CITRA

الهيئة العامة للاتصالات وتقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

سياسة تصنيف البيانات

دولة الكويت

V2.3

الهيئة العامة للاتصالات وتقنية المعلومات

الفهرس

1. التعريفات

يكون للكلمات والعبارات التالية حيثما وردت في هذه السياسة المعاني المخصصة لها أدناه وتعتمد التعاريف الواردة في قانون الهيئة العامة للاتصالات وتقنية المعلومات رقم 2014/37 ولائحته التنفيذية ولائحة مصطلحات وتعريفات تقنية المعلومات والاتصالات الصادرين عن الهيئة.

المصطلح	التعريف
1.1 البيانات	هي معلومات يتم تحريرها وتعديلها وطباعتها او تخزينها عن طريق الحاسوب، وتكون هذه المعلومات على هيئة ملفات نصية، او صوتية، او صور، او فيديو او على هيئة برامج حاسوبية او معلومات رقمية بلغة يفهمها الحاسوب.
1.2 البيانات الشخصية	والتي تشمل على معلومات او مجموعة من المعلومات إذا ما تم تجميعها يمكن من خلالها الاستدلال بشكل واضح ومباشر لهوية الفرد، كما تشتمل على أية معلومات يمكن ربطها بشكل غير مباشر كبيانات الموقع لشخص معين بصرف النظر عما إذا كانت هوية الفرد واضحة أم لا من تلك المعلومات او من مجموعة من تلك المعلومات وغيرها من المعلومات.
1.3 تصنيف البيانات	هو تصنيف (أو وضع أو ترتيب) للبيانات في مستويات أمنية ملائمة بناء على مدى حساسيتها وذلك لتحديد السبل المثلى لتداولها وحمايتها من المخاطر.
1.4 مالك البيانات	قد يكون فرد، او جهة حكومية، او أحد قطاعاتها، او شركة خاصة، او أحد قطاعاتها، حيث يملك بيانات معينة ولديه الصلاحية لمعالجتها، او تعديلها، او نسخها، او تخزينها (على سبيل المثال لا الحصر قطاع الموارد البشرية يملك بيانات موظفي الجهة، قطاع نظم المعلومات يملك بيانات البنى التحتية وبعض الأنظمة، إدارة الشؤون المالية تملك بيانات الرواتب، إدارة خدمة العملاء تمتلك بيانات المراجعين، قسم التوريدات يمتلك بيانات الشراء، الخ...).
1.5 التشفير	هي عملية تحويل البيانات من نص مقروء إلى نص غير مقروء، وتطبق عملية التشفير سواء أثناء تخزين البيانات أو عند نقلها عبر الشبكات.
1.6 اختراق البيانات	كل ضياع للبيانات، أو سوء استخدام، او تشويش للبيانات، أو الاطلاع لغير المصرح لهم أو الوصول للبيانات لغير المصرح لهم أو التعديل عليها او الإفشاء لغير المصرح لهم.

2. المقدمة

تحدد هذه السياسة منهجية لتصنيف جميع البيانات لدى القطاعين العام والخاص. وانتهاجها يؤدي إلى تحديد المستوى المقبول من الحماية الأمنية، وضمان الالتزام بأفضل الممارسات المقبولة، وتحديد سبل تداولها ونقلها ومعالجتها. حيث إن عدم اتباع أي نظام لتصنيف البيانات وتوفير الحماية اللازمة لكل صنف من شأنه تعريض هذه البيانات للمخاطر الالكترونية المتنوعة كتسريب البيانات، أو التداول الخاطئ لها، أو اختراقها.

2.1 أهداف تصنيف البيانات

2.1.1 **الهدف:** تصنيف البيانات إلى فئات منفصلة يساعد على اتخاذ قرارات أفضل بشأن الوصول إلى البيانات ومعالجتها بما يتناسب مع مستويات تصنيف البيانات الواردة في هذه السياسة، ومما يساهم في مساعدة الجهة الحكومية أو الخاصة على اتخاذ كافة التدابير اللازمة لتعزيز أمن وحماية بياناتهم والبيانات الشخصية للأفراد الموجودة لديهم وبما يتوافق مع متطلبات وخطط المؤسسات والقوانين واللوائح المعمول فيها في دولة الكويت.

2.1.2 **النطاق:** نطاق السياسة يشمل البيانات التي تتم معالجتها او تخزينها او تعديلها او تحويلها عن طريق الحاسوب او الأجهزة الذكية، أي البيانات الرقمية (المهيكلة أو غير المهيكلة)، والتي تقوم الجهات الحكومية والخاصة بإنشاءها وجمعها وصيانتها كجزء من وظائف أعمالها الرسمية واستخدامها او مشاركتها لغرض توفير الخدمات العامة. تتضمن أمثلة البيانات المهيكلة بيانات الأفراد (مثل البيانات الشخصية أو بيانات الشركة)، وبيانات غير العملاء (مثل بيانات البيئة)، والبيانات التنظيمية (مثل الموارد البشرية والتمويل والبيانات المتعلقة بالأصول والمشتريات). تشمل البيانات غير المهيكلة البيانات المستندة الى النصوص (على سبيل المثال لا الحصر مستندات معالج النصوص وشرائح العروض التقديمية والصور ومقاطع الفيديو والتسجيلات الصوتية) وتستثنى البيانات التي تكون على هيئة مستندات تمت طباعتها فإنها تقع خارج نطاق هذه السياسة. أما بالنسبة لصلاحيات عملية طباعة او نسخ البيانات الرقمية فيجب تحديدها بناءً على حساسية تلك البيانات وفق مستوى التصنيف الذي تقع به.

3. سياسة تصنيف البيانات

3.1 نص السياسة

3.1.1 يتعين على مالك البيانات تصنيف بياناته الى أربعة مستويات على الأقل. وتستثنى الجهات ذات الطابع الأمني أو العسكري من التقيد بمستويات التصنيف المحددة في هذه السياسة، حيث تملك الجهات ذات الطابع الأمني أو العسكري الخيار بتصنيف بياناتها بما تراه مناسباً. وإن كان لمالك البيانات نظام تصنيف مختلف فيجب عمل ربط للبيانات المصنفة مع نظام التصنيف الوارد في هذه السياسة.

3.1.2 لمالك البيانات الحرية في اختيار طرق حماية البيانات وفقاً لنظام التصنيف والاحتفاظ وجمع ومعالجة البيانات. كما يجب على مالك البيانات التأكد من توفير الحماية اللازمة لطريقة حفظ البيانات وفقاً لدرجة تصنيفها وخصوصاً تلك المصنفة وفق المستوى الثالث والرابع للحفاظ عليها من الاختراق.

3.1.3 يتعين على مالك البيانات إنشاء والحفاظ على دليل البيانات الخاص به والذي يجب أن يتضمن معلومات ومعايير بيانات التعريف الخاصة ببياناتها بتنسيق موحد. كما يجب تحديث هذا الدليل بشكل دوري.

3.1.4 يتوجب على مالك البيانات تشفير كافة البيانات المصنفة وفق المستوى الثالث والرابع حال نقلها من جهة حكومية لأخرى أو من خلال المواقع التابعة للجهة الحكومية الموزعة جغرافياً في أماكن مختلفة وينطبق ذلك على القطاع الخاص.

3.1.5 يتعين على مالك البيانات التأكد من نقل أو إزالة كافة البيانات المصنفة وفقاً للمستوى الثالث والرابع من مراكز البيانات والخوادم قبل التخلص من التجهيزات الآلية لمراكز البيانات والخوادم المستضيفة لتلك البيانات.

3.1.6 تم تطوير مستويات تصنيف البيانات الواردة في هذه السياسة بناء على أفضل الممارسات والمعايير الإقليمية والعالمية. ولمالك البيانات الحرية في استخدام مستويات تصنيف أخرى إذا كانت تتناسب مع نوعية البيانات التي يحتفظ بها وفقاً لأفضل الممارسات العالمية والمعايير مثل NIST 800-53، NIST SP 800-60، ISO 27001، PCI DSS، HIPAA لضمان صحة وجودة التصنيف.

3.2 ما يجب مراعاته قبل بدء عملية تصنيف البيانات

3.2.1 جمع كافة البيانات والتدقيق عليها واستبعاد أو معالجة البيانات غير الكاملة منها أو المبهمة أو الغامضة.

3.2.2 مراعاة الدقة في فرز ووضع البيانات في مستويات التصنيف وفقاً لهذه السياسة لكي يتم تحديد المخاطر التي تحيط بكل مستوى وتقييم هذه المخاطر لضمان سلامة وحماية تلك البيانات.

3.2.3 تشكيل فريق لتصنيف البيانات برئاسة الإدارة العليا أو من يمثلها، وبعضوية كل من: مدير أمن المعلومات، ومدير إدارة نظم المعلومات والحاسب الآلي بالإضافة الى مدراء الإدارات المختلفة المالكة للبيانات المتوفرة لدى لجهة، سواءً كانت هذه البيانات شخصية وتخص المشتركين أو بيانات تخص الجهة\الشركة ذاتها، حيث يقوم هذا الفريق بتصنيف البيانات في الجهة وترميزها وفقاً لحساسيتها لتتماشى مع ما ورد في هذه السياسة.

3.2.4 بغرض ضمان التطبيق الكامل لتصنيف البيانات ودعم توحيد الإجراءات بين مختلف الجهات، يجب على الجهات القيام بما يلزم نحو وضع خارطة طريق وخطة عمل توضح كيفية قيامها بعملية تصنيف البيانات وفقاً للأربعة مستويات الأساسية الموضحة في هذه السياسة، على أن يتم مراجعة تصنيف البيانات بشكل دوري ثابت داخلياً.

3.2.5 تحديد مجموعات البيانات ذات الأولوية، والتي يتوجب إجراء اللازم لتصنيفها قبل المجموعات الأخرى ذات المستويات الأدنى من حيث الأولوية، حيث تكون الأولوية حسب أهمية البيانات وحساسيتها وقيمتها، ويعتمد ذلك على المستويات الحالية لنضج إدارة البيانات ضمن الجهة، وحجم عمليات الجهة، ومدى أهمية البيانات.

3.2.6 تقع على الجهة الحكومية والخاصة مسؤولية تحديد أدوار ومسؤوليات الأفراد العاملين لديها بما يؤدي الى تطبيق وتفعيل سياسة تصنيف البيانات ضمن نطاقها.

3.2.7 يتم تحديد الأدوار والمسؤوليات لإدارة وتصنيف البيانات وفقًا لتقدير كل جهة حسب ما تراه مناسباً، حيث أن كل جهة تختلف عن الجهات الأخرى من ناحية امتلاكها لبنية تحتية وإجراءات خاصة بإدارة تلك البيانات، ويمكن للجهة أن ترتأي استحداث وظائف جديدة للقيام بهذه الأدوار أو إضافة مسؤوليات على الأدوار الحالية.

3.2.8 عدم المبالغة في درجة حساسية البيانات.

3.3 مستويات تصنيف البيانات

المستوى	الوصف
المستوى الأول: "البيانات العامة"	تشير للبيانات الغير مصنفة المتاحة لعامة الناس أو البيانات غير المحمية من الاطلاع العام بموجب أي قانون أو لائحة أو عقد ولا تتطلب أي تشفير، حيث لا تدل على مالك البيانات أو تمتلك طابع القطاع الحكومي أو القطاع الخاص وتشمل بعض الأمثلة على سبيل المثال لا الحصر: 1. البيانات المفتوحة كالسياسات واللوائح والقوانين والمنشورة على المواقع الإلكترونية، او الجريدة الرسمية، او الصحف اليومية، او المجلات، او غيرها من المنشورات. 2. نماذج الخدمة الذاتية المتاحة للأفراد والمؤسسات 3. البيانات والمعلومات العامة المتاحة للجمهور على المواقع الالكترونية
المستوى الثاني: "بيانات خاصة غير حساسة"	تشير الى البيانات المملوكة للقطاع العام والخاص او على المستوى الشخصي. وهي بيانات خاصة غير حساسة تدل على هوية مالك البيانات ولا يؤدي الافصاح غير المصرح به إلى إلحاق أضرار على خصوصية مالك البيانات، ومن أمثلتها على سبيل المثال لا الحصر: 1. الاسم الأول أو الاسم الأخير 2. المسمى الوظيفي والمهام الوظيفية وصاحب العمل 3. عنوان البريد الإلكتروني 4. الرقم المدني 5. الجنس 6. العمر 7. المؤهل الدراسي 8. الحالة الاجتماعية 9. بيانات الاتصال مثل: رقم هاتف العمل أو رقم الهاتف المحمول أو رقم الهاتف المنزلي 10. العنوان
المستوى الثالث: "بيانات خاصة حساسة"	تشير الى البيانات المملوكة للقطاع العام والخاص او على المستوى الشخصي. وهي بيانات تدل على هوية مالك البيانات وتكون مرتبطة بمحتوى مالك البيانات وقد تشمل جزءاً من البيانات غير الحساسة، ويؤدي الافصاح غير المصرح به عن إلحاق أضرار على خصوصية مالك البيانات، ومن أمثلتها على سبيل المثال لا الحصر: 1. محاضر الاجتماعات وخطط العمل 2. التقارير الداخلية للمشاريع 3. ملفات الدعاوي القضائية وما يصدر فيها من أحكام ابتدائية ونهائية، وقرارات وأوامر المحاكم وكافة الملفات ذات الصلة 4. المذكرات والآراء القانونية الصادرة عن المكاتب القانونية 5. السجلات الطبية 6. البصمة الجنائية والبصمة الوراثية

المستوى الرابع: "بيانات عالية الحساسية"	تشير إلى بيانات خاصة وذات طابع حساس جداً، وقد يكون الإفصاح غير المصرح به عن هذه البيانات يلحق ضررا كبيرا على خصوصية مالك البيانات أو تلك المملوكة للقطاع الحكومي أو الخاص او على المستوى الشخصي للأفراد او على المستوى الوطني، وبالتالي يمكن نشرها لشريحة محددة جداً ممن هم في حاجة إلى النفاذ اليها. كما تحتوي هذه البيانات على متطلبات تشفير عالية وتتطلب أعلى مستويات الحماية والأمن، وتشمل بعض الأمثلة على سبيل المثال لا الحصر: 1- مفتاح التشفير 2- الوثائق السياسية أو المفاوضات الدولية أو العلاقات الدولية 3- المعلومات الحساسة ذات الطبيعة العسكرية أو المتعلقة بأمن الدولة

3.4 المهام والمسؤوليات

3.4.1 مهام ومسؤوليات جهات القطاع العام والقطاع الخاص المالكة لبياناتها أو بيانات الأفراد

على جميع جهات القطاع العام والخاص أخذ الجدول التالي بعين الاعتبار حين القيام بتصنيف بياناتها وبيانات الأفراد الشخصية التي لديها.

المستوى	الوصف
الإدارة العليا	1. تعميم هذه السياسة على العاملين لدى الجهة بمختلف قطاعاتها والتأكد من فهمهم لمحتواها ومعالجتهم لبيانات الجهة بما يتناسب مع هذه السياسة. 2. يتعين على الجهة\الشركة تشكيل فريق لتصنيف البيانات برئاسة الإدارة العليا أو من يمثلها، وبعضوية كل من: مدير أمن المعلومات، ومدير إدارة نظم المعلومات والحاسب الآلي بالإضافة الى مدراء الإدارات المختلفة المالكة للبيانات المتوفرة لدى لجهة، سواءً كانت هذه البيانات شخصية وتخص المشتركين أو بيانات تخص الجهة\الشركة ذاتها، حيث يقوم هذا الفريق بتصنيف البيانات في الجهة وترميزها وفقاً لحساسيتها لتتماشى مع ما ورد في هذه السياسة. 3. توجيه العاملين لدى الجهة للإبلاغ على الفور عن أي اخلال في التطبيق لهذه السياسة. 4. تسجيل ذلك الإخلال وعمل اللازم لتصحيحه. 5. اعتماد التصنيف المقدم من مالك البيانات التابع للجهة ذاتها. 6. مراقبة وتأكد امتثال جهتهم مع ما ورد في هذه السياسة ومع الدليل الإرشادي لتصنيف ومناولة البيانات في حال صدوره من قبل الهيئة العامة للاتصالات وتقنية المعلومات. 7. تحديد ضابط اتصال للتواصل وتزويد الجهاز المركزي لتكنولوجيا المعلومات بتقارير ربع سنوية بصفته المشرف على تنفيذ اللوائح والسياسات الصادرة عن الهيئة بشأن مدى تطبيق هذه السياسة.
مالك البيانات	1. مشاركة فريق تصنيف البيانات المذكور أعلاه بتصنيف البيانات المملوكة وفقاً لما ورد في هذه السياسة.

	2. تحديد المخاطر المحيطة بالبيانات وتحديد السبل المثلى لحمايتها وأخذ الدعم اللازم من إدارة نظم المعلومات لدى الجهة لتوفير البيئة الآمنة لاستضافتها. 3. عمل مراجعات وتقييمات دورية للبيانات المصنفة والتعديل عليها إذا لزم الأمر.
إدارة نظم المعلومات	1. دعم الجهة على تطبيق السياسة عن طريق توفير التقنيات التي تمكن مالكي البيانات لدى الجهة من تصنيف بياناتهم. 2. توفير البنية التحتية المناسبة ومعايير الأمن لتمكين تصنيف وحماية البيانات حسب متطلبات مستويات التصنيف الواردة في المادة 3.3 من هذه السياسة.

3.4.2 مهام ومسؤوليات الهيئة العامة للاتصالات وتقنية المعلومات

3.4.2.1 اصدار اللوائح التنظيمية والسياسات والارشادات المتعلقة بتكنولوجيا المعلومات والاتصالات.

3.4.2.2 مراقبة القطاعين العام والخاص لتطبيق السياسات والإرشادات الصادرة عن الهيئة للحرص على الامتثال لها.

3.4.2.3 طلب تقارير دورية من الجهاز المركزي لتكنولوجيا المعلومات لمعرفة مدى امتثال الجهات الحكومية لما ورد في هذه السياسة، حيث تحتوي التقارير على المعلومات التالية:

- دليل يوضح نوع البيانات المتوفرة والمستضافة لدى الجهة، والذي يجب أن يتضمن معلومات ومعايير بيانات التعريف الخاصة ببياناتها بتنسيق موحد.
- ما يوضح مستويات التصنيف المعتمدة والمتبعة لدى الجهة حسب البيانات المتوفرة لديها، مع توضيح الأسس والمعايير المتبعة لوضع مستويات التصنيف.
- ما يوضح طرق حماية البيانات والتشفير وفقاً لنظام التصنيف المتبع عند حفظ وجمع ومعالجة البيانات.
- ما يوضح موقع حفظ البيانات تبعاً لمستويات التصنيف.
- ما يوضح خارطة الطريق لتصنيف البيانات مع خطط العمل وعمليات التشغيل في الجهة لضمان التأكد من دقة وجودة تصنيف البيانات .
- تقرير دوري مرحلي لمدى الإنجاز وفق خطط العمل المتبعة لتوفيق الأوضاع حسب هذه السياسة.

3.4.2.4 التنسيق مع الجهاز المركزي لتكنولوجيا المعلومات لوضع خطة تنفيذية خلال مدة لا تتعدى 3 أشهر من دخول السياسة حيز التنفيذ لتمكين تطبيق السياسة مع الجهات الحكومية، على أن يتم توفيق أوضاع الجهات الحكومية وفق هذه السياسة خلال مدة لا تتعدي عامين.

3.4.2.5 عقد ورش العمل لنشر الثقافة ومساعدة الجهات على تطبيق السياسات والارشادات الصادرة عن الهيئة العامة للاتصالات وتقنية المعلومات.