

سياسة إدارة البيانات

النسخة : 1.0.1

التاريخ : أبريل 2015

المرجع : P001



إخلاء المسؤولية / الحقوق القانونية

قامت وزارة المواصلات والاتصالات بتصميم وإعداد هذا المنشور بعنوان سياسة توثيق الخدمات الإلكترونية ومرجع P001 (المشار إليه فيما يلي باسم "العمل")، والذي يعد في المقام الأول مصدرًا استرشاديًا للجهات الحكومية، والعاملين بالإدارة العليا وإدارة تكنولوجيا المعلومات وإدارة المخاطر وتكنولوجيا المعلومات وأخصائيي إدارة تكنولوجيا المعلومات وأمن تكنولوجيا المعلومات في دولة قطر.

تم إعداد وثيقة "العمل" وفقًا لقوانين دولة قطر، ولا يجوز استخدامها لدعم أي حق نيابة عن أي شخص أو كيان ضد دولة قطر أو مؤسساتها أو مسؤوليها. وإذا نشأ تعارض بين هذه الوثيقة وقوانين دولة قطر، تكون الأولوية للقوانين. لقد تم بذل كل الجهود لتحقيق دقة "العمل"، ولكننا لا نقدم أي ضمان أو تأمين أو تعهد فيما يتعلق بدقة "العمل" أو اكتماله أو حدثاته. تم إدراج روابط إلى المواقع الإلكترونية الأخرى للتسهيل فقط؛ ولا يعتبر ذلك مصادقة على المواد الموجودة في تلك المواقع أو أي جهة أو منتج أو خدمة مرتبطة بها.

يجب أن يشير أي استنساخ لوثيقة "العمل" سواء جزئيًا أو كليًا وبغض النظر عن وسائل الاستنساخ إلى أن وزارة المواصلات والاتصالات هي المصدر والمالك لمحتوى "العمل". ويجب الحصول على إذن كتابي مسبق من وزارة المواصلات والاتصالات في حالة أي استنساخ يتعلق بهذه الوثيقة بقصد التوزيع التجاري. وتحفظ وزارة المواصلات والاتصالات بالحق في تقييم وظائف وقابلية التطبيق لجميع النسخ المعدة للأغراض التجارية. لا يجوز تفسير التفويض من وزارة المواصلات والاتصالات على أنه مصادقة للنسخ التي تم تطويرها ولا يجوز للمنتج أو صاحب العلامة التجارية أو مقدم الخدمة أن يستخدم موافقة الوزارة للدعاية أو الترويج أو إساءة تفسير ذلك بأي وسيلة من وسائل الإعلام أو النقاشات الشخصية / الاجتماعية.

حقوق النشر © 2015

دولة قطر

حكومة قطر الرقمية

وزارة المواصلات والاتصالات

وحدة السياسات والمعايير



حكومة
قطر الرقمية
Qatar Digital
Government

<http://www.qdg.qa>

<http://www.motc.gov.qa>

البريد الإلكتروني : policy@motc.gov.qa

الاختصاص القانوني

تنص المادة (14) من القرار الأميري رقم 16 لسنة 2014 بتعيين اختصاصات الوزارات أن وزارة الاتصالات وتكنولوجيا المعلومات (ويشار إليها فيما بعد باسم "الوزارة")، تختص بالإشراف على قطاع الاتصالات وتكنولوجيا المعلومات وتطويره بما يتفق مع متطلبات التنمية الوطنية، وإيجاد بيئة تنظيمية مناسبة للمنافسة العادلة، ودعم وتنمية وتحفيز هذا القطاع وتشجيع الاستثمار فيه، وتأمين ورفع كفاءة البنية التحتية التكنولوجية والمعلوماتية، وتطوير الجيل التالي منها، وتوعية المجتمع بأهمية تكنولوجيا المعلومات والاتصالات واستخدامها بطرق آمنة لتحسين حياة الفرد والارتقاء بالمجتمع، وصولاً إلى بناء مجتمع واقتصاد رقمي قائمين على المعرفة.

وتنص المادة 12 من القرار الأميري رقم 27 لسنة 2014 بالهيكل التنظيمي للوزارة على اختصاص الوزارة بتطوير الاستراتيجية الوطنية للحكومة الإلكترونية وصياغة مسودة التشريعات والسياسات والمعايير الخاصة بنظم تكنولوجيا المعلومات والمعاملات الإلكترونية والحكومة الإلكترونية، وذلك لتمكين التحول الإلكتروني في الجهات الحكومية بدولة قطر.

التوافق الاستراتيجي

وقد وضعت الحكومة رؤية تقضي بضمان تداول المعلومات لتقديم خدمات عامة أفضل من خلال زيادة التنسيق بين الجهات المعنية. وتتضمن [استراتيجية التنمية الوطنية لدولة قطر 2016-2011](#) ضرورة استخدام تكنولوجيا المعلومات والاتصالات لتحقيق "التكامل المؤسسي" من خلال زيادة تكامل العمليات، وإنشاء مستودعات مركزية للبيانات لتقديم خدمات عامة موجهة للمواطنين، ذلك أن زيادة التنسيق من خلال تداول المعلومات من شأنه التقليل من تجزئة عملية صنع القرار من قبل الجهات الحكومية.

ملخص الوثيقة

الاسم	سياسة إدارة البيانات
الإصدار	1.0.1
مرجع الوثيقة	P001
نوع الوثيقة	سياسة
ملخص	<p>تهدف هذه الاستراتيجية إلى إنشاء نهج للبيانات، وإدارتها، وحمايتها، ومشاركتها على مستوى الحكومة وتعزيزه. وتتمثل فوائد ذلك - على سبيل المثال لا الحصر - في تقارب البيانات ومشاركتها عبر الجهات، ودمج الخدمات بطريقة سلسة، وإجراء التحليلات السليمة، وتطوير نضج البيانات وجودتها عبر دورة حياة البيانات، والممارسات الأخلاقية لاستخدام البيانات، وتمكين مبدأ جمع البيانات لمرة واحدة.</p>
تاريخ النشر	أبريل 2015
تنطبق على	كافة الجهات الحكومية التي تنشئ البيانات والمعلومات أو تجمعها أو ترسلها أو تخزنها أو تعالجها.
فترة الاعتماد	12 شهرًا من تاريخ نشر السياسة
المالك	وزارة المواصلات والاتصالات

* لأية ملاحظات أو استفسارات يرجى التواصل عبر policy@motc.gov.qa



قائمة المختصرات

وزارة المواصلات والاتصالات	MOTC
جمعية الحاسبات البريطانية	BCS
جمعية إدارة البيانات	DAMA
هيئة إدارة البيانات للمعرفة	DMBOK

قائمة المحتويات

2	1 المقدمة
2	1.1 معلومات أساسية
3	1.2 الوضع الراهن
3	1.3 الحاجة إلى إدارة وتداول البيانات
5	1.4 المبادئ التوجيهية
6	2 أهداف السياسة
7	3 حيز السياسة وآليات تطبيقها
8	4 أحكام السياسة
8	4.1 حوكمة البيانات
8	4.2 إدارة البيانات
10	4.3 حماية البيانات
11	4.4 تداول واستخدام البيانات
13	4.5 منصة مركزية لتكنولوجيا المعلومات لدعم عملية تداول البيانات الحكومية
13	4.6 متابعة ومراجعة مراحل التطبيق
15	5 مسرد المصطلحات والتعاريف
16	الملاحق
16	الملحق 1: إدارة دورة حياة البيانات
20	الملحق 2: نموذج بيان الخصوصية
21	الملحق 3: مثال لنموذج معايير البيانات

1 المقدمة

يتمثل الهدف الرئيسي من إدارة البيانات في دعم احتياجات أي جهة من معلومات الأعمال¹. ويمكن تعريف إدارة البيانات² باعتبارها الممارسات والتقنيات والأساليب والأدوات الهيكلية اللازمة لتحقيق الوصول إلى البيانات وتوفيرها بصورة ثابتة عبر مختلف أطراف البيانات وأنواع هياكل البيانات في المؤسسة، لتلبية متطلبات استهلاك البيانات بمختلف تطبيقاتها وعملياتها في مجال الأعمال. ومن منظور الخدمات، تعتبر إدارة البيانات³ خدمة مؤسسية تساعد في تقديم خدمات المعلومات من خلال التحكم في أو تنسيق التعريفات أو استخدام البيانات الموثوق بها والملائمة. وتشمل المجالات الرئيسية لإدارة البيانات ما يلي⁴:

- تطوير سياسة البيانات
- ملكية البيانات
- تجميع البيانات الوصفية
- التحكم في دورة حياة البيانات
- جودة البيانات
- النفاذ إلى البيانات ونشرها

تأخذ هذه الوثيقة في الاعتبار كلاً من إدارة البيانات والوظائف الخدمية لعمليات إدارة البيانات عند تحديد أحكام السياسة، لدعم معلومات الأعمال المطلوبة لتقديم الخدمات الحكومية للجمهور على نحو سلس.

