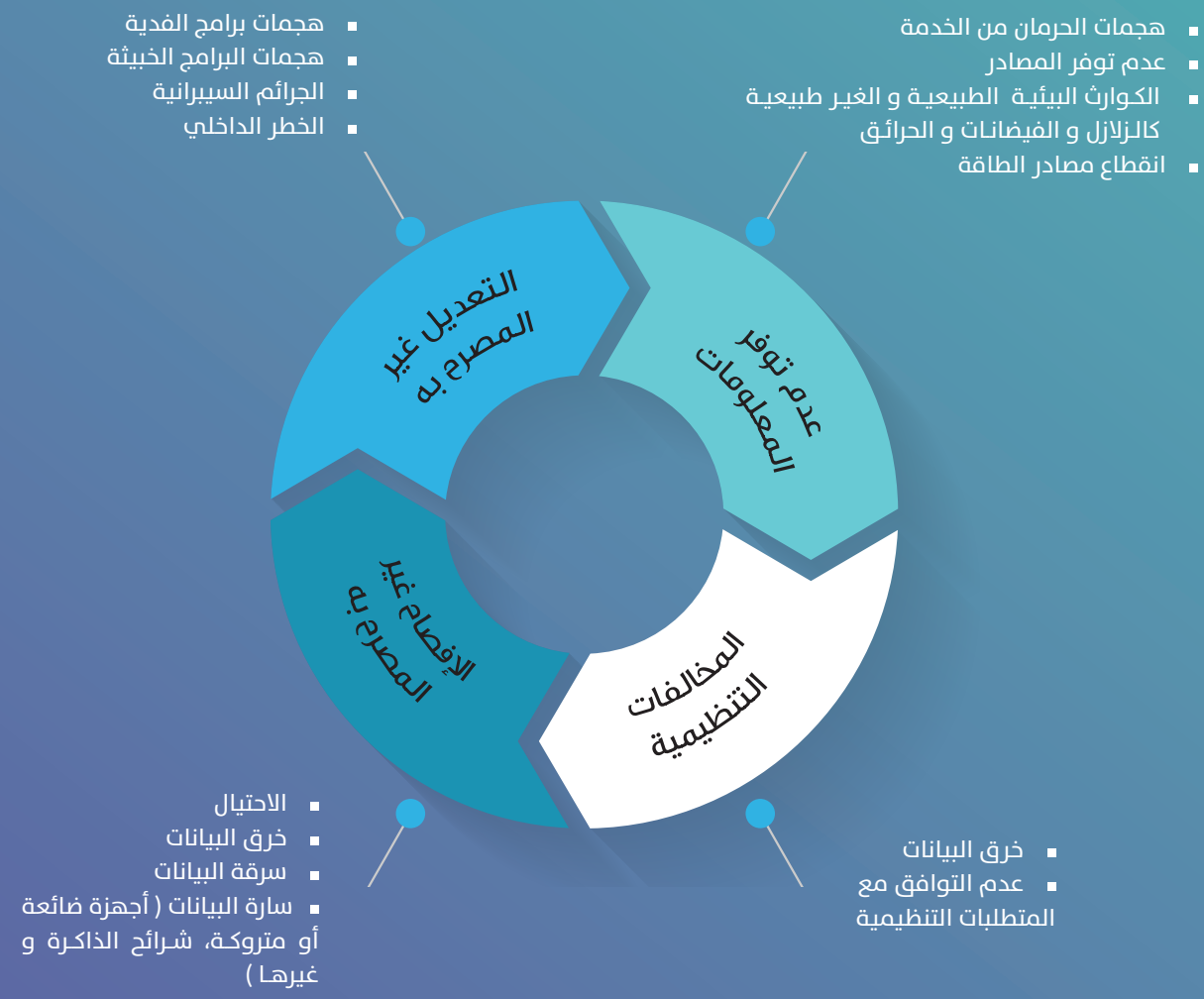
من أهم المفاهيم هو التعامل مع البيانات بمنهجية واضحة ومنظمة وسهلة التبني أو التطبيق. ولذلك فإن الحاجة إلى إدارة البيانات هو حجر الأساس الذي ينبغي على المؤسسات تطبيقه عن طريق تكوين نظرة شمولية ووضع الأسس لإدارة هذه البيانات في بيئة العمل، والتي تحقق الكثير من المنافع ومنها - على سبيل المثال لا الحصر - :

- تلبية توقعات العمل ، والحفاظ على المزايا التنافسية في سوق العمل
- إدارة الموارد بالشكل الأمثل
- توفير الضمان للعملاء وأصحاب المصلحة
- ضمان أمن بيانات العمل والحماية من المخاطر والتهديدات التي قد تتعرض لها
- تحقيق الامتثال مع المتطلبات التنظيمية

أصبحت البيانات من الأصول الحيوية للمؤسسات، والتي تتعرض للكثير من التهديدات ويجعلها في أغلب الأوقات في خطر. يوضح الرسم البياني التالي أهم المخاطر والتهديدات التي قد تتعرض لها البيانات ، والمصنفة حسب نوع التهديدات :

- الإفصاح عن المعلومات غير المصرح به
- تعديل المعلومات غير المصرح به
- عدم توفر المعلومات
- المخالفات التنظيمية

"من منظور وطني، توجد العديد من المخاطر والتهديدات التي قد تؤثر على الأمن السيبراني الوطني والمصالح الاقتصادية"



رسم توضيحي 1: أمثلة عن أبرز المخاطر والتهديدات للبيانات

من الحقائق الملحة في هذا السياق أن ليست كل البيانات في مستوى واحد من الأهمية والحيوية، وأن دور المؤسسات لفهم كيفية التعامل الأمثل مع البيانات وحمايتها أصبح ضرورياً ومن القدرات المهم التركيز على تطويرها.

ومما لا يسع المجال لإخفاءه أنه بدون استخدام نظام ومنهجية موحدة لتصنيف البيانات، سوف يكون لدى جميع المؤسسات مستويات مختلفة من حماية الأصول، بدون وجود مفاهيم محددة مما قد يعيق سير الأعمال خصوصاً أن البيانات في طبيعتها متنقلة.

2,1 الهدف

تهدف هذه السياسة إلى حوكمة تصنيف البيانات على مستوى وطني، وتوفير مرجعية وطنية للمبادئ الرئيسية في إدارة البيانات وتصنيفها عبر مراحلها المختلفة حرصاً على حماية المعلومات والأصول التي تحويها من المخاطر المحتملة ، و تسهيلاً لخلق التوافقية في تبادل البيانات بطريقة آمنة وميسرة.

