الإدارة العامة للبيانات وذكاء الأعمال

1. سياسة تصنيف البيانات

V1.0

May 2023

جدول المحتويات

1. سياسات وإجراءات الإدارة العامة للبيانات وذكاء الأعمال

1.1. سياسة تصنيف البيانات

اسم السياسة	سياسة تصنيف البيانات		
الرمز المرجعي	CPP.711.DBI. 1.2023.V1.0		
رقم الإصدار	01	تاريخ الإصدار	May 2023

الاعتمادات

المهمة	الإدارة المسؤولة	التاريخ	التوقيع
إعداد	مدير عام الإدارة العامة للبيانات وذكاء الاعمال عبدالرحمن خياري (مكلف)	24/5/2023	
اطلاع	مدير عام الإدارة العامة للأمن السيبراني م. علي الغامدي	23-05-2023	
موافقة	مدير عام الإدارة العامة للتميز المؤسسي أ. غيداء السليمان	31-05-2023	
اعتماد	الرئيس التنفيذي للتطوير والتميز المؤسسي م.محمد الثنيان	31-05-2023	

سجل المراجعات

الإصدار	تاريخ المراجعة	سبب المراجعة	المراجع	المعتمد

سجل التغييرات

الإصدار	الأقسام التي تم تغييرها	الوصف	سبب التغيير	الإصدار الجديد	تاريخ الإصدار

1. الهدف

تهدف هذه السياسة إلى وضع السياسات والإجراءات لتصنيف جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الهيئة السعودية للتخصصات الصحية مهما كان مصدرها أو شكلها أو طبيعتها، والتأكد من أن بيانات الهيئة مصنفة حسب حساسية البيانات وطبيعتها ودرجة أثرها وذلك من أجل بناء الضوابط الأساسية لأمن وحماية وخصوصية البيانات.

2. التعريفات

2.1 البيانات: مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصور الثابتة أو التسجيلات المرئية أو التسجيلات الصوتية أو الرموز التعبيرية او الوثائق او السجلات الورقية.

2.2 البيانات الشخصية: كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر - الاسم، رقم الهوية الشخصية، العنوان، رقم التواصل، رقم الحساب البنكي والبطاقة الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

2.3 سرية البيانات: الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.

2.4 البيانات المحمية: البيانات المصنّفة على أنها (سري للغاية، سري، مقيّد).

2.5 البيانات الحساسة: البيانات التي يؤدي فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنية أو أنشطة الجهات الحكومية أو خصوصية الأفراد وحماية حقوقهم.

2.6 جهة التحكم: أي جهة حكومية أو شخصية ذات صفة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك؛ سواء تمت معالجة البيانات بواسطتها أو من خلال جهة المعالجة.

2.7 تصنيف البيانات: تقسيم البيانات إلى مستويات وفقاً لتقييم الأثر المحتمل في حالة الإفصاح غير المصرح به نظاماً عن البيانات أو عن محتواها.

2.8 علامات التصنيف: علامات أو نصوص توضع وفق صيغ محددة على البيانات المصنفة تبين مستوى التصنيف، ومدته، لضمان توفير الحماية المناسبة لها.

2.9 مستويات تصنيف البيانات: مستويات التصنيف التالية: "سري للغاية"، "سري"، "مقيّد"، "عام".

2.10 تسريب البيانات الشخصية: الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.

2.11 ممثل بيانات الأعمال: هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الإدارة الداخلية المالكة للبيانات أو الجهة العامة التي يعمل بها.

3. السياسات

3.1 يجب أن يكون لدى إدارة حوكمة البيانات معايير لتصنيف البيانات ويتم تطبيقها على جميع بيانات الهيئة السعودية للتخصصات الصحية .

3.2 يجب على إدارة حوكمة البيانات تحديد مالك البيانات لكل مجموعات البيانات.

3.3 . يجب على إدارة حوكمة البيانات مراجعة تصنيف البيانات بشكل دوري (مره في السنة).