1.1 معلومات أساسية

بينما نمضي قدماً نحو اقتصاد المعرفة، تصبح المعلومات أحد الأصول الثمينة التي يجب على الحكومة إدارتها باعتبارها أمانة عامة نيابة عن المواطنين. إن استخدام البيانات داخل وعبر الجهات الحكومية بفعالية أمر بالغ الأهمية لتعزيز قدرة الجهات الحكومية على وضع سياسات وتقديم خدمات أكثر ملاءمة للجمهور.

تعتمد الجهات الحكومية، في تقديم الخدمات العامة لجمهورها، على معلومات قد تكون مملوكة لجهات متعددة. والواقع إنها تقوم بجمع واستخدام وتخزين مجموعة واسعة من المعلومات الشخصية، مثل سجلات تاريخ الميلاد، ومعلومات الهوية الوطنية وتفاصيل الوضع السكاني وعناوين الاتصال، وذلك ضمن أداء مهامها. وتستخدم المعلومات للتحقق من الهوية وتأكيد الأهلية وكشف الاحتيال ومنعه.

لذلك، من المهم أن تتم إدارة البيانات باعتبارها ثروة وطنية، لأن ذلك من شأنه زيادة الكفاءة التشغيلية وخفض التكاليف، وتحسين الخدمات وتعزيز أسس الحوكمة. وتهدف هذه الوثيقة إلى وضع عمليات للحوكمة والمعايير لكافة الجهات الحكومية في دولة قطر لإدارة وتداول البيانات.

¹ لماذا نحتاج إلى إدارة المعلومات، الجمعية الدولية لإدارة البيانات.

² تعريف إدارة وتكامل البيانات، مسرد تكنولوجيا المعلومات، جارتز

³ مبادئ إدارة البيانات، تسهيل عملية تداول المعلومات، الجمعية البريطانية للكمبيوتر

⁴ مبادئ إدارة البيانات المتميزة، مكتب نائب رئيس الوزراء، لندن

1.2 الوضع الراهن

تعمل بعض الجهات الحكومية حاليًا على تداول المعلومات لتمكين من توفير خدماتها للجمهور على نحو فعال. على سبيل المثال، وضعت كل من وزارة الداخلية، والمجلس الأعلى للصحة، ووزارة العمل والشؤون الاجتماعية، ووزارة الاقتصاد والتجارة ووزارة التخطيط التنموي والإحصاء، ترتيبات مباشرة لتداول مثل هذه البيانات عبر مختلف الوسائل الإلكترونية وغير الإلكترونية. ومع ذلك، يجري حاليًا تداول هذه البيانات على أساس محدود وثنائي فقط.

هناك جهات لا تعرف بوجود البيانات في القطاع العام، وحتى إذا عرفت بوجود تلك البيانات، فإنها قد لا تعرف مكان وجودها أو كيفية الحصول عليها. وفي بعض الأحيان، يمكن الحصول على بيانات من جهة أخرى، غير أن هذه الجهة لا يمكنها أن تسمح لعملائها بمعرفة حقيقة أنها موجودة في الأصل (أي أنها محظورة من قبل الجهة الموردة للبيانات). وقد تتخوف بعض الجهات من إطلاق / تداول البيانات نتيجة الانطباع السائد بأن أي تداول لتلك المعلومات قد يفسر على أنه إفشاء غير صحيح للبيانات، أو ربما مخالفة.

وحتى لو افترضنا استعداد الجهات لتداول البيانات مع بعضها البعض، فقد لا تكون البيانات متاحة في شكل إلكتروني، أو قد لا تتوفر عمليات مناسبة لإدارة البيانات مثل حماية البيانات ومعايير البيانات، أو قناة أو منصة مناسبة يتم من خلالها تداول البيانات إلكترونياً. وبالمثل، قد تحجم بعض الجهات الحكومية عن اتباع مبادرات جديدة لتداول البيانات بسبب الشكوك حول صلاحيتها القانونية التي تسمح لها بذلك. وتصبح هذه المشكلات أكثر وضوحًا عند الحاجة إلى الحصول على بيانات من جهات متعددة من أجل تقديم خدمة.

في الوقت نفسه، وطبقًا لمسح ميداني⁵، عبّر مستخدمو الإنترنت في دول مجلس التعاون الخليجي عن مخاوف من استخدام بياناتهم الشخصية لأغراض غير تلك التي تم تقديم البيانات من أجلها.

1.3 الحاجة إلى إدارة وتداول البيانات

إن من أكبر التحديات المتعلقة بإدارة وتداول المعلومات هي أن معظم البيانات الحكومية محفوظة في "صوامع"، أو، بعبارة أخرى، داخل إدارات منفصلة. وبينما قد تكون إدارة البيانات فعالة على مستوى كل جهة على حدة، إلا أن تبني نهج موحد لإدارة البيانات من شأنه أن يؤدي إلى مستوى أكبر من التعامل المشترك وبالتالي تبادل البيانات على النطاق الحكومي بطريقة أكثر فعالية.

لقد أدركت الحكومات في جميع أنحاء العالم أهمية إدارة وتبادل البيانات، ووضعت التشريعات والممارسات والعمليات لتسهيل هذا الجانب. وفي هذا الصدد، وجه المكتب التنفيذي لرئيس الولايات المتحدة⁶ رؤساء الإدارات والجهات التنفيذية إلى إدارة المعلومات كثروة، ووضع إطار للمساعدة في إضفاء الطابع المؤسسي على مبادئ الإدارة الفعالة للمعلومات في كل مرحلة من مراحل دورة حياة المعلومات، لتعزيز التعامل المشترك والانفتاح. وتشجع سياسة كندا⁷ في مجال إدارة المعلومات، عملية إدارة المعلومات والسجلات باستخدام نهج موحد عبر جميع الجهات الحكومية. وقد سنت فنلندا⁸ قانونًا حول حوكمة إدارة المعلومات يتضمن أحكامًا بشأن التزامات هيئات معينة في الإدارة العامة عند إجراء مهام إدارة المعلومات بما في ذلك توافر

⁵ تقرير وزارة الاتصالات وتكنولوجيا المعلومات في يوليو 2014 حول: مواقف مستخدمي الإنترنت بمنطقة الشرق الأوسط تجاه الأمن الإلكتروني وخصوصية البيانات (صفحة 29، مخاوف من سوء استخدام البيانات الشخصية)

⁶ مذكرة لرؤساء الإدارات والجهات التنفيذية: سياسة إدارة البيانات المفتوحة كثروة، 9 مايو 2013 مكتب الإدارة والميزانية، المكتب التنفيذي لرئيس الولايات المتحدة الأمريكية

⁷ سياسة إدارة المعلومات، 1 يوليو 2007، مجلس الخزانة لأمانة كندا، حكومة كندا

⁸ قانون حوكمة إدارة المعلومات في الإدارة العامة، 1 سبتمبر 2010، وزارة المالية، حكومة فنلندا

المعلومات في شكل إلكتروني، ونظام التعامل المشترك، وتداول المعلومات. في نفس السياق، عدل برلمان نيوزيلندا⁹ قانون الخصوصية للسماح بعقد اتفاقيات تداول المعلومات المعتمدة لتمكين استخدام وتداول المعلومات بين وداخل الجهات المقدمة للخدمات العامة عن طريق تعديل أو توضيح أسس تطبيق مبادئ خصوصية المعلومات. ووضعت أستراليا¹⁰ كذلك استراتيجية وطنية يهدف إدارة المعلومات الحكومية باعتبارها ثروة استراتيجية لضمان استخدام أكثر كفاءة وفعالية. وقدمت اللجنة القانونية في المملكة المتحدة¹¹، التي أنشئت لتشجيع الإصلاح القانوني، تقريراً للبرلمان عن تداول البيانات بين الجهات الحكومية، يتضمن التوصية بإصلاح قانوني شامل من أجل إنشاء هيكل قانوني مبدئي وواضح لتداول البيانات يضمن كفاءة وفعالية الحكومة، وتقديم الخدمات العامة وحماية الخصوصية، وكذلك وضع قواعد لممارسات إدارة وتداول المعلومات بين الجهات الحكومية.