كما تهدف إلى توحيد التعريفات الخاصة بتصنيف البيانات وخلق مفهوم موحد بين الجهات والمؤسسات في الدولة ومنهجية موحدة تسهيلاً لتبني وتنفيذ المشاريع والمبادرات على مستوى مؤسسي أو وطني. بالإضافة إلى توجيه أصحاب المصلحة (المؤسسات) ومساعدتهم على فهم المبادئ الأساسية في تصنيف البيانات وعنونتها وتطبيق ذلك داخل مؤسساتهم تماشياً مع السياسات الوطنية، والامتثال لها.

2,2 النطاق

يسري نطاق هذه السياسة على المؤسسات والقطاعات بدولة قطر والتي تقع ضمن نطاق المسؤولية الإشرافية للوكالة الوطنية للأمن السيبراني والتي تم إنشاؤها بموجب القرار الأميري رقم (1) لسنة (2021)، وبالتنسيق مع منظمي القطاعات.

2,3 الاستخدام

تحدد هذه السياسة منهجية رفيعة المستوى لتصنيف البيانات في المؤسسات في دولة قطر. سوف يؤدي الاستخدام المتسق لنهج تصنيف البيانات إلى مستويات مختلفة إلى إعطاء القيمة للمعلومات التي تملكها المؤسسة وبالتالي تحديد المخاطر المحيطة و ضمان الالتزام بأفضل الممارسات المقبولة عند معالجتها وحمايتها.

كما سيؤدي الاستخدام المتسق لنهج تصنيف البيانات إلى تيسير أنشطة العمل داخل المؤسسة، وضمان الالتزام بأفضل الممارسات المقبولة عند معالجتها وحمايتها ، والمساعدة على الاحتفاظ بتكاليف أمن المعلومات عند أدنى مستوياتها.

تعتبر هذه السياسة حجر الأساس لمعايير ضمان أمن المعلومات الوطنية وغيرها من المعايير والإرشادات الوطنية ولا يمكن التعامل معها على حدة. إن معايير ضمان أمن المعلومات الوطنية هو المستند المكمل لهذه الوثيقة والذي يوضح الضوابط الرئيسية التي على المؤسسات القيام بها ما بعد تصنيفهم للبيانات، والذي يتم تحديثه حسب الإجراءات المتبعة.

3 التعريفات

البيانات	البيانات هي حقيقة أو مجموعة من الحقائق لم يتم معالجتها أي تكون في صورتها الأولية الأصلية أو في صورة غير منظمة.
تصنيف البيانات	العملية التي يتم فيها تصنيف البيانات إلى مستويات بناءاً على ثلاثة محددات رئيسية: السرية، النزاهة والتوفر، وذلك لمعرفة كيفية التعامل معها بناءاً على تصنيفها الأمني
برنامج تصنيف البيانات	النشاط الذي تقوم به المؤسسة لتطبيق تصنيف البيانات حسب المنهجية الموصى بها، وبالتعاون مع كافة الأطراف المعنية
المؤسسات الحكومية	المؤسسات في دولة قطر والتي تتبع الديوان الأميري، أو مكتب رئيس مجلس الوزراء، أو الأمانة العامة لمجلس الوزراء، أو مكتب نائب الأمير.
المعلومات	هي البيانات التي تم معالجتها والتي أصبحت ذات معنى.
المنهجية	مجموعة الطرق، والعمليات والإجراءات، والتكتيكات والقواعد لتحقيق هدف معين
المؤسسات	أي كيان مؤسسي يقوم بتنفيذ أعمالاً داخل نطاق دولة قطر
البيانات الشخصية	بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أي بيانات أخرى.

4 المبادئ الرئيسية لتصنيف البيانات

تستند هذه السياسة على مجموعة من المبادئ الرئيسية التي يجب وضعها في عين الاعتبار عند تصنيف البيانات، تتيح هذه المبادئ الرئيسية الفرصة لإرشاد المؤسسات لأخذ القرارات بما يتعلق بمستوى تصنيف البيانات والضوابط المتعلقة به، وهي كالآتي:

1. فهم طبيعة البيانات
2. تبني نهج مراحل (أو دورة حياة) البيانات
3. التصنيف المبني على تقييم المخاطر
4. موازنة الاحتياجات
5. خلق الحوكمة

المبدأ الأول: فهم طبيعة البيانات

يعتبر فهم البيانات نقطة البداية في المنهجية المتبعة لتصنيف البيانات. إن فهم البيانات ضروري جداً، فطبيعة البيانات قد تكون مختلفة من نواحٍ متعددة منها: هل هي منظمة Structured أو غير منظمة Unstructured، المصدر، هل هي بيانات شخصية أم مملوكة لدى مؤسسة، هل تحوي في طبيعتها نوع من المخاطر عندما يتم تجميعها، وغيرها.

المبدأ الثاني: نهج مراحل (أو دورة حياة) البيانات

إن طبيعة التعامل مع البيانات تتضمن النظر في أصلها المتغير. وهي تمر بمراحل مختلفة كثيرة مثل : الإنشاء ، الاستقبال ، التنقل، التعديل ، الاستخدام، النسخ، التخزين ، المحو أو الإزالة، الاستعادة. ولذلك فإن عملية تصنيف البيانات يجب أن يتم النظر إليها من هذا المنطلق عبر استخدام التصنيفات المتوائمة مع دورة حياة البيانات. وتقسم مراحل إدارة البيانات إلى خمسة مراحل يتم التطرق إليها في الفصل اللاحق من هذا المستند.

المبدأ الثالث: التصنيف القائم على تقييم المخاطر

إن الغرض الأساسي من عملية تصنيف البيانات هو اتخاذ نهج يسهل على المؤسسات حمايتها من المخاطر المحتملة. وبالتالي فإن تقييم المخاطر هو من المبادئ الأساسية التي يجب اعتبارها عند تصنيف البيانات والتي يتم تحديد حساسية وأهمية هذه البيانات بالنسبة للأعمال التي تقوم بها المؤسسة. توجد مدارس تفكير ومنهجيات متعددة في الوسط المتخصص فيما يتعلق بكيفية تقييم المخاطر.