3.4 يجب على إدارة حوكمة البيانات التأكد بأن مالك البيانات وممثلي بيانات الاعمال وتقني وفنيين البيانات تم تحديدهم وتفعيل ادوارهم لدى الهيئة السعودية للتخصصات الصحية.

3.5 يجب على إدارة حوكمة البيانات التأكد بأن جميع بيانات الهيئة السعودية لتخصصات الصحية مصنفة.

3.6 ممثلي بيانات الاعمال مسؤولين عن اختيار التصنيف المناسب للبيانات بناء على سياسة تصنيف البيانات بالتنسيق مع مالك البيانات .

3.7 يجب على إدارة حوكمة البيانات التأكد بأنه تم تصنيف البيانات بالشكل الصحيح وبناء على سياسة تصنيف البيانات قبل اعتماد التصنيف.

3.8 في حال تم اكتشاف ان البيانات مصنفة بشكل غير صحيح او لم يتم تصنيفها بناء على سياسة تصنيف البيانات، يجب على ممثلي بيانات الاعمال ابلاغ إدارة حوكمة البيانات لاتخاذ الاجراء الازم .

3.9 يجب على ممثلي بيانات الاعمال تصنيف البيانات الخاصة بهم بناء على معايير تصنيف البيانات.

3.10 يجب على مالك البيانات، ممثلي بيانات الاعمال, تقني وفني البيانات فهم معايير الخصوصية والمخاطر مع البيانات التي تتدفق ضمن انشطتهم, وابلاغ إدارة حوكمة البيانات وإدارة الأمن السيبراني في حال وجود أي تسريب او خطر على البيانات.

3.11 في حالة الخلاف حول مستوى التصنيف الذي سيتم استخدامه, يجب اعتماد المستوى الأكثر أماناً.

3.12 في حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقًا لمعايير التصنيف، تُعامل هذه البيانات على أنها "مقيّدة" حتى يتم تصنيفها بشكل صحيح.

3.13 يجب على إدارة حوكمة البيانات تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقا لمستويات التصنيف.

3.14 يجب على ممثل بيانات الاعمال او مدير حوكمة البيانات تحديد كيانات البيانات التي يجب تصنيفها.

3.15في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال وإدارة حوكمة البيانات لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.

3.16 يجب الغاء تصنيف البيانات أو خفض مستوى تصنيفها بعد انتهاء مدة التصنيف او عندما لا تكون الحماية مطلوبة أو انها لم تعد مطلوبة على المستوى الأصلي للتصنيف.

4. المبادئ والضوابط الخاصة بتصنيف البيانات بحسب مكتب إدارة البيانات الوطنية:

4.1 مبادئ تصنيف البيانات.

4.1.1 المبادئ الرئيسية لتصنيف البيانات

4.1.1.1 المبدأ الأول: الاصل في البيانات الاتاحة:

4.1.1.1.1 الأصل في البيانات أن تكون متاحة مالم تقتضٍ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية؛ وسرية للغاية مالم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

4.1.2 المبدأ الثاني: الضرورة والتناسب:

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

4.1.3 المبدأ الثالث: التصنيف في الوقت المناسب:

4.1.3.1 يتم تصنيف البيانات عند أنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.

4.1.4 المبدأ الرابع: المستوى الأعلى من الحماية:

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

4.1.5 المبدأ الخامس: فصل المهام:

4.1.5.1 يتم الفصل بين مهام ومسؤوليات العاملين- فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو اتلافها- بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤولية.

4.1.6 المبدأ السادس: الحاجة الى المعرفة:

4.1.6.1 يتم تقييد الوصول الى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة, ولأقل عدد من العامليين.

4.1.7 المبدأ السابع: الحد الأدنى من الامتيازات:

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

4.2 ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم الادارة العامة للبيانات وذكاء الاعمال بمساعدة الإدارة العامة للأمن السيبراني بتحديد الضوابط الأمنية المناسبة والإشراف على تطبيقها لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن.

كما يجب تصنيف البيانات التي لم يتم تصنيفها وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل تعدها الإدارة العامة للبيانات وذكاء الاعمال ويتم اعتمادها من سعادة امين عام الهيئة.