وحرصاً من وزارة الاتصالات وتكنولوجيا المعلومات على ضمان التوصل إلى استخدام أكثر فعالية للبيانات في القطاع العام في دولة قطر، ضمن نطاق التشريعات الحالية، ومن أجل الحفاظ على الحماية الأساسية لخصوصية البيانات، فقد أخذت الوزارة زمام المبادرة لتطوير سياسة من شأنها قيادة وتوجيه الجهات في مجال إدارة وتداول البيانات على مستوى القطاع العام. وتسعى هذه الوثيقة إلى تمكين وتوجيه الجهات الحكومية في دولة قطر نحو إدارة وتداول البيانات ضمن القوانين السائدة من أجل تسهيل توفير الخدمات الحكومية على نحو فعال، مع ضمان حماية المعلومات والخصوصية. وكخطوة متقدمة أخرى، تخطط الوزارة أيضاً لتطوير منصة للتطبيق تسهلاً لتداول البيانات عبر الجهات.

⁹ تعديلات حول تداول المعلومات في قانون الخصوصية لعام 1993، فبراير 2013، حكومة نيوزيلندا

¹⁰ الاستراتيجية الوطنية لتداول المعلومات الحكومية، يوليو 2007، مكتب إدارة المعلومات، حكومة أستراليا

¹¹ تداول البيانات بين الجهات الحكومية، تقرير تشخيصي، 10 يوليو 2014، اللجنة القانونية، وزارة العدل، المملكة المتحدة

1.4 المبادئ التوجيهية

تهدف هذه الوثيقة إلى توفير أساس يضمن أن أي بيانات يتم تداولها ستستخدم فقط لأغراض مشروعة، ووضع أساس لإدارة البيانات على نحو فعال. ويتعين على الحكومة وهي تتولى عملية جمع وحفظ واستخدام معلومات شخصية، أن تتصرف بوصفها راعية لتلك البيانات وصيانة وحماية أمن المعلومات وفقاً لأحكام القوانين والتشريعات والسياسات ذات الصلة. كما يتعين عليها تحديد قواعد للجهات لتسهيل تداول البيانات داخل تلك الجهات وفيما بينها بطريقة فعالة.

فيما يلي المبادئ التوجيهية الرئيسية المطبقة في صياغة هذه السياسة:



أ. ينبغي أن تدار البيانات كمورد استراتيجي يدعم السياسات واتخاذ القرار، علاوة على مبادئ المساءلة والتنفيذ الفعال للبرامج والخدمات الحكومية.

ب. يجب ألا ينظر إلى البيانات التي يتم جمعها أو استحداثها من قبل كل جهة -على أنها ملك لتلك الجهة وحدها، بل باعتبارها متاحة للتداول مع جهات أخرى، ضمن حدود الخصوصية وحقوق المؤلف والاعتبارات القانونية والأمنية.

ج. حيثما كان ذلك ممكناً، يجب الحصول

على البيانات مرة واحدة واستخدامها لأغراض متعددة أو عامة، وتجنب الازدواجية في الحصول على البيانات.

يحدد مجمل معارف إدارة البيانات لجمعية إدارة البيانات¹² الوظائف العشر لإدارة البيانات على النحو الموضح في الشكل أعلاه، وتستمد هذه الوثيقة معلوماتها من هذا الإطار فيما يتعلق ببعض الوظائف ذات الصلة في صياغة السياسة.

¹² مصدر معارف إدارة البيانات، مطبوعة تصدر عن جمعية إدارة البيانات (DAMA) - (www.dama.org)

2 أهداف السياسة

الأهداف الرئيسية لهذه السياسة هي:

- 2.1 إنشاء حوكمة بيانات وعمليات قياسية بين الهيئات الحكومية لإدارة البيانات ومشاركتها.
- 2.2 عمل فهرس لمعايير البيانات والبيانات الوصفية المناسبة لدعم تقارب البيانات، وإمكانية التشغيل البيئي، والمشاركة، والاكتشاف داخل الجهات وفيما بينها.
- 2.3 دعم الخدمات التي تركز على المواطنين من خلال الاستخدام السلس للبيانات بين الهيئات المتعددة.
- 2.4 وضع الأساس للإدارة الفعالة للبيانات لضمان استخدام البيانات فقط لأغراض مشروعة مع الجهات التي تعمل كراعية لتلك البيانات، إلى جانب الاحتفاظ بالبيانات وحمايتها، وفق أحكام القوانين والتشريعات والسياسات¹³ ذات الصلة.
- 2.5 الدفع نحو تطوير منصة تبادل بيانات قياسية، ونشرها، واعتمادها، وبالتالي إنشاء نهج مشترك للبيانات لقابلية التشغيل البيئي يستبدل أية مشاركة ثنائية مخصصة غير قياسية.
- 2.6 المضي نحو مبدأ المرة الواحدة لضمان معلومات قياسية مرة واحدة بين الجهات الحكومية.
- 2.7 تحسين ثقة الجمهور في قدرة الجهات الحكومية على التصرف كأوصياء على المعلومات والبيانات الشخصية من خلال المحافظة على البيانات، وفق أحكام القوانين والتشريعات والسياسات ذات الصلة.

¹³ يرجى الرجوع إلى المبادئ التوجيهية للمخاطبين بأحكام القانون

3 حيز السياسة وآليات تطبيقها

3.1 تنطبق على كافة الجهات الحكومية التي تنشئ البيانات والمعلومات أو تجمعها أو ترسلها أو تشاركها أو تخزنها أو تعالجها.

3.2 معالجة دورة حياة المعلومات (راجع الملحق 1) مع التركيز على المجالات الأساسية التالية:

- حوكمة البيانات
- إدارة البيانات
- حماية البيانات
- مشاركة البيانات

3.3 تنطبق على جميع البيانات الإلكترونية (المهيكله وغير المهيكله) والأنظمة ذات العلاقة التي تنشئ، وتجمع، وتحافظ على المعلومات كجزء من خصائص الأعمال الرسمية الخاصة بها، والتي إما يتم استخدامها أو مشاركتها من أجل تقديم الخدمات العامة. ومن أمثلة البيانات المهيكله:

- بيانات العملاء (مثل البيانات الشخصية وبيانات الشركات)
- بيانات غير العملاء (مثل البيانات البيئية)
- البيانات التنظيمية (مثل بيانات الموارد البشرية، والبيانات المالية، والبيانات المتعلقة بالأصول والمشتريات)
- أما البيانات غير المهيكله، فهي مثل مستندات معالج الكلمات، وشرائح العرض التقديمي، والصور، ومقاطع الفيديو، ومقاطع الصوت، ويشمل ذلك البيانات النصية والنقطية.

3.4 تخضع عمليات التشغيل لاعتبارات الخصوصية، وحقوق النشر، والأمن. ويجب على الهيئات التأكد من توافقها مع كافة التشريعات ذات الصلة¹⁴ المعمول بها في دولة قطر.

¹⁴ تشمل التشريعات والمراسيم والتوجيهات والقوانين والسياسات الصادرة من السلطات المختصة بدولة قطر

4 أحكام السياسة

يضع هذا القسم للجهات الحكومية في دولة قطر الأحكام التي تضمن حسن إدارة البيانات وحمايتها وأيضاً تداولها فيما بينهما من أجل توفير خدمات متميزة للجمهور.

وتتطلب سياسة إدارة البيانات هذه من جميع الجهات الحكومية في دولة قطر اتخاذ الخطوات التالية:

4.1 حوكمة البيانات

- أ. على الجهات تعيين أحد كبار الموظفين لتحمل مسؤولية الإشراف على إدارة ومراقبة بيانات الجهة والعمليات ذات الصلة.
- ب. يجب أن يكون من يتولى هذه المسؤولية في درجة عليا مناسبة نظراً لاختصاصاته الإشرافية وتمثيل الجهة في جميع المسائل المتعلقة بإدارة البيانات وتداول البيانات عبر مختلف الجهات.
- ج. يتعين على الموظف المعين التأكد من وجود عمليات وإجراءات فعالة لإدارة دورة حياة المعلومات¹⁵ لضمان استحداث وتخزين وإدارة ومعالجة البيانات على نحو دقيق وآني ومكتمل. ويتولى الموظف أيضاً مسؤولية ضمان الامتثال للتشريعات ذات الصلة في هذا الشأن.
- د. يجب تصعيد جميع القضايا المشتركة بين الجهات فيما يخص إدارة وتداول البيانات إلى اللجنة التوجيهية للحكومة الإلكترونية. وتختص اللجنة التوجيهية للحكومة الإلكترونية بمراقبة البيانات وضمان موافقتها وتقديم التوجيه العام والمشورة بشأن قضايا إدارة البيانات لتسهيل تداول البيانات عبر الجهات داخل الإطار التشريعي القائم.