المبدأ الرابع: موازنة الاحتياجات

يجب أن يوضع بعين الاعتبار الموازنة والتناسب بين المخاطر التي تهدد البيانات ، ومستوى التصنيف الذي يتم اختياره بحيث تحقق هذه العملية مستوى التصنيف الأنسب و مستوى الحماية الضروري دون المبالغة ودون إضافة أية أعباء إدارية أو مالية أو تقنية قد تشكل عائقاً في سير الأعمال داخل المؤسسة.

المبدأ الخامس : خلق الحوكمة

لضمان نجاح تصنيف البيانات داخل المؤسسة، من المهم أن تضع المؤسسة إطار عمل حوكمة يضمن أن عملية إدارة وتصنيف البيانات تتم بالطريقة المتوقعة من قبل إدارة المؤسسة وبما يحقق الأهداف المرجوة منها. من المستحسن أن يمتلك شخص داخل المؤسسة برنامج تصنيف البيانات ويكون مسؤولاً عن تنفيذه واعتماده داخل المؤسسة كل حسب تخصصه والأدوار المناط بها.

إن عملية تصنيف البيانات ليست عملية تابعة لشخص أو جهة واحدة، وإنما تتطلب تظافر الجهود داخل المؤسسة لضمان أن يتم تنفيذ العملية طبقاً للمبادئ والأسس وأفضل الممارسات. لذلك فإن تحديد الأدوار والمسؤوليات وتوزيعها بالشكل المناسب وضمان وجود مبدأ المسؤولية والمسائلة داخل المؤسسة من المبادئ الرئيسية التي يجب النظر لها بعين الاعتبار.

5 مراحل إدارة البيانات

من المبادئ الرئيسية لسياسة تصنيف البيانات هي تكاملها مع مفهوم المرحلية أو (دورة حياة). تعتبر قيمة البيانات غير ثابتة إذ قد تتغير قيمتها حسب المرحلة التي تكون فيها مما ينعكس على درجة تصنيفها. ففي بعض المراحل تكون ذات قيمة عالية وفي بعض الأحيان قد تفقد قيمتها تماماً مما يؤدي الى الحاجة إلى التخلص منها.

أهم مراحل دورة حياة البيانات :

1	حصر البيانات
2	تصنيف البيانات
3	حماية البيانات
4	إعادة تقييم البيانات
5	إزالة البيانات

يتم في البداية حصر البيانات أو استكشافها وجردها، ثم يتم تصنيف البيانات بناءاً على قيمتها وعلى مبدأ تحليل المخاطر، ثم يتم تصميم وتحديد الضوابط الأساسية لحماية البيانات طبقاً لتصنيفها. كما لا تخلو العملية من التأكيد على أهمية المراجعة وإعادة تقييم البيانات مما ينعكس على التصنيف والضوابط. في حالة الحاجة إلى إزالة أو إتلاف البيانات يتم تنفيذ ذلك بالنظر إلى محددات معينة.

سيتم التطرق لتفاصيل مراحل إدارة البيانات في الملحق (أ).

1.6 مستويات التصنيف

يتم العمل على تصنيف البيانات وذلك بناءً على أهمية وحساسية البيانات التي تتعامل معها ومن الأغلب تتم هذه العملية خلال المرحلة الثانية من إدارة البيانات. يتم تصنيف البيانات بناءً على ثلاثة معايير أساسية وهي: السرية، النزاهة والتوفر.

يتم ذلك عبر مبدأ تحليل المخاطر، والتي تنظر إلى أثر قيمة هذه البيانات ضمن صميم أعمال المؤسسة أو جهة العمل وأهدافها. كما تنظر إلى المخاطر المحتملة التي تهدد سرية ونزاهة وتوفر هذه البيانات وبالتالي يتم وضع التصنيف المتناسق معها.

يتم تصنيف البيانات على أساس النظر إلى ثلاثة مستويات من السرية (ويشار إليها بالحرف C) والنزاهة (ويشار إليها بالحرف I) والتوفر (ويشار إليه بالحرف (A). بدءاً من المستوى (صفر) وهو أقل المراتب أثراً ، وانتهاءاً بالمستوى (3) وهو أعلى المراتب أثراً.

وباستخدام المصفوفة التالية، يتم النظر للمحددات الثلاثة ومستوياتها وإسقاطها ضمن المصفوفة التالية للتعرف على مستوى تصنيفها كـ : مرتفع (ويشار إليه بالحرف H) ، متوسط (ويشار إليه بالحرف M) أو منخفض (ويشار إليه بالحرفا)

		A0	A1	A2	A3
C0	I0		L	M	H
	I1	L	L	M	H
	I2	M	M	M	H
	I3	H	H	H	H
C1	I0	L	L	M	H
	I1	L	L	M	H
	I2	M	M	M	H
	I3	H	H	H	H
C2	I0	M	M	M	H
	I1	M	M	M	H
	I2	M	M	M	H
	I3	H	H	H	H
C3	I0	H	H	H	H
	I1	H	H	H	H
	I2	H	H	H	H
	I3	H	H	H	H

جدول 1: مصفوفة تصنيف البيانات

يتم استخدام مستويات التصنيف (مرتفع ، متوسط ، منخفض) على أصول المؤسسة، وتحدد الضوابط الأمنية اللازمة لحماية تلك الأصول عبر الوسائل التقنية والإدارية المختلفة، والتي يمكن الاستناد على معايير ضمان أمن المعلومات الوطنية لتحديدها وتطبيقها (انظر الفصل السابع) .

2.6 وسم تصنيف البيانات

تتم إضافة وسوم لبعض الأصول بالنظر إلى تصنيفها وذلك من ضمن أفضل الممارسات المتعارف عليها، مما يسهل على المستخدم معرفة كيفية التعامل مع البيانات أو المعلومات التي تحويها تلك الأصول.

إن وسوم تصنيف البيانات يتم اختيارها بناءاً على مستوى السرية التي يجب أن تتوفر لها ، وذلك لتسهيل عملية معالجة و مشاركة هذه البيانات مع الأطراف ذات الصلة، ومعرفة مستوى الحماية اللازم للتعامل معها من ناحية إجرائية أو تقنية.