أدناه الأمثلة على الضوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرجوع إلى ما يصدر من الهيئة الوطنية للأمن السيبراني من ضوابط وإرشادات تتعلق بحماية البيانات:

4.1 علامات الحماية

4.1.1 يجب على الإدارة العامة للأمن السيبراني تُطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقًا لكل مستوى من مستويات التصنيف.

4.2 الوصول

4.2.1 يُمنح الوصول – المنطقي والمادي - إلى البيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة".

4.2.2 يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو انهاء الخدمة المهنية للعاملين بالجهة.

4.3 الاستخدام

4.3.1 تُستخدم البيانات المصنفة وفقًا لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" على مواقع محددة سواء مادية – كالمكاتب – أو افتراضية - باستخدام ترميز الأجهزة أو تطبيقات خاصة.

4.3.2 يجب ان يتم معالجة البيانات الشخصية داخل الحدود الجغرافية للمملكة العربية السعودية.

4.4 التخزين

4.4.1 لا تُترك البيانات المصنفة على أنها "سري للغاية" و"سري" و "مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.

4.4.2 يجب على الإدارة العامة للأمن السيبراني حماية البيانات المصنفة على أنها "سري للغاية" و"سري" و "مقيّد" الغير المراقبة أثناء تخزينها مادياً أو إلكترونيًا باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

4.4.3 يجب أن يكون تخزين البيانات الشخصية داخل الحدود الجغرافية للمملكة العربية السعودية.

4.5 مشاركة البيانات

4.5.1 تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.

4.5.2 يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجهات ستستخدم الوسائل المستخدمة حاليًا لتبادل البيانات أم لا، على سبيل المثال قناة التكامل الحكومية وشبكة مركز المعلومات الوطني والشبكة الحكومية الآمنة، أو إعداد اتصال مباشر جديد أو وسائط التخزين القابلة للإزالة أو الشبكة اللاسلكية، أو الوصول عن بعد، أو الشبكة الخاصة الافتراضية...الخ.

4.6 الاحتفاظ بالبيانات

4.6.1 يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات والبيانات الشخصية المصنفة من قبل الإدارة العامة للبيانات وذكاء الاعمال.

4.6.2 يتم تحديد فترة الاحتفاظ بناءً على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة.

4.6.3 يتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

4.7 التخلص من البيانات

4.7.1 يتم التخلص من جميع البيانات بشكل آمن وفقًا للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال تحت اشراف الإدارة العامة للأمن السيبراني والإدارة العامة للبيانات وذكاء الاعمال.

4.7.2 يتم التخلص من البيانات التي تم تصنيفها على أنها "سرية للغاية" و"سري" التي يتم التحكم بها الكترونياً باستخدام أحدث طرق التخلص من الوسائط الإلكترونية تحت اشراف الإدارة العامة للأمن السيبراني والإدارة العامة للبيانات وذكاء الاعمال.

4.7.3 يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.

4.7.4 يتم إعداد سجل مفصّل عن جميع البيانات التي تم التخلص منها.

4.8 الأرشفة

4.8.1 يتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يوصي بها ممثل بيانات الأعمال.

4.8.2 يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.

4.8.3 يتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و"سري" باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

4.8.4 يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

4.9 إلغاء التصنيف (رفع السرية)

4.9.1 يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها للحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.

4.9.2 يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، قد تتضمن هذه العوامل ما يلي:

4.9.2.1 فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (على سبيل المثال، عامين بعد الإنشاء).

4.9.2.2 فترة زمنية محددة بعد اتخاذ أخر إجراء على البيانات (على سبيل المثال، ستة أشهر من تاريخ آخر استخدام).

4.9.2.3 بعد انقضاء تاريخ محدد (على سبيل المثال، من المقرر مراجعتها في 1 يناير 2021).

4.9.2.4 بعد ظروف أو أحداث معينة تؤثر تأثيرًا مباشرًا على البيانات (على سبيل المثال، إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية).