4.2 إدارة البيانات

4.2.1 ملكية البيانات

- أ. البيانات التي يتم جمعها من قبل أي جهة هي في النهاية ملك لحكومة قطر، ولذا يجب أن تكون متاحة للتداول مع جهات أخرى في حدود القوانين والسياسات والأنظمة القائمة.
- ب. يتعين على الجهات المصدرة للبيانات وضع تدابير من شأنها صيانة البيانات بما في ذلك التعامل مع أية تحديثات لاحقة للبيانات ونشرها بين الجهات المستخدمة.
- ج. لضمان سلامة البيانات على المستوى الحكومي، يجب على الجهات أن تطلب البيانات التي تحتاجها لاستكمال معاملات الخدمة أولاً من الجهات المصدرة للبيانات، في حالة وجودها. إما إذا لم تكن هناك جهة مصدرة للبيانات المطلوبة، فيمكن للجهات جمع بيانات من مصادر أخرى مناسبة.

4.2.2 جمع البيانات

- أ. على الجهات التأكد من أن جميع المعلومات أو السجلات مخزنة إلكترونياً في أنظمتها، ومصنفة ومؤمنة تماشياً مع سياسة تأمين المعلومات الوطنية (الإصدار الثاني). يجب على الجهات أيضاً إنشاء وصيانة سجل لهذه البيانات والمعلومات باللغة الأهمية.

¹⁵ يرجى الرجوع إلى الملحق رقم 1 حول المبادئ التوجيهية

ب. على الجهات التأكد من أن البيانات يتم جمعها عن طريق الوسائل المشروعة والنزيهة، ويجب أن يقتصر الجمع على ما هو ضروري لتلبية متطلباتها القانونية أو المتصلة بنشاطها العملي. يجب تطبيق أحكام السياسة رقم 1.2.4 (ج) الواردة في هذه الوثيقة عند تحديد ما إذا كان للجهة أن تحصل على البيانات من جهة أخرى (جهة مصدرة للبيانات) أو جمعها من مصادر مناسبة أخرى.

ج. ينبغي على الجهات طلب الحصول على معلومات أو مستندات داعمة من أفراد أو شركات لاستكمال معاملات الخدمة، فقط في حالة عدم توفر هذه المعلومات إلكترونياً لديها أو عدم توفرها لأغراض التداول إلكترونياً لدى أي جهة حكومية أخرى.

د. يجب على الجهات التأكد من أن الفرد المعني بالمعلومات الشخصية لديه معرفة وأبدي موافقته على جمع واستخدام أو الإفصاح عن بياناته الشخصية إلى جهة خارجية أو جهة أخرى لغرض استكمال معاملات الخدمة.

هـ. على الجهات إجراء مراجعات لتحديد الخدمات التي يمكن فيها التخلص من أو تقليل المستندات أو تعبئة الاستمارات المطلوبة من قبل الأفراد والشركات إلى أدنى حد ممكن:

1. إجراء مراجعات لتحديد ما إذا كانت المعلومات أو المستندات ضرورية فعلاً لاستكمال خدمة أو معاملة معينة.

2. النظر في طرق بديلة للحصول على المعلومات من خلال:

- الحصول على المعلومات المطلوبة داخلياً من المستودعات وقواعد البيانات.
- طلب الإثباتات والبيانات المطلوبة خارجياً من الجهات المصدرة للبيانات.
- أتمتة العمليات المشار إليها أعلاه والمتعلقة بالحصول على المعلومات من مصادر داخلية أو خارجية.

4.2.3 معايير البيانات

تعتبر معايير البيانات حجر الزاوية في عملية الاستخدام المشترك، ومن شأن اعتماد مجموعة من معايير البيانات للاستخدام في كافة الجهات الحكومية أن يفضي في النهاية إلى إزالة الغموض والتضارب في استخدام البيانات وتحقيق أساليب أكثر فعالية من حيث استخدام وتداول البيانات.

أ. تتحمل كل جهة مسؤولية إنشاء وصيانة كتالوج¹⁶ لمعايير البيانات الذي يجب أن يشمل المعلومات الوصفية والمعايير المتعلقة بالبيانات الخاصة بها في شكل موحد. من شأن كتالوج معايير البيانات أن يساعد أيضاً في تحديد المسئول الرئيسي عن العمل أو الجهة المصدرة للبيانات فيما يتعلق ببيانات معينة.

ب. على الجهات نشر كتالوج معايير البيانات للموظفين المخولين في الجهات الحكومية الأخرى لكي يحددوا مدى توافر البيانات وكذلك معايير المعلومات الوصفية.

ج. على الجهات المستخدمة للبيانات اعتماد معايير البيانات الخاصة بالجهات المصدرة للبيانات بالنسبة لعناصر بيانات بعينها.

د. تتحمل الجهة المصدرة للبيانات المسؤولية عن تحديث كتالوج معايير البيانات لديها بإضافة سمات جديدة أو محدثة، وإخطار الأطراف ذات المصلحة على مستوى الدولة بكل هذه المراجعات.

¹⁶ يرجى الرجوع إلى الملحق 3 - نموذج معايير البيانات

4.2.4 النفاذ إلى البيانات

يقتصر منح حق النفاذ إلى البيانات فقط على الأفراد والجهات التي لديها أسباب مشروعة ومبررة للوصول إليها، وذلك في حدود القوانين والسياسات واللوائح ذات الصلة.

- أ. على الجهات أن تميز بوضوح بين عناصر البيانات ذات النفاذ المقيد، وتلك البيانات ذات النفاذ المفتوح والتي يتم تصنيفها على أساس أنها بيانات عامة تماشيًا مع [سياسة تأمين المعلومات الوطنية \(الإصدار الثاني\)](#).
- ب. يتعين على الجهات وضع ضوابط تضمن أن فرصة الوصول إلى البيانات ذات النفاذ المقيد مقصور فقط على الأفراد والجهات التي لديها أسباب مشروعة ومبررة للوصول إليها، وكذلك الموافقات اللازمة لذلك.

4.3 حماية البيانات

4.3.1 حماية المعلومات والبيانات

كل جهة مسؤولة عن حماية جميع البيانات بما فيها البيانات الشخصية المودعة في عهدها.

- أ. يجب على الجهات حماية جميع ما في حوزتها من المعلومات والبيانات (بما في ذلك البيانات الواردة من جهات أخرى)، أو عند الكشف عن البيانات لجهة خارجية أو جهة أخرى. كما يجب وضع ضمانات أمنية لحماية البيانات من أي نوع من النفاذ أو الإفشاء أو التعديل غير المصرح به.
- ب. على الجهات الالتزام بـ [سياسة تأمين المعلومات الوطنية \(الإصدار الثاني\)](#) الصادرة من الوزارة فيما يتعلق بوجود احتياطات كافية لضمان حماية جميع أنظمة ووسائط التخزين الإلكتروني المعنية بالتعامل مع البيانات لمنع أي نوع من النفاذ أو التعديل للبيانات غير المصرح به.
- ج. على الجهات إجراء مراجعات دورية لسياساتها وعملياتها لضمان وجود احتياطات كافية لحماية البيانات، وأيضاً إجراء عمليات تدقيق دورية للتأكد من أن التدابير الرامية إلى حماية البيانات تتوافق مع هذه السياسات.
- د. على الجهات أن تضمن وجود إجراءات تكفل حماية سرية وسلامة البيانات التي يتم الحصول عليها من جهات أخرى.
- هـ. على الجهات التأكد من أن تصنيف وتخزين جميع أصول المعلومات والبيانات يتم وفق مستويات السلامة الموضوعية لكل منها (يرجى الرجوع إلى [سياسة تأمين المعلومات الوطنية - الإصدار الثاني](#) - الصادرة من الوزارة).

4.3.2 حماية المعلومات الشخصية

- أ. يجب على الجهات الالتزام بمبادئ خصوصية المعلومات وكذلك القوانين المعمول بها في دولة قطر بشأن جمع ومعالجة وتداول البيانات الشخصية. كما يتعين عليها التأكد من أن السياسات والعمليات المطبقة لديها لحماية البيانات الشخصية حديثة ويتم التقيد بها في جميع عمليات معالجة البيانات داخل الجهة وعند نقل أو تداول البيانات مع جهة أخرى أو إلى طرف ثالث.
- ب. على الجهات التأكد من أن سياساتها وعملياتها المتعلقة بمعالجة البيانات الشخصية تشمل المجالات التالية:
 1. البيانات الشخصية التي هي في حوزة الجهة أو التي تتاح لجهات أخرى والتي تعتبر ضرورية لأغراض الوفاء بشرط قانوني أو تنظيمي، أو لأغراض تقديم خدمة عامة،

2. الإجراءات التي تمكن الفرد من الحصول على مزيد من المعلومات أو الوصول إلى البيانات الشخصية التي قدمها في وقت سابق للجهة، وكذلك الإجراءات ذات الصلة باستخدام وإفشاء تلك البيانات الشخصية من قبل الجهة.
3. تفاصيل الاتصال بالموظف المسؤول المكلف باستقبال الاستفسارات والملاحظات المتعلقة بالبيانات الشخصية.
- ج. يجب على الجهات نشر بيان بشأن الخصوصية على مواقعها الإلكترونية. يرجى الرجوع إلى [الملحق 2](#) المتضمن نسخة من عينة بيان الخصوصية.
- د. يجب على الجهات تطبيق عمليات تكفل التخلص من أو تدمير البيانات الشخصية بشكل آمن وذلك لمنع الأطراف غير المصرح لها من الوصول إلى تلك البيانات.