إن وسوم تصنيف البيانات الموازية للتصنيف والموصى بها في هذه السياسة هي على النحو التالي :

- C0 عام
- C1 داخلي
- C2 محدود الوصول
- C3 سري
- C4 سري للغاية

بالنسبة لوسم تصنيف البيانات المذكورة فهي إلزامية للمؤسسات الحكومية. بالنسبة للمؤسسات غير الحكومية ، قد يُسمح ببعض المرونة في اختيار الوسوم مثل المستويات C3 ، ويمكن استخدام "مؤتمن" بدلاً من "سري" ، ولكن من الضروري أن تحتفظ المنظمة بمخطط تصنيف موحد في عملية التصنيف الخاصة بها.

يجب أيضاً توفير الأدوات الإدارية والتقنية التي تمكن من استخدام الوسوم، كما بالإمكان استخدام الترميز بالألوان للوسوم.

فيما يلي مثال إلى مستويات سرية البيانات وإسقاطها على الوسوم التابعة لها، وأمثلة على الفئات المستهدفة لاستخدامها:

أنواع وسوم تصنيف البيانات

C0	C1	C2	C3	C4
البيانات المتاحة للجميع	بيانات خاصة بالاستخدام الداخلي	بيانات حساسية اذا تم اخترقها فسوف تأثر على الخطة التشغيلية للمؤسسة	عالية السرية و التي تتضمن بيانات العملاء او بيانات العمل و اذا تم تسريبها فستتعرض المؤسسة للمسائلة القانونية و تشويه السمعة	عالية السرية
نوع الوصول: عام	الفئة المستهدفة: موظفي المؤسسة	الفئة المستهدفة: أشخاص محددين أو مجموعات تحدد بقوانين العمل	الفئة المستهدفة: فئة محدودة من الأشخاص	الفئة المستهدفة: الشخص المستقبل فقط

7 ضوابط تصنيف البيانات

بناءاً على مستوى التصنيف الذي تم تحديده ، يتم اختيار وتطبيق الضوابط الأمنية التي تساعد على حماية البيانات. يتم تطبيق الضوابط الأمنية بالنظر إلى المعايير والإرشادات الوطنية المتبعة. إن (معايير تأمين أمن المعلومات الوطنية هو المعيار المعتمد في دولة قطر، والذي يتم تحديثه وتطويره بالنظر إلى المعايير والإرشادات الوطنية التي تصدرها الوكالة الوطنية للأمن السيبراني.

بالإضافة إلى تطبيق ضوابط تصنيف البيانات الأمنية، هناك مجموعة من النقاط المهمة للنظر إليها وهي:

1- تقوم كل مؤسسة بإنشاء سياسة تصنيف معلومات داخلية خاصة بها تلتزم باتباعها لنهج تصنيف البيانات تماشياً مع القوانين ذات الصلة في دولة قطر ، مثل قانون حماية خصوصية البيانات الشخصية (قانون رقم 13 لسنة 2016) ، وقانون الحق في الحصول على المعلومات (قانون رقم 9 لسنة 2022) ، وكذلك مع السياسات والمعايير الوطنية.

2- يجب أن تخضع الضوابط المختارة لنوعية البيانات فهي قد تكون إما بيانات عابرة أو بيانات ساكنة أو بيانات مستخدمة.

3- من الضروري جداً، النظر في الخطوات اللاحقة لتصنيف البيانات وذلك لأهميتها البالغة في التأكد من نجاح وكفاءة سير عملية تصنيف البيانات. ومن أهم الخطوات اللاحقة:

- **دعم الإدارة:** طلب الدعم من أعلى سلطة إدارية في المؤسسة (الوزير، الرئيس التنفيذي وغيره).
- **الاتفاق الجماعي:** إنشاء مجموعات عمل أو لجان من عدة أقسام بالمؤسسة لتنفيذ المبادرة، وتحديد الأدوار والمسؤوليات
- **أطر العمل:** تحديد وتنفيذ السياسات والإجراءات اللازمة والخاصة بتصنيف البيانات وكيفية تنفيذ ومراجعة العملية.
- **التدريب والتوعية:** نشر الوعي وتدريب موظفي المؤسسة. يجب أن يكون جميع المستخدمين على علم ودراية بالمهام والواجبات المعلقة بإدارة البيانات.ولذلك يجب على المؤسسة أن تقدم التدريب المطلوب للموظفين حول طريقة التصنيف المتبعة في المؤسسة، ومتابعة الالتزام بها.
- **الحلول التكنولوجية**: تحديد وتطبيق الحلول التكنولوجية المتاحة والمناسبة للمؤسسة في هذا الشأن. وعلى المؤسسة أن تقدم حلولاً تكنولوجية لتسهيل عملية تصنيف البيانات بما في ذلك حصر البيانات وأدوات تصنيفها وإضافة الوسوم وطريقة مشاركتها ومعالجتها عبر مراحلها المختلفة بما يتناسب مع مستوى الحماية المطلوب.

4- **الوضوح في الأدوار والمسؤوليات:** تحديد الأدوار والمسؤوليات فيما يتعلق بتصنيف البيانات وكيفية حمايتها من أبرز المحددات في الوصول إلى الأهداف المتعلقة بعملية إدارة البيانات بنجاح وكفاءة.

5- إن الميل إلى المبالغة في تصنيف البيانات ، سوف يخلق الكثير من العوائق على المستوى الإداري والمادي. لذلك يجب النظر إلى التصنيف بطريقة متوازنة تحقق مستوى الحماية المطلوب دون المبالغة فيه.

6- C1 يمثل التصنيف الافتراضي للبيانات غير المصنفة والذي يوازي المسمى: (داخلي)

7- في حالة التعامل مع البيانات الشخصية وهي البيانات عن الفرد الذي تكون هويته محددة أو يمكن تحديدها بصورة معقولة، فإنه يجدر الإشارة أنها تخضع لقانون حماية خصوصية البيانات الشخصية (قانون رقم 13 لسنة 2016) والسياسات والإرشادات التي تصدرها الإدارة المختصة بالوكالة الوطنية للأمن السيبراني (المكتب الوطني لحماية خصوصية البيانات الشخصية) . لكن قد يكون من المقترح أن يتم اختيار وسم تصنيف البيانات (محدود الوصول) أو C2 في حالة التعامل مع البيانات الشخصية، وفي حالة البيانات الشخصية ذات الطبيعة الخاصة يتم اختيار وسم (سري) أو C3. لكن يجب أن لا يتم استخدام هذه الوسوم إلا بعد تحقيق المنهجية المتبعة في النظر إلى البيانات ومراحل إدارة البيانات.

