وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

إعداد:
م/ صـــادق الصوفي

5

Data Classification

سياسة تصنيف وحساسية المعلومات

1 بنود السياسة

2 محتويات إعداد السياسة

2.1 النطاق

2.2 الأهداف

2.3 عمليات تصنيف البيانات

2.4 مراحل إدارة البيانات

2.5 الأدوار والمسئوليات

بنود السياسة

- تتضمن المعلومات المعنية في خطة أمن المعلومات لأي جهة حكومية كافة المعلومات التي يتم حفظها أو تبادلها بشتى الوسائل، سواءً كانت إلكترونية أو غير إلكترونية، مثل المعلومات المكتوبة، أو تلك التي يتم تبادلها مشافهةَ مثل الهاتف أو بشكل مرئي مثل الاجتماعات المرئية والمسموعة .
- على الجهة الحكومية وضع معايير شاملة تتضمن تفاصيل مواردها المعلوماتية بهدف تحديد أهميتها وحساسيتها وآثارها القانونية، ووضع خطة التصنيف المتبعة بالتوافق مع هذه السياسة.
- يجب وضع تصنيف لجميع المعلومات المملوكة للجهة الحكومية وتوضيح مدى حساسية وأهمية كل صنف، ووضع آلية تتم فيها إدارة المعلومات بشكل صحيح ابتداءً من مرحلة إنشائها، مروراً بالاستخدام المرخص لها، وانتهاءً بالطريقة الصحيحة لإتلافها بحيث تتناسب هذه الالية مع مستوى التصنيف.

سياسة تصنيف وحساسية المعلومات

بنود السياسة

- الجهة الحكومية مسئولة عن تصنيف المعلومات، ويتم تصنيفها إلى أربعة مستويات وهي:

أ) المستوى الأول: المعلومات العادية

- هي معلومات قليلة الحساسية، لا يؤثر الإفصاح عنها على خصوصية أو أمن الجهة الحكومية أو أي من المتعاملين معها مثل الموظفين والعملاء والشركاء، أو تؤدي إلى (الاضرار /إيذاء) أي من المصالح السياسية أو الاقتصادية أو غيرها، وتكون عادة متاحة للنشر عبر وسائل الاتصال والإعلام.
- لا توجد صلاحيات أو تحديدات على هذا النوع من التصنيف

بنود السياسة

ب) المستوى الثاني: المعلومات المحدودة

- هي معلومات حساسة معدة للاستخدام الرسمي، وإذا ما تم الإفصاح عنها فإنها يمكن أن تعرض خصوصية وأمن الجهة الحكومية أو أي من المتعاملين معها للخطر، وبالتالي فإن الإفصاح غير المرخص عن المعلومات المحدودة يمكن أن يؤثر سلباً على الثقة بالموظفين والمواطنين، مثل البريد الإلكتروني غير المشفر، والتعميمات والمذكرات الداخلية، والمعلومات التي يتم وسمها بطريقة تعكس محدوديتها، مثل" لاستخدام الجهة فقط ."
- يجب على الجهة وضع وإعلان التعليمات المناسبة للكشف عن هذه المعلومات قبل تقديمها لأي جهات خارجية.
- يتم تصنيف المعلومات الشخصية على أنها" محدودة "ما لم تحدد تعليمات الجهة الحكومية غير ذلك

بنود السياسة

ج) المستوى الثالث: المعلومات السرية

- معلومات حساسة معدة للاستخدام الرسمي المحدود، وإذا تم الإفصاح عنها فإنها ستعرض أمن وخصوصية الجهة الحكومية والمتعاملين معها للخطر، أو تسبب لهم ضرراً سياسياً أو اقتصادياً أو نحو ذلك، مثل المعلومات التي من المتوقع أن تكون مفيدة لبلدان أجنبية أو جهات غير حكومية، والمعلومات المستثناة من الإفصاح عن المعلومات العادية والمحدودة.
- إن تصنيف المعلومات على أنها "أو" سرية للغاية "يجب ألا يتم بشكل عشوائي، وإنما يجب أن يكون حسب التعليمات والأنظمة والقوانين.
- إن مسئول المعلومات في الجهة الحكومية المخول الوحيد وله صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات وبموافقة قيادة الجهة.