4.9.3 يتطلب إلغاء التصنيف – رفع السرية - أو خفض مستويات التصنيف، بعيدًا عن العوامل المساعدة على إلغاء التصنيف الواضحة تمامًا، فهمًا سليمًا لمحتوى البيانات السرية والسياق الذي وردت فيه.

5 الإجراءات

#	المسؤول	المهمة	النماذج
1	إدارة حوكمة البيانات	- تحديد كيانات البيانات من اجل بدأ عملية التصنيف. - تعيين مهام تصنيف البيانات الى مختص بيانات الاعمال.	-

#	المسؤول	المهمة	النماذج
2	**مختص بيانات الأعمال (Data Steward)**	- يحدد مختص بيانات الأعمال مستوى تصنيف البيانات بناءً على الآثار المحددة ومستوياتها (عالي، متوسط، منخفض، لا يوجد أثر)، ومن ثم تصنيف البيانات. - تحديد الفئة المتأثرة من عملية تصنيف البيانات. - تحديد مستوى التأثير: عالي: تصنف على انها بيانات سرية للغاية وبذلك ينتهي الاجراء. متوسط: تصنف على انها بيانات سرية وبذلك ينتهي الاجراء. منخفض: تصنف على انها بيانات عامة وبذلك ينتهي الاجراء. - تقييم بيانات منخفضة التأثير إذا تتعارض مع القانونين تصنف على انها بيانات سرية وبذلك ينتهي الاجراء. - اذا لم تتعارض مع القوانين، يتم تقييم إذا كانت فوائد الإفصاح تفوق على التأثيرات السلبية: إذا نعم، تصنف سرية وتضاف علامة الخصوصية وبذلك ينتهي الاجراء. إذا لا، تصنف عامة وبذلك ينتهي الاجراء.	-
3	**مشرف ممثلي بيانات الأعمال**	- مراجعة واعتماد مستويات تصنيف البيانات التي يحددها ممثل بيانات الأعمال.	-

#	المسؤول	المهمة	النماذج
	(Lead Data Steward)		
4	مالك البيانات (Data Owner)	- الاعتماد النهائي لتصنيف البيانات بعد مراجعة واعتماد مشرف ممثل البيانات.	-
5	إدارة حوكمة البيانات	- مراجعة واعتماد النهائي لتصنيف البيانات.	-
6	الإدارة العامة للأمن السيبراني	- تعيين ضوابط للتعامل مع البيانات وحمايتها بناء على تصنيفها لضمان معالجة ومشاركة والتعامل والتخلص من البيانات بشكل امن من خلال اتباع لوائح الهيئة الوطنية للأمن السيبراني.	-

6 مستويات تصنيف البيانات

مستوى التصنيف	درجة الأثر	الوصف
سري للغاية	عالي	تصنف البيانات على أنها "بيانات سرية للغاية" إذا كان الوصول غير مصرح به الى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي الى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على: - المصالح الوطنية بما في ذلك الإخلال بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة المملكة أو بالعلاقات

مستوى التصنيف	درجة الأثر	الوصف
		الدبلوماسية والانتماءات السياسة أو الكفاءة التشغيلية للعمليات الأمنية، أو العسكرية، أو اقتصاد الوطني، أو البنية التحتية الوطنية، أو الاعمال الحكومية. - أداء الجهات العامة مما يلحق ضرراً بالمصلحة الوطنية. - صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين. - الموارد البيئية أو الطبيعية.
سري	متوسط	تصنف البيانات على انها "بيانات سرية" إذا كان الوصول غير مصرح به الى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي الى ضرر جسيم على: - المصالح الوطنية مثل إلحاق ضرر جزئي بسمعة المملكة والعلاقات الدبلوماسية أو الكفاءة التشغيلية للعمليات الأمنية، أو العسكرية، أو الاقتصاد الوطني، أو البنية التحتية الوطنية والأعمال الحكومية. - يُحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية او كليهما معاً. - يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد. - تؤودي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية. - التحقق في القضايا الكبرى المحددة نظاما, كقضايا تمويل الإرهاب.