8 الأدوار والمسؤوليات

إن عملية إدارة تصنيف البيانات هي عملية متكاملة تشتمل عدة مراحل (انظر إلى الملحق (1) حول مراحل إدارة البيانات) لذلك من الضروري تحديد الأدوار والمسؤوليات خلال هذه المراحل بطريقة تضمن المسؤولية والمسائلة.

كما تعد حوكمة إدارة البيانات من المبادئ الأساسي في تحقيق أفضل النتائج بشكل متزن ومدروس بحيث تكون كافة الأطراف ذات الصلة على علم بمسؤولياتها ومهامها، وتكون المؤسسة على علم ودراية بالطرق اللازمة لتحقيق مبدأ المسائلة. إن تصميم الحوكمة داخل المؤسسات قد يخضع للكثير من المتغيرات بحسب طبيعة عمل وحجم المؤسسة وهيكلية إداراتها، لكن توجد بعض الأدوار والمسؤوليات المحددة والتي تتطرق لها أفضل الممارسات العالمية ومنها:

كبير مسؤولي البيانات: الشخص المحدد من قبل الإدارة العليا ليكون مسؤولاً عن برنامج تصنيف البيانات في المؤسسة. يكون مسؤولاً عن تطوير السياسات والإجراءات اللازمة لإدارة البيانات وتصنيفها والإشراف على الضوابط المناسبة لحمايتها. ويكون مسؤولاً أيضًا عن تعيين الأدوار والمسؤوليات والإشراف عليها لأصحاب المصلحة المختلفين من أجل تنفيذ تصنيف البيانات الفعال في المؤسسة.

مالك البيانات : هو الشخص المسؤول عن البيانات التي تملكها المؤسسة وهو الذي يملك اتخاذ القرارات في تحديد قيمة البيانات بالنظر لسير الأعمال في المؤسسة. غالباً ما يكون مالك البيانات مسؤولاً عن وحدة الأعمال في المؤسسة ،ولذلك تكون لديه المعرفة الكافية بقيمة البيانات ويملك القدرة على اتخاذ القرارات بمستوى تصنيفها. يعد مالك البيانات أيضاً مسؤولاً عن ضمان وتسمية السجلات الخاصة بتصنيف البيانات عند إنشاءها وبإمكانه أن يوكل هذه المهام إلى (مختص تصنيف البيانات).

مختص حماية البيانات: هو الشخص المسؤول عن حماية البيانات عبر اتخاذ القرار في استخدام الضوابط الأمنية المتناسبة مع التصنيف، وغالباً ما يكون هذا الشخص من إدارة تقنية المعلومات والذي لديه الخبرة التقنية والاطلاع اللازم بأفضل الممارسات المتبعة في تطبيق الضوابط الأمنية وحماية البيانات في مراحلها المختلفة طبقاً للسياسات والمعايير المتبعة.

مستهلك أو مستخدم البيانات: هو الشخص الذي يقوم بالتعامل مع البيانات واستخدامها ومعالجتها حسب سير الأعمال الموكل إليه، ويجب أن يكون على دراية واطلاع كافٍ و مسؤولاً على الالتزام بالطريقة المثلى لاستخدام وحماية البيانات حسب السياسات المتبعة في المؤسسة والالتزام بما يوكل إليه من مهام خلال مراحل إدارة البيانات وعدم تعريضها للمخاطر المحتملة.

مختص تصنيف البيانات: هو شخص متدرب ولديه القدرة على فهم بيانات العمل وتوكل إليه مهام مساعدة الأقسام المختلفة في المؤسسة لتوفير الدعم الخاص بتنصيف البيانات تماشياً مع استراتيجية المؤسسة وسياستها المتبعة. غالباً ما يكون شخصاً من نفس وحدة الأعمال التي ينتمي لها مالك البيانات، لذلك يكون عليه القدرة على فهم بيانات العمل وتحديد قيمتها وتصنيفها.

مدقق البيانات: هو الشخص المسؤول عن مراجعة تصنيف البيانات وتحديد ما إذا كانت تتماشى مع متطلبات العمل والشؤون التنظيمية والامتثال وغيرها. كما ينظر إلى الضوابط الأمنية والحلول التكنولوجية المقدمة لتطبيقها والنظر في تطويرها وتحسينها. يستعرض مدقق البيانات أيضاً المقترحات الواردة من مستخدمي البيانات ويقيم المواءمة بين الاستخدام الفعلي للبيانات وسياسات وإجراءات معالجة البيانات الحالية. ومن الغالب أن ينتمي هذا الشخص إلى الوحدات الإدارية الخاصة بالحوكمة المؤسسية وإدارة الجودة.

9 شروط السياسة

من خلال هذه السياسة، تعرف الوكالة الوطنية للأمن السيبراني النهج الوطني لتصنيف البيانات لاستخدامه في مؤسسات الدولة. تسري هذه الشروط والأحكام كشروط معيارية متعلقة بمتطلبات الامتثال.

1- تحدد هذه السياسة مستويات التصنيف في المؤسسات الحكومية و هي خمسة (5) مستويات . بالنسبة للمؤسسات غير الحكومية ، يجب أن تحدد أربعة (4) مستويات تصنيف كحد أدنى.

2- بالاتساق مع مستويات التصنيف، يجب على المؤسسات استخدام وسوم تصنيف البيانات، وهي: C0 عام، C1 داخلي ، C2 محدود الوصول، C3 سري، C4 سري للغاية.

3- C1يمثل التصنيف الافتراضي للبيانات غير المصنفة والذي يوازي المسمى: (داخلي)

4- يجب على المؤسسات حماية البيانات بناءاً على تصنيفها، والذي يشمل المحددات: السرية، النزاهة، التوفر

5- يجب استخدام المبادئ الرئيسية لتصنيف البيانات والمذكورة في الفصل الرابع من هذا المستند كمرجعية استرشادية للوصول إلى التصنيف الأمثل للبيانات

6- يجب على المؤسسات إدارة بياناتها بالالتزام بمفهوم المرحلية أو دورة حياة البيانات، والتأكد من تطبيق العمليات والإجراءات المناسبة لتسهيل ذلك.

7- بالاتساق مع هذه السياسة، يجب على المؤسسات أن تصدر سياسة داخلية تستند إلى الالتزام بنهج تصنيف البيانات المذكور في هذه السياسة.