سياسة تصنيف وحساسية المعلومات

بنود السياسة

د) المستوى الرابع: المعلومات السرية للغاية

- هي المعلومات التي تعتبر غاية في الحساسية والأهمية للجهة الحكومية، والتي تعرض أمنها وخصوصيتها والمتعاملين معها للخطر الشديد، أو تلك المعلومات المعدة للاستخدام من قبل جهات معنية، ويمكن أن يؤدي الإفصاح عنها بشكل غير مرخص إلى تهديد حياة الأشخاص، أو أضرار مادية أو معنوية للجهة أو المتعاملين معها، أو يسبب ضرراً جسيماً بالمصلحة القومية للبلد ويعرض أمن الدولة للخطر، بالإضافة إلى المعلومات التي يترتب الإفصاح عنها بشكل غير مرخص إلى مسائلات قانونية، مثل معلومات الحسابات الشخصية، والتحقيقات الجارية، ومعلومات تتعلق بأمن الدولة، والمعلومات ذات الأهمية الاستخباراتية أو العسكرية.

- إن مسئول المعلومات في الجهة الحكومية وحده له صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات وبموافقة قيادة الجهة.

بنود السياسة

- يجب أن تتوافق عملية حفظ المعلومات مع مستويات تصنيفها، فيجب حفظ جميع وسائط التخزين في مكان آمن حسب تصنيف المعلومات المخزنة فيها، فمثلاَ: (حفظ المعلومات العادية دون الحاجة إلى تطبيق إجراءات أمنية صارمة، في حين يجب حفظ المعلومات" السرية" و"السرية للغاية" بطريقة صحيحة محمية من أي تهديدات أو أخطار ومن الوصول إليها أو تداولها بشكل غير مرخص).

- يجب تداول المعلومات في الجهة الحكومية بطريقة تضمن حمايتها من الوصول إليها أو الإفصاح عنها أو تغييرها بشكل غير مرخص أو فقدانها، ولهذا، فإنها يجب أن تعالج وتحفظ حسب مستويات تصنيفها في سبيل حماية سريتها ومستوى حساسيتها وسلامتها وإتاحتها.

سياسة تصنيف وحساسية المعلومات

بنود السياسة

- على الجهة الحكومية وضع التعليمات الخاصة بإتلاف المعلومات عند الحاجة إلى ذلك بطريقة تتوافق مع مستوى تصنيفها وبطريقة تتوافق مع القوانين والتشريعات الحكومية والأحكام والأنظمة والتعليمات السارية .
- يجب تخزين جميع المعلومات" السرية للغاية "في مكان معزول وآمن، ويجب عزل جميع المعلومات ضمن تصنيفاتها بطريقة فيزيائية أو إلكترونية حسب مستوى حساسيتها.

النطاق

تسري هذة السياسة على كافة المعلومات التي يتم حفظها أو تبادلها بشتى الوسائل، سواءً كانت إلكترونية أو غير إلكترونية، مثل المعلومات المكتوبة، أو تلك التي يتم تبادلها مشافهةَ مثل الهاتف أو بشكل مرئي مثل الاجتماعات المرئية والمسموعة .

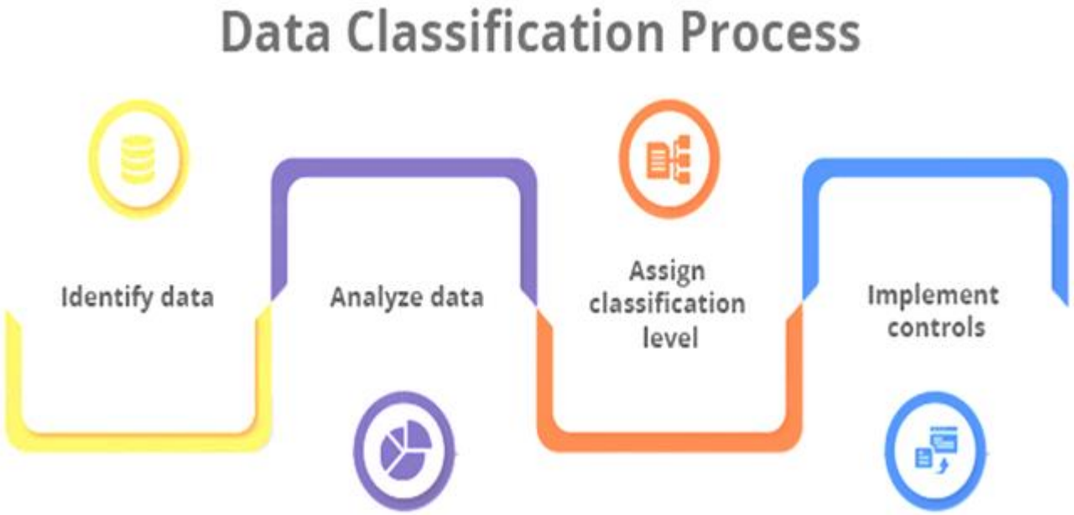
كما تسري هذه السياسة على جميع موظفي الجهة والأطراف الخارجية ذات العلاقة.

