الدليل الإجرائي لحوكمة بيانات المشاريع

النسخة الأولى، أكتوبر2023

تصنيف الوثيقة: عام

وزارة الاقتصاد والتخطيط
MINISTRY OF ECONOMY & PLANNING

NDMO
مكتب إدارة البيانات الوطنية
National Data Management Office

قائمة المحتويات

المقدمة 3

نطاق التطبيق 3

الأهداف 3

خطوات مشاركة البيانات مع الاطراف الخارجية لأغراض تنفيذ المشاريع 3

توصيات عامة 6

الملحق 1 7

الملحق 2 7

المقدمة

يهدف هذا الدليـل الإجرائـي إلى مسـاعدة الجهـات الحكوميـة على الالتزام بسـياسـات حوكمة البيانات الوطنية والتي تضـع الضوابط المنظمة للتعامل مع البيانات الوطنية، بما في ذلك تصـنيفها ومشاركتها مع الأطراف الخارجية المتعاقدة مع الجهات الحكومية بما يتوافق مع ضوابط الأمن السيبراني للبيانات

نطاق التطبيق

ينطبق هذا الدليل على البيـانـات الحكومية مهما كان شـكلها أو طبيعتهـا، التي يتم مشـاركتها مع الأطراف الخارجية لتنفيذ الأعمال والمشاريع

الاهداف

يساعد الدليل الإجرائي على تحقيق الأهداف التالية:

- **المحافظة على البيانات الحكومية**: يسـاعد على تقييد الوصـول للبيانات المصـنفة للحد اللازم لتنفيذ متطلبات المشروع
- **تحسـين الكفـاءة والأمـان**: من خـلال تطبيـق أفضـل الممارسـات في رفع التوعيـة وتطبيق الضـوابط الأمنية والسيبرانية والتأكد من فعاليتها
- **ضـمان الالتزام :** يسـاعد في تسـهيل الالتزام بالمتطلبـات التنظيمية الأخـرى مثل سـياسـات حوكمة البيـانـات الوطنية والقواعد واللوائـح ذات الصـلة بتقنيـات الذكاء الإصـطنـاعي والتي تصـدرها الهيئة السـعودية للبيـانـات والذكـاء الاصطناعي وضوابط الأمـن السيبراني الصـادرة عن الهيئة الوطنية للأمن السيبراني

خطوات مشاركة البيانات مع الأطراف الخارجية لأغراض تنفيذ المشاريع

أولاً : تشكيل فريق عمل

على الجهة الحكومية المالكة للمشروع القيـام بتشكيل فريق عمل يتكون من: مالك المشروع مدير المشروع من إدارة المشـاريع ممثل إدارة المخـاطر المراجعة ممثل مكتب إدارة البيـانـات في الجهة ممثـل الأمـن السيبراني في الجهة ومن تراه الجهة المالكة للمشروع. ويتولى الفريق المشـكل المسـاهمة في حماية البيـانـات والحد من تسـربها عند مشـاركتها مع الأطراف الخـارجية وضـمان الالتزام بسـياسـات حوكمة البيـانـات الوطنية وضـوابط الأمـن السـيبراني للبيانات أثناء مراحل المشروع

مهام فريق العمل

1- تحديد درجة تصنيف المشروع

2- الأطراف الخارجية تحديد الحد الأدنى من البيانات التي يجب مشاركتها مع.

البيانات الحكومية: هي جميع البيانات – مهما كان شكلها أو مصدرها أو طبيعتها – التي يتم إنشاؤها أو الحصول عليها من قبل الجهات الحكومية في سياق ممارسة اختصاصاتها المقررة نظاما

3- مراجعة تصنيف البيانات المطلوبة قبل مشاركتها مع الأطراف الخارجية

4- دراسة وتقييم أثر البيانات المطلوبة من قبل الأطراف الخارجية

5- تحديد واقتراح البنود التعاقدية النظامية التي تكفل حماية البيانات وإدراجها ضـــمن النصـــوص المتغيرة وفق نماذج العقود المعتمدة لوزارة المالية - المتصلة بنظام المنافسات والمشتريات الحكومية

6- تحديد الضوابط المناسبة لضمان حماية البيانات الحكومية وفقاً لمستوى التصنيف

ثانياً: تقييم ودراسة أثر المشروع ووثائقه

على فريق العمل القيام بتحديد مستوى تصنيف المشروع وفقاً لسياسة تصنيف البيانات من خلال

أ- تحديد فئة الأثر وقد تشمل واحدة أو أكثر

- المصلحة الوطنية
- أنشطة الجهات
- صحة وسلامة الأفراد
- الموارد البيئية

ب- تحديد مستوى الأثر

- مدة الأثر وصعوبة السيطرة على الضرر
- فترة تدارك وإصلاح الأضرار بعد وقوعها
- حجم الأثر على مستوى وطني، مناطقي، عدة جهات، جهة واحدة، عدة أفراد ... إلخ