8- يجب على كل مؤسسة تحديد شخص يقوم بمهام (كبير مسؤولي البيانات) والذي يكون مسائلاً عن حوكمة وإدارة البرنامج الخاص بتصنيف البيانات.

9- يجب على (كبير مسؤولي البيانات) التأكد أن برنامج تصنيف البيانات داخل المؤسسة يتضمن التالي:

أ- الحصول على الدعم والالتزام من الإدارة العليا في المؤسسة

ب- القيام بتحقيق التوقعات المطلوبة من أصحاب العمل في حماية البيانات بالطرق المثلى

ت- أن يكون ملتزماً بنشر الوعي ونقل الخبرات والمهارات الضرورية لبيئة العمل حول تصنيف البيانات

ث- أن يقيّم الحلول التكنولوجية اللازمة لتسهيل تبني برنامج نهج تصنيف البيانات ونجاحه

ج- تطبيق أدوات الحوكمة الضرورية لتسهيل تبني وتطبيق برنامج نهج تصنيف البيانات، والتواصل مع الأطراف ذات الصلة لتوزيع الأدوار والمسؤوليات داخل المؤسسة

10- بإمكان (كبير مسؤولي البيانات) التواصل مع الإدارة المختصة في الوكالة الوطنية للأمن السيبراني حول التحديات المتعلقة ببرنامج تصنيف البيانات في المؤسسة.

11- تعتبر شؤون الحوكمة والضمان السيبراني الوطني هي الإدارة المختصة في الوكالة الوطنية للأمن السيبراني والمسؤولة عن هذه السياسة.

1.10 الامتثال والالتزام

تضع السياسة الأساس لتنفيذ نظام إدارة أمن المعلومات داخل المؤسسة، وسيتم استكمالها بمعيار تأمين المعلومات الوطنية V2.1 الذي يحدد ضوابط الأمان ذات الصلة التي تحتاج المؤسسات إلى تنفيذها بناءً على التصنيف الأمني للبيانات.

2.10 الفترة الانتقالية والتاريخ الفعلي للتنفيذ

- **1.2.10 التاريخ الفعلي للتنفيذ**

تصبح السياسة سارية عند نشرها على القنوات الرسمية للوكالة الوطنية للأمن السيبراني.

- **2.2.10 الفترة الانتقالية**

بالنسبة للمؤسسات التي تندرج تحت نطاق تطبيق هذه السياسة، سوف تمنح مهلة (6 شهور) من تاريخ نشر هذه السياسة ، لتقوم برسم خارطة الطريق للامتثال لهذه السياسة.

3.10 الاستثناءات

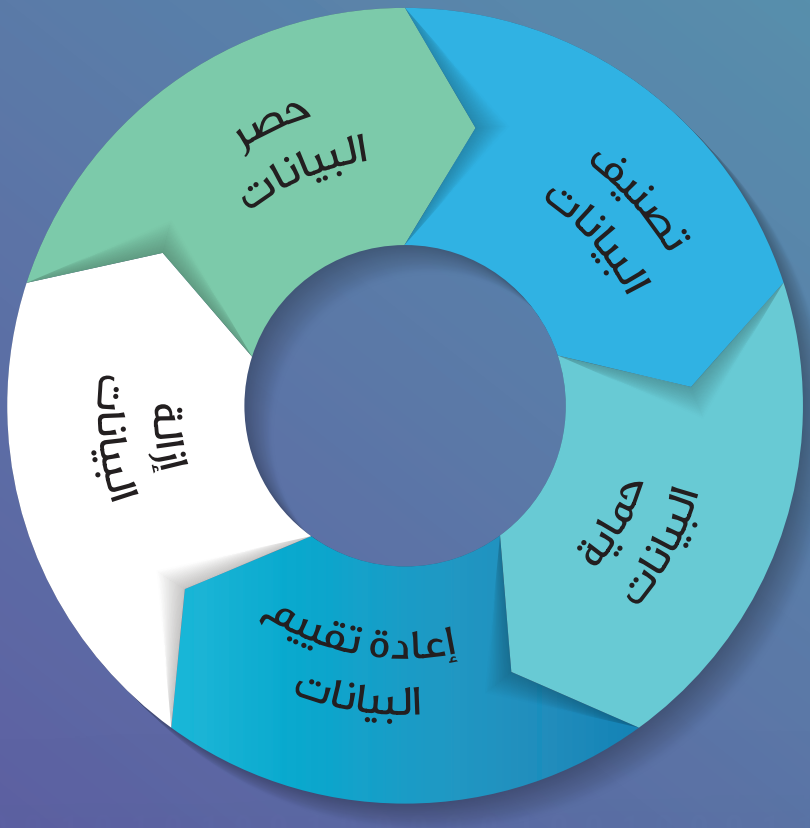
- 1.3.10 يسري نطاق تطبيق هذه السياسة على المؤسسات، وبالتالي يجب عليها أن تقوم بالعمل على تصنيف بياناتها بناءاً على نهج تصنيف البيانات.
- 2.3.10 أي اختلاف عن هذه السياسة يجب أن يتم فيه مخاطبة الوكالة الوطنية للأمن السيبراني ، عن طريق وسائل المراسلات الرسمية ، يتم فيه شرح الأسباب ووجهات النظر بالإضافة إلى خطة إدارة المخاطر والتي تم فيها تحديد المخاطر، وتحليلها وكيفية معالجتها ، وإثبات أنها قد تمت الموافقة عليها من قبل الإدارة العليا لدى المؤسسة. بناءاً على ذلك، ستقوم الإدارة المعنية في الوكالة الوطنية للأمن السيبراني بموافاة المؤسسة بتقييم طلب الاستثناء ، وبالتنسيق مع منظم القطاع (إن توفرت الشروط).

الملحق (أ) :
مراحل إدارة البيانات

تعد دورة حياة البيانات غير ثابتة إذ قد تتغير قيمة البيانات مع مرور الوقت وفي بعض الأحيان قد تفقد قيمتها تماماً مما يؤدي الى الحاجة الى التخلص منها.