الهدف

- حماية المعلومات من خلال تحديد تصنيف المعلومات حسب حساسيتها وكيفية ومدى نشرها.
- الحفاظ على خصوصية وسلامة وتوفر المعلومات
- تحسين قدرات الجهة على حماية بياناتها من الهجمات الإلكترونية

سياسة تصنيف وحساسية المعلومات

عمليات تصنيف المعلومات



تتكون عملية تصنيف البيانات من الخطوات التالية:

- **تحديد البيانات**: تتضمن هذه الخطوة تحديد البيانات التي تحتاج إلى تصنيف. وذلك بفهم نوع البيانات وقيمتها والمخاطر المرتبطة بها.
- **تحليل البيانات**: يعد تحليل البيانات لفهم مستوى حساسيتها جزءًا مهمًا من تصنيف البيانات. تتضمن هذه العملية تحديد متطلبات السرية والنزاهة والتوافر للبيانات.
- **تعيين مستوى التصنيف**: بناءً على التحليل، يتم تعيين البيانات إلى مستوى تصنيف. وذلك وفقًا لحساسية البيانات والمتطلبات التنظيمية وقيمتها.
- **تنفيذ الضوابط**: تتضمن الخطوة الأخيرة تنفيذ الضوابط المناسبة لحماية البيانات بناءً على مستوى التصنيف. وتشمل هذه الضوابط ضوابط الوصول والتشفير والمراقبة.

عوامل تصنيف وحساسية المعلومات

تصنف البيانات بناء على مايلي:

- Confidentiality Classification
- Regulatory Classification
- Value Classification
- Access Classification
- Life Cycle Classification

- **السرية**: حيث يتم التصنيف بناءً على مستوى حساسية البيانات.
- **المتطلبات التنظيمية**: ويتم التصنيف بناءً على المتطلبات التنظيمية

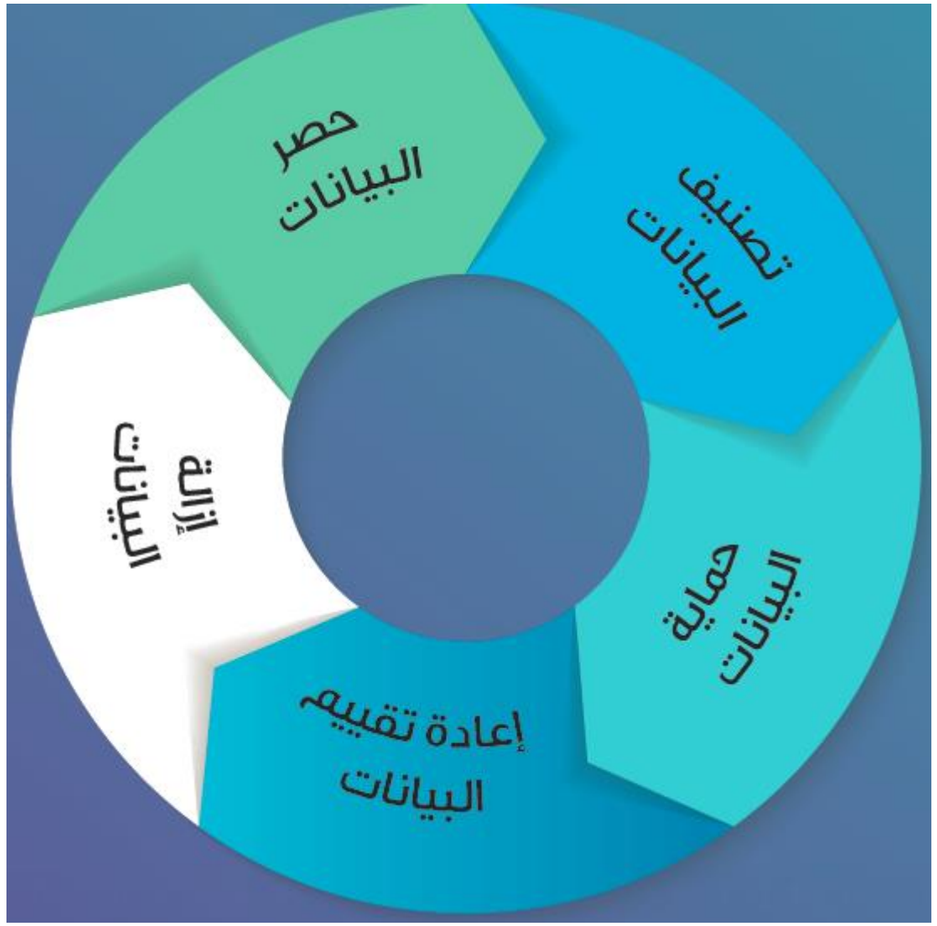
للتعامل مع البيانات.