4.4 تداول واستخدام البيانات

4.4.1 تداول البيانات

ينبغي على الجهات عدم جمع بيانات من الجمهور إذا كانت تلك البيانات متوفرة لدى جهات حكومية أخرى. ومن شأن هذا أن يكفل أن الجمهور سيقدم البيانات مرة واحدة فقط للجهات الحكومية من أجل الحصول على خدمات متعددة؛ وبالتالي ضمان مصدر وحيد للحقيقة، ودقة وسلامة البيانات.

- أ. يجب على الجهات المصدرة للبيانات تداول البيانات المكتسبة أو المستحدثة مع الجهات الأخرى وفق الالتزامات القانونية واعتبارات الخصوصية، ما دام هناك غرض واضح وسليم للتداول.
- ب. على الجهات الحصول على موافقة الأفراد، وذلك على النماذج الورقية أو الإلكترونية لطلب الخدمة، للسماح بإعادة استخدام وتداول البيانات الشخصية لغرض توفير الخدمات الحكومية لهم. وقد تكون هذه الموافقة في شكل بيان مفاده أنه بتقديم الطلب للحصول على الخدمة المطلوبة، فإن الشخص يوافق على تداول وإعادة استخدام بياناته الشخصية من قبل الجهات الحكومية في دولة قطر لأغراض تلبية طلباته الحالية والمستقبلية من الخدمات الحكومية.
- ج. بالنسبة لإعادة استخدام أو تداول تلك البيانات لأي غرض بخلاف توفير الخدمات، يجب على الجهات الحصول على موافقة الأفراد فيما يتعلق بتلك الأغراض تحديداً.
- د. على الجهات المصدرة للبيانات تسهيل وتمكين تداول البيانات مع الجهات المستخدمة حتى يتمكن القطاع العام من:
 1. تحقيق أكبر قدر من الراحة للأفراد والكيانات (بمعنى أنهم سيقدمون البيانات مرة واحدة لحكومة قطر للحصول على العديد من الخدمات العامة بدلاً من الاضطرار لتقديمها لجهات مختلفة عند الحاجة لمعاملات مختلفة).
 2. توفير الخدمات الكاملة من البداية إلى النهاية (المنصوص عليها تماشياً مع [استراتيجية الحكومة الإلكترونية لدولة قطر 2020 الصادرة عن وزارة الاتصالات وتكنولوجيا المعلومات](#)).
 3. تطوير سياسات أكثر وعياً وتركيزاً من خلال النفاذ إلى بيانات أكثر وأفضل من حيث النوعية.
 4. تعزيز الكفاءة وخفض التكلفة من خلال زيادة تداول البيانات.

4.4.2 الغرض من تداول البيانات

ينبغي على الجهات تداول البيانات مع بعضها البعض فقط لأغراض واضحة وسليمة.

- أ. يجب على الجهة المستخدمة للبيانات تحديد غرض واضح للجهة المصدرة للبيانات، ما لم تكن هناك موافقة مسبقة على استخدام البيانات لجميع الأغراض، من قبل الجهة المصدرة للبيانات.
- ب. على الجهة المستخدمة للبيانات استخدام البيانات فقط للأغراض المحددة.
- ج. يجب وضع اتفاقيات لتداول البيانات، متى ما كان ذلك مناسباً، لإلزام جميع الأطراف المشاركة في مبادرة التداول، على أن يتضمن مثل هذا الاتفاق لتداول البيانات: الغرض من تداول البيانات والمنظمات المعنية، مجموعات / عناصر البيانات التي سيتم تداولها، والقواعد المحددة لاستبقاء وحفظ وحذف عناصر البيانات المتداولة، وإجراءات التعامل مع انتهاء/إنهاء اتفاقيات تداول البيانات.

4.4.3 التداول داخل الجهات الحكومية

- أ. يجب تداول البيانات التي يتم جمعها أو استحداثها من قبل أي جهة مع الجهات الأخرى، وذلك في حدود القوانين المعمول بها ومبادئ خصوصية البيانات، لتمكين الجهات الحكومية من تحقيق الأهداف التالية:
1. توفير خدمات موجهة للعملاء
 2. تحقيق مبدأ الجودة في صياغة السياسات
 3. تسهيل عمليات التحليل والبحث
- ب. فيما يتعلق بالبيانات الحساسة، يجب على الجهات المصدرة للبيانات العمل مع الجهات المستخدمة للبيانات لتحديد الحد الأدنى من البيانات اللازمة لتلبية احتياجات المستخدمين، مع التأكد من وجود احتياطات كافية لضمان حماية البيانات، على سبيل المثال، بتحديد ما إذا كان في الإمكان تحقيق الهدف دون ذكر المصدر.
- ج. يجب أن تقتصر البيانات التي سيتم تداولها على ما يلبي أغراض الطلب. على سبيل المثال، إذا كان الغرض من البيانات المطلوبة هو التحقق مما إذا كان مقدم الطلب يكسب أقل من 10000 ريال قطري لكي يتأهل لبعض الفوائد الاجتماعية، فينبغي على مستخدمي البيانات السؤال عن مؤشرات الدخل، أي الإجابة بـ "نعم" إذا كان الدخل أكثر من 10000 ريال قطري أو بـ "لا" إذا كان الدخل أقل من 10000 ريال قطري، بدلاً من السؤال عن دخل الفرد كمبلغ محدد.
- د. يجب على الجهات المستخدمة للبيانات الامتثال، حيثما أمكن، لمعايير البيانات الموضوعية من قبل الجهات المصدرة للبيانات لضمان سهولة الحصول على تلك البيانات.
- هـ. إذا اعتبرت معايير بيانات الجهات المصدرة غير مناسبة من قبل الجهات المستخدمة للبيانات، لأغراض التداول أو لتقديم الخدمات، استناداً إلى أسباب مشروعة ومبررة، فيجب على الأولى تحديث معايير البيانات القائمة وجعل البيانات متاحة في الشكل المتفق عليه وخلال إطار زمني معقول.
- و. يجب على الجهات التي تعمل في مجال تداول البيانات وضع تدابير للتعامل مع التحديثات والملاحظات المتعلقة بجودة البيانات.
- ز. على الجهات تضمين نصوص واضحة بشروط استخدام ومعاملة والتخلص من البيانات، بما في ذلك فترات الاستبقاء والترتيبات اللازمة لحذف البيانات المرسله أو المستلمة، قبل تحويل البيانات إلى الجهات المستخدمة.
- ح. على الجهات المستخدمة للبيانات عدم تداول البيانات مع جهات أخرى دون موافقة صريحة من الجهة المصدرة للبيانات، ما لم يكن ذلك مخولاً أو مطلوباً وفقاً لقانون أو مرسوم، أو إذا كانت البيانات متاحة للاستخدام لجميع الأغراض بموافقة مسبقة من الجهة المصدرة للبيانات.

ط. على الجهة المصدرة للبيانات تداول جميع البيانات المصنفة "معتمدة مسبقاً للاستخدام لجميع الأغراض" من خلال المنصة المركزية لتكنولوجيا المعلومات (راجع الفقرة 4.5 أدناه) الخاصة بخدمات تداول البيانات لأغراض إعادة استخدامها من قبل الجهات الحكومية.

4.4.4 التداول مع الجمهور

أ. على الجهات تبادل البيانات غير الشخصية فقط مع الجمهور وذلك في حدود القوانين والسياسات واللوائح التنظيمية ذات الصلة.

ب. إن لم تكن البيانات ملكاً للجهة، فيجب عليها الحصول على موافقة الجهة المصدرة للبيانات قبل إطلاق تلك البيانات للجمهور، ما لم يكن ذلك مخولاً أو مطلوباً وفقاً لقانون أو مرسوم.