مستوى التصنيف	درجة الأثر	الوصف
مقيد	منخفض	تصنف البيانات على انها "مقيد" كان الوصول غير المصرح به الى هذه البيانات أو الإفصاح عنها أو عن محتوها يؤدي إلى: - تأثير سلبي محدود على عمل الجهات العامة أو الأنشطة الاقتصادية في المملكة أو على عمل شخص معين. - ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي التنافسي. - ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية.
عام	لا يوجد	تصنف البيانات على أنها "بيانات عامة" عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الاثار أعلاه- في حال عدم وجود تأثير على مأتى: - المصلحة الوطنية. - نشطة الجهات. - مصالح الأفراد. - الموارد البيئة.

7 علامات الخصوصية

علامات الخصوصية	نوع البيانات	أمثلة
بيانات حساسة	البيانات التعرف الشخصية	الاسم الأول, اسم العائلة, البريد الالكتروني , رقم الجوال, الهوية او الإقامة, العنوان, صورة شخصية, التوقيع, عنوان بروتوكول

علامات الخصوصية	نوع البيانات	أمثلة
	البيانات تدل على الأشخاص	الانترنت, لوحة السيارة, رخصة القيادة, البصمة, تاريخ الميلاد.
	البيانات الشخصية البيانات المالية	الجنس, الحالة الزوجية, العمر, مكان الميلاد, المنطقة, الجنسية. رقم حساب البنك, رصيد البنك, رقم بطاقة الائتمان, الراتب, القروض.
	البيانات الشخصية البيانات الطبية	معلومات التأمين الطبي, الظروف الطبية الحالية, تاريخ الطبي, الأدوية, الحساسية, معلومات دخول المستشفى, معلومات الإعاقة, معلومات الخروج , نتائج المختبرات.
بيانات شخصية	البيانات الشخصية البيانات التعليمية	الشاهدات الاختصاصية, الشاهدات الجامعية, المعدل. تاريخ الالتحاق, تاريخ المغادرة, بيانات الحضور, بيانات الخروج من المكتب, بيانات الخدمة, بيانات طلبات الموارد البشرية, الدورات التدريبية, بيانات تقييم الأداء, بيانات العقود, الإدارة, المدير, المكان, المرتبة.
	البيانات الشخصية بيانات العمل	
	البيانات الشخصية بيانات السلوك الرقمي	بيانات تصفح الانترنت, ملفات تعريف الارتباط, بيانات تتبع العين.

علامات الخصوصية	نوع البيانات	أمثلة
بيانات المؤسسة	بيانات المؤسسة	بيانات البائعين المعتمدين, الصفقات الحالية, بيانات التدفق النقدي, القوائم المالية, بيانات تسعير المشاريع, بيانات الإيرادات والخسائر, القروض الحالية.

8 اتفاقيات مستوى الخدمة

#	الطرف الأول	الطرف الثاني	وصف العملية	المستهدف
1	لا ينطبق			

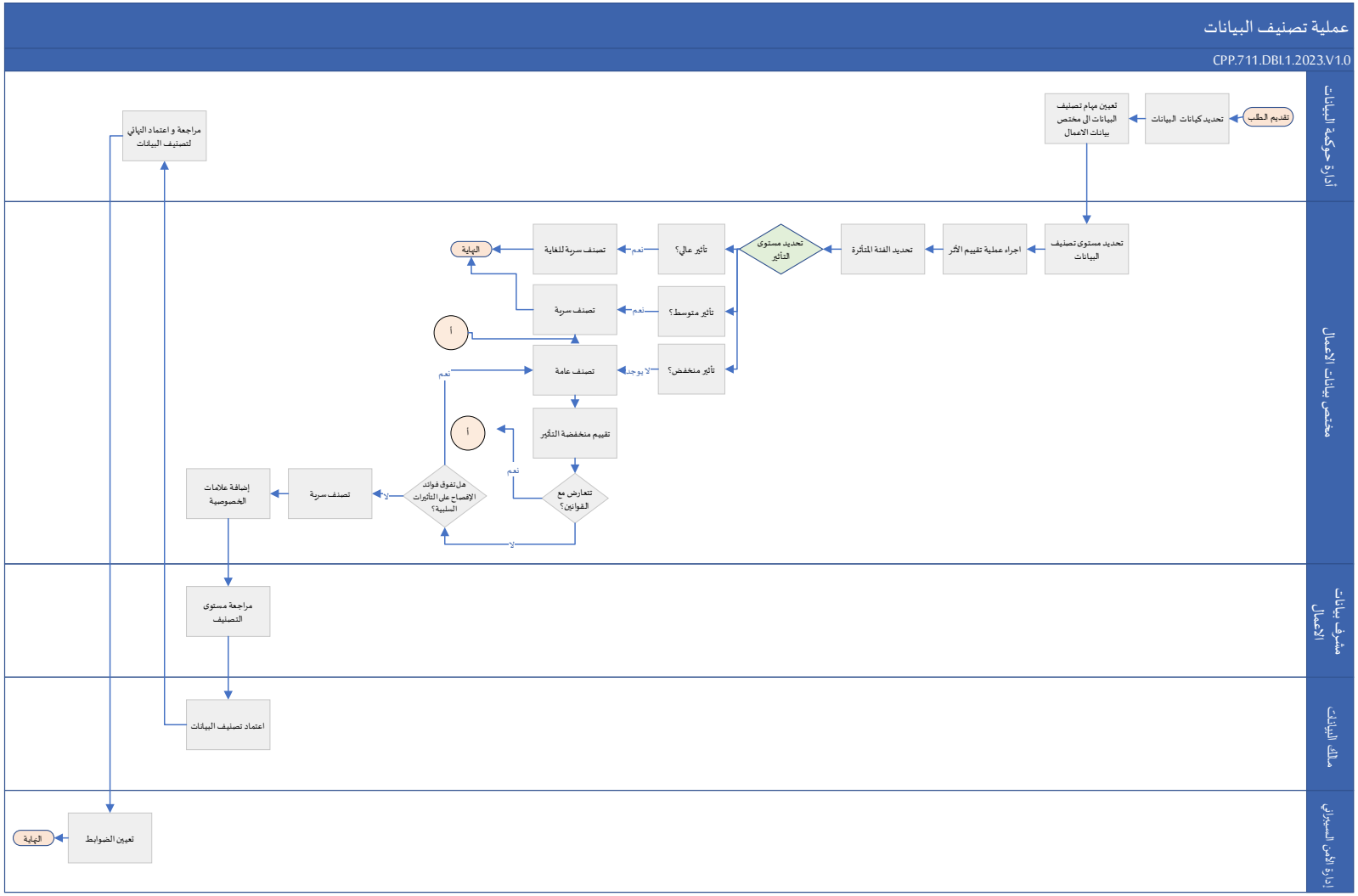
9 اللوائح العامة والقواعد التنفيذية

#	اسم اللائحة	الوصف
1	سياسات حوكمة البيانات الوطنية	السياسات الصادرة من مكتب إدارة البيانات الوطنية.
	ضوابط الهيئة الوطنية للأمن السيبراني	الضوابط الأساسية وغيرها من الضوابط ذات العلاقة الصادرة من الهيئة الوطنية للأمن السيبراني.

10 النماذج

#	رمز النموذج	اسم النموذج	الوصف
1	لا ينطبق		

11 خريطة تدفق العملية



12 مصفوفة المسؤوليات (RACI)

	مسؤول	محاسب	مستشار	مطّلع
إدارة حوكمة البيانات	✔			
مالك البيانات		✔		
مختص بيانات الأعمال	✔			
مشرف ممثلي بيانات الأعمال	✔			
إدارة الامن السيبراني			✔	

الملحقات

ملحق أ – النماذج

12 الملحق أ – النماذج

لا ينطبق

الملحقات

الملحق ب - مستندات أخرى

الملحق ب - مستندات أخرى

لا ينطبق