- **القيمة**: وهنا يتم الصنيف بناءً على قيمة البيانات بالنسبة للجهة.
- **الوصول**: حيث يتم التصنيف بناءً على مستوى الوصول المطلوب للبيانات.
- **دورة الحياة**: ويتم التصنيف بناءً على مرحلة دورة حياة البيانات.

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 تماما مما يؤدي الى الحاجة إلى التخلص منها.
- يتم في البداية حصر البيانات أو استكشافها وجردها، ثم يتم تصنيف البيانات بناءا على قيمتها وعلى مبدأ تحليل المخاطر، ثم يتم تصميم وتحديد الضوابط الأساسية لحماية البيانات طبقا 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.

مراحل إدارة البيانات



أهم مراحل دورة حياة البيانات :

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

تسريب المعلومات السرية للغاية

تسريب المعلومات السرية للغاية يمكن أن يتسبب في وقوع الأضرار التالية:

- **الضرر بالمصالح الوطنية**: يمكن أن تستخدم المعلومات السرية للغاية لأغراض ضارة، مثل التجسس أو الإرهاب.
- **الضرر بالأفراد والجهة**: يمكن استخدام المعلومات السرية للغاية للإضرار بالأفراد أو الجهة، مثل الابتزاز أو التهديد.
- **الضرر بالسمعة**: يمكن أن يؤدي الإفصاح الغير مرخص عن المعلومات السرية للغاية إلى تضرر سمعة الجهة التي تم الإفصاح عنها.
- **التجسس**: يمكن استخدام المعلومات السرية للغاية للحصول على معلومات حول القدرات العسكرية أو الاقتصادية أو الدبلوماسية للدولة.
- **الإبتزاز:** يمكن استخدام المعلومات السرية للغاية لتهديد الأفراد أو الشركات للحصول على المال أو الامتثال لمطالب معينة.
- **الأنشطة الضارة والتخريبية**: يمكن استخدام المعلومات السرية للغاية لشن هجمات أو تهديدات.

الأدوار والمسئوليات

ضابط أمن المعلومات :

- تحديد البيانات الحساسة بناءً على العوامل المحددة في السياسة.
- تحليل البيانات الحساسة لتحديد متطلبات السرية والنزاهة والتوافر.
- تعيين البيانات إلى مستوى تصنيف بناءً على العوامل المحددة في السياسة.
- تنفيذ الضوابط المناسبة لحماية البيانات بناءً على مستوى التصنيف.
- مراجعة البيانات المصنفة بانتظام لضمان دقة التصنيف..

الأدوار والمسئوليات

المستخدمون:

- حماية البيانات التي يمتلكونها أو يتعاملون معها ومن أهم مسئولياتهم:
- الإمتثال لسياسة تصنيف وحساسية المعلومات.
- إستخدام أنظمة وتطبيقات آمنة للوصول إلى المعلومات.
- حماية المعلومات من الضياع أو السرقة.

انتهى