يمكن الاستفادة من أداة التصنيف لتحديد التصنيف المناسب

ثالثاً: آلية التعامل مع المشروع حسب التصنيف

أ- في حال كان تصنيف المشروع سري فأعلى

يقوم الفريق المشـكل بتحديد الآلية النظامية المناسـبة لطرح المشـاريع المصـنفة على سـري فأعلى. بعد ذلك، يقوم الفريق المشكل بتحديد الضوابط اللازمة لحماية البيانات عند مشاركتها

الحد الأدنى من الضوابط للمشاريع المصنفة سري فأعلى

1- إجراء المسح الأمني للأطراف الخارجية

2- تعهد الأطراف الخارجية بعدم استخدام تطبيقات التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية أو الخاصة بالطرف الخارجي لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجهة الحكومية باستثناء التطبيقات الآمنة المعتمدة من الجهات ذات العلاقة

3- تخصيص موقع ملائم لموظفي الطرف الخارجي لأداء اعمالهم مع توفير أجهزة مخصصة مملوكة للجهة يتم من خلالها مشاركة البيانات ومعالجتها للبيانات التي يحددها الفريق.

ملحق 2: أداة تصنيف البيانات

4- توفير عناوين بريد إلكتروني من قبل الجهة المالكة للمشـــروع لموظفي الطرف الخارجي، وحصـــر مشـــاركة البيانات من خلالها، مع التزام موظفـي الطرف الخارجي بعدم اســـتخدام عنـاوين البريد الإلكتروني الخاصـــة بالطرف الخارجي في الأعمال المتعلقة بالمشروع

5- تفعيل أنظمة التحكم بالدخول والخروج من الموقع المخصص على أن يكون للمصرح لهم فقط

6- منع خروج الأجهزة ووحدات التخزين والبيانات ، ومنع إدخال أي أجهزة الكترونية للقاعة.

7- يتم تقييد الوصول إلى البيانات واستخدامها للغرض المطلوب لأقل عدد من العاملين

8- استخدام طرق وخوارزميات آمنة للتشفير عند الانشاء والتخزين والمشاركة

ويمكن للجهة إضافة الضوابط المناسبة حسب ما تستدعيه حاجة المشروع مع عدم الإخلال بسياسات حوكمة البيانات الوطنية والأنظمة واللوائح ذات الصلة

ب- في حال كان تصنيف المشروع مقيد

يلتزم الفريق بتطبيق الضوابط التالية كحد أدنى

1- تعهد الأطراف الخارجية بعدم استخدام تطبيقات التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية لإنشـــاء أو تخزين أو مشـــاركة البيانات الخاصـــة بالجهة باســـتثناء التطبيقات الآمنة المعتمدة من الجهـات ذات العلاقة

2- يتم تقييد الوصول إلى البيانات واستخدامها للغرض المطلوب لأقل عدد من العاملين

3- استخدام طرق وخوارزميات آمنة للتشفير عند الإنشاء والتخزين والمشاركة

4- يتم التدرج في مشاركة البيانات وفقاً لسياسة مشاركة البيانات

ويمكن للجهة إضافة الضوابط المناسبة حسب ما تستدعيه حاجة المشروع مع عدم الإخلال بسياسات حوكمة البيانات الوطنية والأنظمة واللوائح ذات الصلة

رابعاً: مراجعة مستوى تصنيف بيانات المشروع أثناء التنفيذ

نظراً لما قد يطرأ من وجود بيانات مصـنفة على درجات السرية أثناء تنفيذ مشـاريع مصـنفة على مسـتوى مقيد أو عام، على الفريق المشكل القيام بالمراجعة الدورية للوثائق والمتطلبات التي يتم مشاركتها مع الأطراف الخارجية أثناء مرحلة التنفيذ. على أن يتم دراســـة أثر ذلك وتطبيق ما يلزم من الضـــوابط لحماية تلك البيانات. مع مراعاة الحاجة للمعالجة المســـبقة في حال تطلب الأمر ذلك، على ســـبيل المثال: الحجب وإخفاء الهوية والتجميع بالإضـــافة إلى ذلك، اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات بمستويات تصنيف مختلفة

خامساً: تقييم الأثر للمخرجات

على الجهة المتعاقدة مع الأطراف الخارجية في حال اسـتلامها للمخرجات والبيانات بتصـنيفها وفقاً لسـياسـة تصـنيف البيانات، وفي حال ُصـنفت البيانات من قبل الجهة المنفذة يتم مراجعة تصـنيفها، وعلى الجهة تطبيق ضـوابط الأرشـفة والتخزين الآمن للمخرجات التي تم اسـتلامها من قبل الأطراف الخارجية والتحقق من تطبيق الضـــوابط الآتية للأطراف الخارجية مثل: تنفيذ عمليات الاتلاف أو الحذف الآمن للبيانات، ومنع حق الوصول إلى البيانات بمجرد انتهاء المشروع