4.5 منصة مركزية لتكنولوجيا المعلومات لدعم عملية تداول البيانات الحكومية

أ. على وزارة الاتصالات وتكنولوجيا المعلومات إنشاء وصيانة منصة لتبادل البيانات الحكومية يكون بوسعها أن تتيح للجهات تبادل وتصفح البيانات المتاحة لأغراض تقديم الخدمات العامة، ويمكن للمنصة أن تتضمن المكونات الرئيسية التالية:

1. بنية تحتية لتكنولوجيا المعلومات - منصة إلكترونية مؤمنة لتبادل البيانات الحكومية يكون من شأنها أن

تتيح للجهات المصدرة للبيانات أن تتداول البيانات بينما يكون بوسع الجهات المستخدمة للبيانات أن تبحث في وأن تطلب البيانات المتاحة.

2. دليل معايير البيانات - قواميس بالبيانات المتوفرة لدى جميع الجهات الحكومية بعد حصرها وتحديثها على النحو المبين في الفقرة 3.2.4 (أ) تتضمن المعلومات الوصفية ومعايير البيانات.

3. حوكمة وإدارة المنصة - إنشاء هيكل وإجراءات الإدارة بغرض الإشراف على فعالية وكفاءة استخدام البيانات بين الجهات الحكومية بما في ذلك شروط الاستخدام، النفاذ، اتفاقيات مستوى الخدمة...إلخ.

ب. على جميع الجهات تداول وتبادل البيانات مع الجهات الحكومية الأخرى في دولة قطر من خلال منصة تبادل البيانات الحكومية عند اكتمال تشغيلها، والالتزام بالإجراءات والمعايير المنظمة.

4.6 متابعة ومراجعة مراحل التطبيق

مسؤوليات الهيئة:

4.6.1 يجب على الهيئات بذل جهوداً حثيثة لمشاركة البيانات بين الجهات الحكومية لتقديم خدمة حكومية إلكترونية شاملة من أجل خدمة شعب دولة قطر على نحو أفضل.

4.6.2 يجب على الهيئات أن تقدم تقريراً مفصلاً عن حالة تنفيذ هذه السياسة إلى وزارة المواصلات والاتصالات عند الطلب.

مسؤوليات وزارة المواصلات والاتصالات:

4.6.3 يجوز للوزارة إصدار إجراءات إضافية أو تكميلية، وإرشادات، وأفضل الممارسات من آخر لدعم تلك السياسة.



4.6.4 يجب على الوزارة مراقبة تنفيذ الهيئات الحكومية لهذه السياسة، ويجوز للوزارة في أي وقت طلب معلومات (أ) و تقرير مفصل حول اعتماد هذه السياسة.

مسرد المصطلحات والتعاريف

المصطلح	التعريف
الجهة	تعني جهة حكومية ما لم يتم استخدام المصطلح أو تتم الإشارة إليه في سياق مختلف.
الجمعية البريطانية للكمبيوتر (BCS)	هي هيئة مهنية دولية وجمعية ذات دراية علمية تهدف إلى تشجيع دراسة وتطبيق تكنولوجيا الاتصالات وتكنولوجيا الحوسبة ونشر المعرفة في مجال تكنولوجيا المعلومات والاتصالات (ICT) لفائدة الممارسين المهنيين والجمهور العام. وتعتبر الجمعية الكيان المهني الوحيد بالمملكة المتحدة التي تمنح مؤهلات قانونية للمتخصصين في تكنولوجيا المعلومات في إطار ميثاقها الملكي.
البيانات	وإدارتها تشير، لأغراض هذه الوثيقة، إلى كل البيانات والمعلومات في صيغة إلكترونية والتي تجمعها أو تسترجعها أو تتداولها أو تعالجها الجهات الحكومية لأغراض تقديم الخدمات الإلكترونية للجمهور وللزوار وللأعمال التجارية.
جمعية إدارة البيانات (DAMA)	هي جمعية دولية غير ربحية ومستقلة تضم فنيين ومتخصصين في مجال الأعمال، وتكرس أعمالها في مجال تطوير مفاهيم وممارسات إدارة مصادر المعلومات (IRM) وإدارة مصادر البيانات (DRM)
معالجة البيانات	وتعني لأغراض هذه الوثيقة إجراء أي عملية أو مجموعة عمليات على البيانات بما في ذلك جمع وتلقي وتدوين وتنظيم وتخزين وتكييف وتعديل واسترجاع، والتشاور حول، واستخدام وكشف ونشر وبث وحظر ومحو أو تدمير مثل تلك المعلومات.
تداول البيانات	يعني إفشاء البيانات من جهة/كيان أو جهات إلى جهة أو كيان آخر أو جهات أو كيانات أخرى، أو تداول البيانات بين الوحدات الخاصة بجهة أو كيان.
الجهة المصدرة للبيانات	تعني الجهة التي يتم فيها تدوين وحفظ وصون البيانات باعتبارها صاحبة الحق في هذه البيانات، والتي تقوم بتوفير / تبادل البيانات مع الجهات الأخرى.
الجهة المستخدمة للبيانات	تعني الجهة التي تطلب / تتلقى البيانات.
البيانات الإلكترونية	جميع البيانات الصادرة في صيغة إلكترونية، منظمة كانت أو غير منظمة.
جهة حكومية	تشير إلى جميع الوزارات والجهات العامة التي تتبع مباشرة للوزارات أو مجلس الوزراء في دولة قطر.
البيانات الشخصية	تشير إلى (1) أي معلومات عن شخص معروف الهوية أو يمكن التأكد من هويته، إلى حد معقول، عن طريق تلك المعلومات أو تركيبة منها ومن معلومات أخرى و(2) أي معلومات، بما فيها بيانات الموقع التي يمكن، إلى حد معقول، ربطها بشخص معين بصرف النظر عما إذا كانت هوية الشخص ظاهرة من خلال تلك المعلومات أو تركيبة منها ومن معلومات أخرى.
جهة خارجية	تعني العبارة، لأغراض هذه الوثيقة، أي شخص أو كيان يقوم بمعالجة البيانات بخلاف الجهة المصدرة للبيانات أو الجهات المستخدمة للبيانات ونيايةً عنها، وتشمل العبارة أي شخص أو كيان آخر يتم تعيينه من قبل الجهة الخارجية للغرض المشار إليه.

الملاحق

الملحق 1: إدارة دورة حياة البيانات

يعرض هذا القسم دليلاً موجزاً لفهم مختلف الخطوات المتبعة في عملية إدارة دورة حياة المعلومات للجهات بغرض وضع سياسات وإجراءات تشغيلية مناسبة لإدارة البيانات على نحو فعال.

وتتمثل إدارة دورة حياة المعلومات نهجاً لإدارة السجلات والبيانات والمعلومات المؤسسية (ويشار إليها فيما يلي باسم "البيانات" في هذا القسم لسهولة الرجوع إليها)، خلال كامل دورة حياتها، أي من منشئها حتى التخلص منها. وهي تستند إلى فرضية أن قيمة البيانات تتغير مع مرور الوقت ويجب إدارتها وفقاً لهذه التغيرات.

تتضمن إدارة دورة حياة المعلومات ثلاث مراحل أساسية: (1) مرحلة الإنشاء والالتقاط (2) مرحلة التخزين والإدارة (3) مرحلة التوزيع والتعامل:

1.1 الإنشاء والالتقاط

تتضمن المرحلة الأولى إنشاء أو الحصول على البيانات في شكل رقمي. قد تكون بعض البيانات موجودة أصلاً في شكل رقمي، مثل ملفات XML المستخرجة من نظام الكمبيوتر أو البيانات المتاحة في شكل رقمي مثل جداول البيانات الواردة من مصادر أخرى. بينما يمكن رقمنة البيانات غير الرقمية من مصادر أخرى مثل المستندات الورقية من خلال الإدخال اليدوي إلى النظام أو عن طريق المسح الضوئي.

وتعتبر عملية الحصول على البيانات وتخزينها من مصادر رقمية، أسهل نسبياً بالمقارنة مع إنشاء بيانات رقمية من مصادر غير رقمية. وتشمل الحلول التقنية التي تساعد في عملية إنشاء والحصول على البيانات، النماذج الرقمية، حلول إدارة الوثائق، المسح الضوئي والتصوير، وحلول تكامل الأنظمة.

على الجهات تطوير عمليات وإجراءات تتوافق مع قانون دولة قطر رقم (2) لسنة 2011 بشأن الإحصاءات الرسمية، عند الاقتضاء، لتغطية جميع جوانب إنشاء والحصول على البيانات، وبقدر الإمكان أتمتة خطوات العملية.

1.2 التخزين والإدارة

بمجرد اكتمال عملية جمع وإنشاء البيانات، لا بد من تخزينها على نحو يمكن من دعم الأعمال بأفضل طريقة ممكنة. وتتضمن المرحلة الثانية إدارة البيانات التي تم الحصول عليها وتخزينها في البنية التحتية لتكنولوجيا المعلومات في المنظمة، وفقاً لسياساتها التشغيلية. وتشمل العناصر الرئيسية في هذه المرحلة من إدارة دورة حياة المعلومات ما يلي:

1.2.1 تصنيف البيانات

إن الغرض الأساسي من تصنيف المعلومات إلى درجات، هو التحقق من وجود تقييم صحيح لبنود المعلومات، وتحديد مخاطرها، وإجراءات الحماية المناسبة الواجب تطبيقها. ويجب تصنيف جميع البيانات التي تم إنشاؤها والحصول عليها وفقاً لسياسة تأمين المعلومات الوطنية - الإصدار الثاني.

1.2.2 أمن البيانات وإمكانية الوصول إليها

لا بد من مراعاة الأمن المادي، وأمن الشبكات، وأمن أنظمة الكمبيوتر والملفات، لضمان سلامة البيانات ومنع النفاذ غير المصرح به، أو أي تغييرات على البيانات أو الكشف عنها أو إتلافها. ويجب أن تكون الترتيبات الأمنية متناسبة مع طبيعة البيانات والمخاطر التي قد تتعرض لها.

من ضمن أهم الخطوات الأخرى في هذه العملية للمساعدة في اكتشاف طبيعة البيانات وسهولة الوصول إليها، فهرسة البيانات والكشف عن البيانات الوصفية من خلال واجهة قابلة للبحث.

أدناه بعض الممارسات التأمينية للبيانات:

- يتطلب الأمن المادي للبيانات ما يلي:
 - التحكم في دخول الغرف والمباني التي توضع فيها البيانات وأجهزة الكمبيوتر أو الوسائط.
 - تسجيل جميع حالات إزالة أو الوصول إلى الوسائط أو المواد المطبوعة داخل غرف التخزين.
 - مراعاة عدم نقل البيانات الحساسة إلا في حالات استثنائية، حتى لو كان النقل لأغراض التصليح. على سبيل المثال، قد يشكل إعطاء محرك أقراص صلبة به خلل ويحتوي على بيانات حساسة إلى شركة مصنعة لأجهزة كمبيوتر خرقاً لإجراءات التأمين والسلامة.
- أمن الشبكات يعني:
 - عدم تخزين بيانات سرية مثل تلك التي تحتوي على معلومات شخصية على الخوادم أو أجهزة الكمبيوتر المتصلة بشبكة خارجية، خاصة الخوادم التي تستضيف خدمات الإنترنت.
 - نظام جدار الحماية (Firewall) والتحديثات المتعلقة بالأمن ووضع رقع واقية على أنظمة التشغيل لتجنب الفيروسات والشفرات الخبيثة.
- قد يشمل أمن أنظمة الكمبيوتر والملفات ما يلي:
 - إغلاق نظام الكمبيوتر باستخدام كلمة مرور وتركيب نظام جدار الحماية.
 - حماية الخوادم بأنظمة الحماية من طفرات الطاقة من خلال تركيب أنظمة إمدادات الطاقة غير المتقطعة (UPS).
 - تطبيق إجراءات الحماية للملفات البيانات من خلال كلمة المرور والتحكم بالدخول، على سبيل المثال، حظر الدخول، للقراءة فقط، للقراءة والكتابة، فقط بإذن من الشخص المسؤول.
 - التحكم في الوصول إلى المواد المحظورة، عن طريق التشفير.
 - إلزام المديرين أو مستخدمي البيانات السرية باتفاقيات الحفاظ على السرية وعدم الإفشاء.
 - عدم إرسال بيانات شخصية أو سرية عبر البريد الإلكتروني أو أي وسائل أخرى لتحويل الملفات بدون تشفيرها أولاً.
 - تدمير البيانات بطريقة منتظمة عند الحاجة.
 - عدم استخدام خدمات تداول الملفات مثل مستندات جوجل أو برنامج دروبوكس (Dropbox) وغيرها من الوسائل غير الآمنة.
 - تفعيل نظام تعقب للمراجعة ونظام التحكم في الإصدار لتعقب التعديلات على الأنظمة وقواعد البيانات.
- أمن البيانات الشخصية:
 - يجب معاملة البيانات التي تحتوي على معلومات شخصية بمستويات أعلى من الأمن مقارنة بغيرها. ومن الممكن جعل التأمين أسهل عن طريق:
 - إخفاء مصدر البيانات أو تجميع البيانات.
 - إزالة المعلومات الشخصية مثل الأسماء والعناوين من ملفات البيانات، وتخزينها على نحو منفصل.

○ تشفير البيانات التي تحوي معلومات شخصية قبل تخزينها – ومن المعلوم بالضرورة أن يتم التشفير قبل البث.

على الجهات تحديد عمليات وإجراءات أمن المعلومات بما يتماشى مع [سياسة تأمين المعلومات الوطنية - الإصدار الثاني](#).

1.2.3 جودة البيانات

تعتبر البيانات ذات نوعية جيدة إذا كانت مكتملة ودقيقة ومتاحة في الوقت المناسب. ومن الأخطاء الشائعة التي تؤثر على جودة البيانات السجلات الرئيسية المكررة، وعدم وجود معايير مشتركة وغياب الروابط بين عناصر المعاملات. وتشمل الخطوات الرئيسية في عملية جودة البيانات الآتي:

● تقييم البيانات:

تتألف مرحلة تقييم البيانات من تحليل هياكل البيانات ورسم مخطط يتضمن كل التفاصيل بين أنظمة المصدر وأنظمة الوجهة. وتعنى هذه المرحلة بتحديد متطلبات تنقية البيانات ووضع الأولويات.

● ضبط جودة البيانات:

تركز هذه المرحلة على تصحيح وتوحيد البيانات لمراقبة سلامة البيانات على مر الزمن، وتشمل أساساً ثلاث خطوات: مقايسة البيانات، تنقية البيانات وتجميع البيانات. وبينما تضمن مقايسة البيانات اتساق البيانات في كافة الأنظمة، تتم تنقية البيانات لضمان سلامة البيانات وإعدادها لتلبية احتياجات نقل محددة. أما تجميع البيانات فهو يحد ويقلل من المعلومات المكررة وغير الضرورية في مستودع البيانات.

● التحقق من جودة البيانات

يجب إجراء اختبارات دورية للتحري عن أي أخطاء في البيانات. إن التحقق من البيانات يوفر القدرة على اكتشاف الأخطاء وأسباب ذلك والإجراءات التصحيحية الممكنة.

على الجهات إنشاء إطار جودة معلومات يتميز بالاستمرارية والاتساق لضبط جودة البيانات.

1.2.4 النسخ الاحتياطي للبيانات

الغرض الرئيسي من النسخ الاحتياطي هو استعادة البيانات بعد فقدانها، سواء كان ذلك بسبب حذف البيانات أو تلفها. ويشكل النسخ الاحتياطي عموماً جزءاً من خطط مجابهة الكوارث في المؤسسة. على الجهات وضع عمليات للنسخ الاحتياطي بما يتفق مع [سياسة تأمين المعلومات الوطنية - الإصدار الثاني](#) - وسياسات وإجراءات التعافي من الكوارث.

1.2.5 التخلص من البيانات وأرشفتها

التخلص من البيانات يعني محو البيانات التي أصبحت بالية أو زائدة عن الحاجة ولا داعي لحفظها أو أرشفتها بشكل آمن، بينما تعني الأرشفة فرز ونقل البيانات الخاملة من أنظمة الإنتاج الحالية إلى أنظمة متخصصة لتخزين المحفوظات لمدد طويلة.

تتضمن هذه العملية خطوة أساسية هي تحديد سياسات حفظ بيانات المؤسسة. وفيما يلي بعض الأحكام القانونية والتنظيمية المعمول بها في دولة قطر بشأن حفظ السجلات¹⁷:

- حفظ السجلات المتعلقة بتحديد هوية العملاء لمدة 6 سنوات من نهاية العلاقة (هيئة مركز قطر للمال – لوائح مكافحة غسيل الأموال، المادة 10).
- حفظ الدفاتر المحاسبية الخاصة بجميع التجار (بما في ذلك الشركات) والمؤسسات لمدة 10 سنوات، ويجب الحفاظ على الوثائق الأساسية لمدة 5 سنوات (القانون التجاري، المادة 28).
- على دافعي الضرائب الذين يزاولون نشاطاً في دولة قطر الاحتفاظ بالدفاتر المحاسبية والسجلات والمستندات وفقاً للمعايير المحاسبية الدولية (قانون ضريبة الدخل، المادة 18)، وذلك لمدة 10 سنوات في المكان الذي يتم فيه مزاوله النشاط (قانون ضريبة الدخل، المادة 19).
- على جميع مؤسسات هيئة مركز قطر للمال حفظ السجلات المحاسبية لمدة 6 سنوات من نهاية الفترة المحاسبية أو حتى إتمام أي استفسارات حول العوائد للفترة المحاسبية (LLC: لوائح شركات هيئة مركز قطر للمال، المادة 79؛ LP: لوائح الشراكة لهيئة مركز قطر للمال، المادة 62؛ LLP: لوائح شركات هيئة مركز قطر للمال ذات المسؤولية المحدودة، المادة 34؛ الفروع التابعة لشركات غير مسجلة في هيئة مركز قطر للمال: لوائح الشراكة في هيئة مركز قطر للمال، المادة 81).

يجب على الجهات مراجعة جميع التشريعات واللوائح والمعايير المعمول بها وتحديد سياسات حفظ البيانات على أساس نطاق تطبيقها على أنواع البيانات التي تحتفظ بها، وذلك بما يتماشى مع [سياسة تأمين المعلومات الوطنية - الإصدار الثاني](#) - (المادة 11، حفظ البيانات والمحفوظات الجزء ب - حوكمة التأمين، وعمليات التأمين، دليل تأمين المعلومات الوطنية القطرية). يجب على الجهات أيضاً إنشاء نظام آمن للتخلص من البيانات وأرشفتها استناداً إلى السياسات الموضوعية.

1.3 التوزيع والتعامل

خلال هذه المرحلة، غالباً ما يتم إرسال البيانات بمجرد إنشائها وتخزينها إلى أحد مسارات العمل لتوجيهها كجزء من العمل. ولمعالجة البيانات، فإنه يتم تصفحها وتداولها بنشاط من قبل الجهات الحكومية وموظفيها في هذه المرحلة. ويتم تحديد القواعد الخاصة بأحقية الوصول إلى أي سجلات في المرحلة السابقة، بحيث توفر بيئة مناسبة للنفذ السهل إلى معلومات آنية ودقيقة ومتاحة، في إطار المبادئ التوجيهية المتعلقة بالأمن والخصوصية. ويجب على الجهات إرساء عمليات من شأنها تسهيل اكتشاف وتصفح البيانات المدخلة، وإدارة البيانات المنتجة.

¹⁷ القوانين المذكورة اعلاه هي أمثلة فقط ولا تمثل بالضرورة قائمة حصرية. وعلى الجهات مراجعة كل التشريعات المعمول بها لتحديد سياسات أمد حفظ البيانات. التشريعات والسياسات إلخ خاضعة للتعديل والتغيير لذا يجب مراجعتها دورياً للتأكد من استمرارية سريانها في ضوء التعديلات والتغييرات.

الملحق 2: نموذج بيان الخصوصية

هذا هو الموقع الإلكتروني ل(اسم الوزارة / الجهة)

نحن ملتزمون بحماية خصوصيتك وتوفير بيئة إلكترونية آمنة، ونتخذ الاحتياطات اللازمة لحماية المعلومات الخاصة بك. وعندما تقدم معلومات حساسة عبر شبكة الإنترنت، تأكد أن معلوماتك تجد الحماية الكافية سواء على الإنترنت أو خارج الشبكة.

جمع واستخدام وتداول وتصحيح المعلومات:

إذا كنت تتصفح هذا الموقع فقط، تأكد بأننا لن نطلع على أي معلومات تتيح لنا التعرف على هويتك الشخصية.

إذا كنت ترغب في تقديم طلب لخدمة إلكترونية عبر الإنترنت يحوي معلومات شخصية تتعلق بك، فقد نقوم بتداول هذه البيانات مع جهات حكومية أخرى، أو مع جهات غير حكومية مخولة لتقديم خدمات حكومية محددة، وذلك لخدمتك بطريقة فعالة و متميزة، ما لم يكن مثل هذا التبادل محظوراً بحكم القانون.

من أجل راحتك، قد نعرض لك البيانات التي قدمتها لنا أو لجهات حكومية أخرى سابقاً، وسيساعد هذا على تسريع المعاملات، كما يوفر عليك الوقت الذي ستستغرقه في تزويدنا بنفس المعلومات التي أرسلت بها من قبل.

وبالرغم من أننا سوف نبذل كل ما بوسعنا لتحديث المعلومات الخاصة بك، يرجى التكرم بتزويدنا بأحدث المعلومات التي تخصك إذا رأيت أنها تحتاج إلى تحديث.

الأمن:

لحماية معلوماتك الشخصية، نود التأكيد على أن جميع وسائل التخزين الإلكتروني ونشر البيانات الشخصية قد جرى تأمينها باستخدام التقنيات الأمنية المناسبة.

الاتصال بمواقع إلكترونية خارجية:

قد يحتوي هذا الموقع على روابط لمواقع خارجية غير حكومية تختلف تداويرها المتعلقة بحماية البيانات وسياسة الخصوصية عن ممارساتنا نحن، وبالتالي فنحن لا نتحمل أي مسؤولية تجاه ممارسات وسياسات المحتوى والخصوصية لدى تلك المواقع الأخرى.

يرجى الاتصال بنا باستخدام نموذج الملاحظات التفاعلية لموقعنا في حالة:

- أ. الاستفسار أو إبداء ملاحظات حول سياستنا وإجراءاتنا المتعلقة بحماية البيانات، أو
- ب. إذا كنت في حاجة لمزيد من المعلومات حول البيانات التي أرسلتها إلينا أو حول الوصول إليها.

تحديثات سياسة الخصوصية:

قد تتغير سياسة الخصوصية للموقع من وقت إلى آخر، وسوف يتم نشر كافة التحديثات على هذه الصفحة.

الملحق 3: نموذج معايير البيانات

ملاحظات	تاريخ النشر يوم/شهر/سنة	آخر إصدار	نظام السجل	الإدارة الراعية	الجهة الراعية	عنصر البيانات الفرعي	عنصر البيانات الأصلي	مخطط XML	بطاقة XML	القيمة (نموذج)	الطول	الشكل	الوصف	عنصر البيانات	م
	16/01/2014	2.0	System Z	الإدارة Y	الجهة X	رقم المبنى معلومات عن الموقع معلومات عن المدينة	(عنصر الجذر)	عنوان-v2-0.xsd	تركيبية العنوان				تمثل تركيبية العنوان في قطر	تركيبية العنوان	1.0.0
	01/09/2013	1.0	System Z	الإدارة Y	الجهة X		تركيبية العنوان	مبنى-v1-0.xsd	رقم المبنى	18-A	5	حرف ابجدي رقمي	يحدد رقم المبنى	رقم المبنى	1.1.0
	16/01/2014	1.1	System Z	الإدارة Y	الجهة X	اسم الموقع اسم الشارع رقم المنطقة	تركيبية العنوان	موقع-v1-1.xsd	معلومات عن الموقع				يحدد الموقع في مدينة	معلومات الموقع	1.2.0
	01/09/2013	1.0	System Z	الإدارة Y	الجهة X	معلومات عن الموقع	معلومات عن الموقع	اسم الموقع-v1-0.xsd	اسم الموقع	المرخية	30	حرف ابجدي رقمي	يحدد اسم الموقع	اسم الموقع	1.2.1
	01/09/2013	1.0	System Z	الإدارة Y	الجهة X	معلومات عن الموقع	معلومات عن الموقع	الشارع- v1-0.xsd	اسم الشارع	الخليفة	30	حرف ابجدي رقمي	يحدد معلومات عن الشارع	رقم الشارع	1.2.2
	16/01/2014	1.1	System Z	الإدارة Y	الجهة X	معلومات عن الموقع	معلومات عن الموقع	المنطقة v1-1.xsd	رقم المنطقة	67	5	رقمي	يحدد رمز المنطقة	رقم المنطقة	1.2.3
	01/09/2013	1.0	System Z	الإدارة Y	الجهة X	تركيبية العنوان	تركيبية العنوان	المدينة 0.xsd-v1-	يحدد اسم المدينة	الدوحة	30	حرف ابجدي رقمي	يحدد اسم المدينة	اسم المدينة	1.3.0

* هذا مجرد نموذج ولا يمثل بياناً لمعايير البيانات الفعلية

قد يتوسع هذا القالب كلما تم تطوير معايير بيانات إضافية ومع استمرار الجهات في التعاون والتنسيق

إعداد من قبل
وحدة السياسات والمعايير
وزارة المواصلات والاتصالات
النسخة رقم 1.0.1 لسنة 2015

البريد الإلكتروني: policy@motc.gov.qa
www.motc.gov.qa