أهم مراحل دورة حياة البيانات :

- حصر البيانات
- تصنيف البيانات
- حماية البيانات
- إعادة تقييم البيانات
- إزالة البيانات



رسم توضيحي 3: مراحل(أو دورة حياة) البيانات

المرحلة الأولى : حصر البيانات

تتكون عملية حصر البيانات من خطوتين:

أ- معرفة مصدر البيانات

ب- إنشاء سجل للبيانات (جرد البيانات)

أ. معرفة مصدر البيانات

لمعرفة مصدر البيانات، سيكون من الضروري معرفة العمليات المؤسسية والخدمات والمسؤوليات. ومن ثم معرفة تدفق البيانات خلال سير هذه العملية، ع طريق معرفة المدخلات، وكيفية معالجة البيانات خلال العمليات المؤسسية. كما سيكون من الضروري معرفة أين تتم معالجة البيانات أو تخزينها، ومن الغالب أن مصدرها يكون ضمن ثلاثة طرق:

إنشاء البيانات: يعد إنشاء البيانات هو انشاء أي مستند أو سجل من الصفر. على سبيل المثال إنشاء ملف word أو كتابة ايميل و غيره

معالجة البيانات: هو معالجة أي سجل عن طريق تطبيق أو نظام. على سبيل المثال: إنشاء تقرير شهري للحضور والانصراف أو وصل الراتب بناءً على سجل الحضور والانصراف، الرد على رسالة البريد الالكتروني، تنبيه تم إنشاءه بواسطة نظام ما بناءً على مدخلات وغيرها.

استلام البيانات: هو استقبال البيانات من مصدر بيانات خارجي على سبيل المثال استقبال ملفات عن طريق USB أو أجهزة ترسل مدخلات الى خادم رئيسي كإرسال السجلات من نظام الحضور والانصراف إلى نظام الرواتب.

ب. إنشاء سجل للبيانات (جرد البيانات)

تعد هذه العملية بمثابة اجراء مسح للبيانات التي تمتلكها المؤسسة. وكما هو الحال مع أي جرد فيتم تسجيل ملكية أصول البيانات بما في ذلك العمليات والأنظمة المرتبطة بها.

المرحلة الثانية : تصنيف البيانات

وتتم عن طريق خطوتين رئيسيتين:

1- تحديد قيمة البيانات وتأثيرها على سير الأعمال في المؤسسة وبالتالي تصنيفها بناء على منهجية تصنيف البيانات.

2- تحديد وسوم تصنيف البيانات بناءاً على مستوى السرية المطلوب.

المرحلة الثالثة: حماية البيانات

وذلك عن طريق تطبيق الخطط ومنهجيات العمل اللازمة لحماية البيانات ، وتطبيق الضوابط الأمنية سواءاً الإدارية منها أو التقنية اللازمة حسب ما يتناسب مع تصنيفها.

المرحلة الرابعة: إعادة تقييم البيانات

من الطبيعي أن تتغير قيمة البيانات من وقت لآخر بناءً على عدة عوامل منها: وقت المعالجة، الحق في الاستخدام، التوافق مع طبيعة العمل وغيرها من الامور. وهذا من شأنه أن يؤثر على تصنيف البيانات.

يجب القيام بإعادة التقييم والتحقق من صحة تصنيف البيانات من وقت لآخر وعلى الأقل مرة واحدة سنوياً أو عند نهاية فترة الاحتفاظ بالبيانات.

يجب اتخاذ إجراءات تصحيحية من حيث الضوابط المطبقة بناءً على إعادة التقييم.

المرحلة الخامسة: التخلص من البيانات

عادة ما يتم التخلص من البيانات في حالتين:

- نهاية دورة حياة البيانات: لا ينصح بالاحتفاظ بالبيانات للأبد فبمجرد أن تخدم البيانات الغرض المطلوب منها ينبغي التخلص منها وإزالتها بعد التشاور مع الشؤون القانونية في المؤسسة والتي تحدد سياسة الاحتفاظ بالبيانات مع الأخذ بعين الاعتبار أي متطلبات قانونية وتنظيمية وتعاقدية قد تكون موجودة.
- المتطلبات القانونية: في بعض الأحيان يكون هناك متطلب قانوني يلزم إزالة البيانات من الأنظمة مثل:
    - طلبات المستخدمين: بناءً على عدة قوانين وخصوصاً فيما يتعلق بقوانين حماية خصوصية البيانات الشخصية ، يحق للمستخدمين طلب إزالة بياناتهم الشخصية من الأنظمة ، وتخضع هذه العملية للقوانين المعمول بها.
    - طلبات إزالة: عن علم أو غير علم، قد يكون لدى المؤسسة معلومات غير قانونية أو غير مرخصة أو محمية بحقوق الطبع والنشر داخل أنظمتها مما يشكل خرقاً للقانون ويجب إزالتها بأثر فوري.

على المؤسسة إجراء تقييم وتنفيذ للضوابط عند الحاجة وأخذ الموافقات المطلوبة قبل إعادة تصنيف البيانات. كما على المستخدمين معرفة وممارسة أساليب التخلص الآمن للبيانات.

الملحق (ب):
النهج العام لتنفيذ برنامج تصنيف البيانات

ستكون سياسة تصنيف البيانات قابلة للتطبيق ويتم تنفيذها على كافة المؤسسة. وعلى الرغم من أنه يجب تنفيذ خطوات معينة في البداية عبر المؤسسة، عندما يتعلق الأمر بالتنفيذ الفني للضوابط، فقد تكون هناك حاجة إلى تنفيذ ممارسات معينة مختلفة عن السياق في نطاقات فرعية محددة. فيما يلي نهج عالي المستوى يمكن استخدامه كخطوات استرشادية من قبل المؤسسات لتصميم وتنفيذ برنامج تصنيف البيانات داخل مؤسستها.

الخطوة 1: التزام الإدارة: تحتاج الإدارة إلى إنشاء برنامج تصنيف البيانات رسميًا داخل مؤسستها.

الخطوة 2: تحتاج الإدارة إلى تعيين شخص «كبير مسؤولي البيانات» يتمتع بالمهارات المناسبة وفهم الأعمال يحتاج إلى امتلاك البرنامج وإدارته.

الخطوة 3: تحتاج الإدارة إلى توفير الموارد اللازمة (الأموال والأشخاص) للبرنامج.

الخطوة 4: سيحدد «كبير مسؤولي البيانات» خارطة الطريق لتنفيذ برنامج تصنيف البيانات داخل المنظمة بما يتماشى مع هذه السياسة.

الخطوة 5: سيضع «كبير مسؤولي البيانات» الحوكمة اللازمة لتنفيذ هذا البرنامج. وهذا يشمل، من بين أمور أخرى، السياسات والإجراءات اللازمة وتخصيص الأدوار والمسؤوليات.

الخطوة 6: سيقوم «كبير مسؤولي البيانات» بإنشاء برنامج لبناء الوعي والمهارات داخل المؤسسة.

الخطوة 7: سيقوم «كبير مسؤولي البيانات» بتقييم التقنيات المناسبة لتسهيل اعتماد سياسة تصنيف البيانات داخل المنظمة، بالتعاون مع مختص حماية البيانات.

الخطوة 8: اعتمادًا على حجم المؤسسة / العمل، يمكن تقسيم التنفيذ الفني إلى نطاقات لتسهيل التنفيذ.

الخطوة 9: من المهم أن يركز التنفيذ على العمليات والوظائف الهامة الخاصة بك ، وعلى هذا النحو يجب على المؤسسات إجراء تحليل تأثير الأعمال (BIA) لتحديد العمليات / الوظائف الحاسمة داخل المؤسسة. يجب إعطاء الأولوية لهذه العمليات / الوظائف الحاسمة على العمليات المؤسسية غير الأساسية الأخرى.

الخطوة 10: تحديد نطاق البرنامج.

الخطوة 11: ضمن النطاق المحدد، يتم تحديد أصول البيانات ذات الصلة و بإنشاء جرد للأصول .عملية اكتشاف البيانات OBASHI ، هي إحدى المنهجيات التي يمكن أن تساعد في هذا التمرين.

الخطوة 12: بالنسبة لأصول البيانات المحددة، يتم إجراء تمرين تصنيف البيانات. سيساعد هذا في فهم الأهمية العامة للبيانات، وعلامة تصنيف البيانات ذات الصلة.

الخطوة 13: استخدام التكنولوجيا اللازمة لتسهيل وسم تصنيف البيانات.

الخطوة 14: النظر إلى المتطلبات الأمنية العامة للبيانات وتنفيذ الضوابط اللازمة بناءً على معيار تأمين المعلومات الوطني V2,1

الخطوة 15: تنفيذ العمليات، لإعادة تقييم تصنيف البيانات وإعادة تقييم البيانات من وقت لآخر بناءً على محفزات الأعمال ذات الصلة.

الملحق (ج):
تحليل تأثير الأعمال

لتحديد الأولويات الخاصة بتصنيف أصول المعلومات والمستوى المقابل من الحماية الأمنية، ينبغي إجراء تقييم للأثر بالوسائل المقترحة. ومع ذلك، إذا كان لدى المؤسسات أسلوب لتقييم الأثر على سير العمل، يمكن استخدام ذلك الأسلوب بدلاً من الأسلوب المنصوص عليه بهذا الملحق.

يتم إجراء تحليل الأثر على العمل ، عن طريق تقييم أثر فقدان أو تدهور العملية على المؤسسات من خلال عوامل التأثير التالية:

- الأثر على السمعة.
- الأثر الخارجي (الأثر على الهيئات الخارجية والمؤسسات وغيرها).
- الأثر الداخلي (الأثر على الموظفين والمؤسسات ذاتها).
- الأثر القانوني (المسؤوليات الناجمة عن عدم الوفاء بالالتزامات القانونية، وعلى سبيل المثال، عدم الالتزام للاتفاقيات واللوائح والتشريعات الخاصة بمستوى خدمة.. إل).
- الأثر الاقتصادي(خسائر الإيرادات المباشرة والفرص الاقتصادية الضائعة.. إلخ).

ينبغي اتخاذ الخطوات التالية لتقييم مدى أهمية العمليات:

1. تقييم مدى أهمية كل عامل من عوامل الأثر لدى المؤسسات اعتماداً على التصنيف أدناه. ويتم حساب عامل التقييم هذا (a 1 to a5) مرة واحدة فقط ويتم استخدامه في كل عملية يتم تقييمها. يتم تحديد قيمة عامل التقييم من منظور المؤسسة.

0 ◂	غير هام
1 ◂	منخفض الأهمية
2 ◂	متوسط الأهمية
3 ◂	شديد الأهمية
4 ◂	شديد الأهمية للغاية

2. لكل عملية يجب أن يتم تحديد الأثر ويُرمز إليه بالرمز (I) على الموسسات فور تعرضها للخسائر أو التدهور من خلال استخدام المقياس أدناه. و فيما يتعلق بالعمليات القائمة على عنصر الوقت يجب التأكد من حساب الأثر في أوقات ذروة الاستخدام. يتم تحديد درجة قياس الأثر من منظور الوحدة الإدارية المسؤولة عن العملية المؤسسية.

0 ◂	لا يوجد تأثير
1 ◂	تأثير ضئيل
2 ◂	تأثير متوسط
3 ◂	تأثير كبير
4 ◂	تأثير كبير للغاية

استخدام المعادلة التالية لتحديد مدى الأهمية (وفقاً لمقياس حتى 100) لكل عملية:

قيمة التأثير = 1.25 (α1I1 +α2I2 +α3I3 +α4 I4 +α5I5)

مثال عملي

3. عمليات تقييم عوامل التأثير التنظيمية:

1.	تقييم الأثر على السمعة: شديد الأهمية (α1=3)
2.	تقييم الأثر الخارجي: شديد الأهمية (α2=3)
3.	تقييم الأثر الداخلي: متوسط الأهمية (α3=2)
4.	تقييم الأثر القانوني: شديد الأهمية للغاية (α4=4)
5.	تقييم الأثر الاقتصادي: متوسط الأهمية (α5=2)

4. اسم العملية: حساب رواتب العاملين والأثر في الأوقات الهامة

1.	الأثر على السمعة: تأثير كبير (I1=3)
2.	الأثر الخارجي: تأثير ضئيل (I2=1)
3.	الأثر الداخلي: تأثير كبير (I3=3)
4.	الأثر القانوني: تأثير منخفض (I4=1)
5.	الأثر الاقتصادي: لا يوجد تأثير (I5 = 1)

قيمة التأثير = 1.25 (2x1 +4x1 + 2x3 + 3x1 + 3x3)

نتحصل من المعادلة اعلاه على قيمة التأثير و هي : 30

www.ncsa.gov.qa

هاتف: 16555 | فاكس: 2362080

البريد الالكتروني: info@ncsa.gov.qa | الرمز البريدي: 24100 الدوحة - قطر

تابعونا على