توصيات عامة

- تتولى الجهات الحكومية مواءمة هذا الدليل مع سياساتها الداخلية وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعدادها
- توازن الجهات الحكومية وبحسب طبيعة المشروع بين تصنيف البيانات وحق الاطلاع والحصول على المعلومات مع المتطلبات الضرورية الأخرى كتحقيق الأمن الوطني والمحافظة على سرية بيانات المشاريع وفقاً لمعيار الموازنة بين المزايا والآثار من سياسة تصنيف البيانات

- في المراحل الأولية من المشروع تقوم الجهة الحكومية بتضمين العقود البنود اللازمة للتأكد من التزام المتعاقد معه بحماية البيانات والمحافظة عليها وفق التزامات نظامية محددة. **على أن تشمل**

1- إجراء المسح الأمني حسب ما تستدعيه حاجة المشروع

2- خطاب موثق من الجهة المنفذة يتضمن التأكيد على أنه تم تسليم جميع وثائق المشروع أو اتلافها حسب الأحوال –تعتمده الجهة الحكومية بموافقة خطية- دون الإخلال بسياسات حوكمة البيانات الوطنية وضوابط الأمن السيبراني المتعلقة بالإتلاف

3- تطبيق علامات الحماية النصية على البيانات سواء بالصيغة الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات تصنيف البيانات

4- اتفاقية عدم الإفشاء ملائمة لاختصاصات المشروع وتوقيع الأطراف عليها (NDA) تصميم وثيقة

5- التوقيع على اتفاقية مشاركة البيانات في الأحوال التي تتطلب ذلك وفق سياسة مشاركة البيانات

6- تحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها

7- تعهد موظفي الجهات المنفذة بعدم استخدام تطبيقات التراسل أو التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية أو تقنيات الذكاء الإصطناعي لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجهة، باستثناء تطبيقات التراسل الآمنة المعتمدة من الجهات ذات العلاقة ووفقا للأنظمة واللوائح والقواعد ذات الصلة

ملحق (3) الخطوة 5 من الخطوات اللازمة لتصنيف البيانات

الملحق 1

أداة تصنيف البيانات

المصلحة الوطنية			
الفئة الفرعية (أمثلة مقترحة وليست شاملة)	الأسئلة	الجواب	التصنيف
الدفاع	بيانات عن مخازن الأسلحة والذخائر التابعة للقوات المسلحة؟		سري للغاية
	بيانات عن تحركات القوات المسلحة أو قوى الأمن الداخلي أو تحركات كبار الشخصيات؟		سري للغاية
	بيانات عن إجراءات الجهات أو القوات الأمنية في حالة الحرب؟	نعم	سري للغاية
البنية التحتية	بيانات عن مفاتيح وآليات التشفير المستخدمة في البنية التحتية الوطنية؟		سري للغاية
	البيانات التي تسبب أي انقطاع للأصول الحيوية في المملكة (مثل شبكات الطاقة ومصافي البترول والنقل والصحة وما إلى ذلك)؟		سري للغاية
سمعة المملكة	البيانات التي يمكن أن تخضع لاهتمام وسائل الإعلام الدولية أو الوطنية وتؤدي إلى الإساءة لسمعة المملكة؟		سري للغاية
الأمن الوطني	بيانات القضايا الإرهابية والمخططات المهددة للمملكة؟		سري للغاية
العلاقات الدبلوماسية	البيانات المتعلقة بالاتفاقيات الثنائية ومذكرات التفاهم الدبلوماسية بين المملكة والدول الأخرى مالم ينص على أنها عامه؟		سري
الاقتصاد الوطني	بيانات يمكن أن تؤثر سلباً في سوق العمل في المملكة؟		سري
	البيانات التي تسبب انخفاضاً كبيراً في أسعار الموارد الطبيعية؟		سري
	مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو إقتصادية استراتيجية للمملكة		سري
	البيانات التي تسبب انخفاضاً كبيراً في صادرات المملكة؟		سري
مهام الجهات الحكومية	أي نوع من البيانات التي يمكن أن تحد من إمكانية الجهات الحكومية للقيام بالعمليات اليومية ووظائف الأعمال؟		سري
البنية التحتية	بيانات عن التخزين اللوجستي أو المخازن الاستراتيجية؟		سري
	بيانات قد تضر بالمنشآت الحيوية؟		سري

الملحق 2

وثيقة ضوابط الأمن السيبراني للبيانات

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني

للبيانات

Data Cybersecurity Controls
(DCC -1: 2022)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام