سياسة وحوكمة بيانات المشاريع بجامعة تبوك

V.0.1

جامعة تبوك

تفاصيل الوثيقة

اسم الوثيقة	سياسة و حوكمة بيانات المشاريع بجامعة تبوك
المؤسسة	جامعة تبوك – مكتب إدارة البيانات
مالك الوثيقة	مكتب إدارة البيانات
رقم الإصدار	0.1
الحالة	إصدار
تاريخ الإصدار	٢٠٢٣/١٠/١٠م
تصنيف الوثيقة	عام

جدول اعتماد الوثيقة

الإصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
0.1	٢٠٢٣/١٠/١٠م	لا يوجد	د. عائشة عبدالله الحكمي مسؤول إدارة البيانات	د. حسين العزيزي المسؤول القانوني	د. محمد متعب العتيبي مدير مكتب إدارة البيانات

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د. محمد متعب العتيبي	مدير مكتب إدارة البيانات	٢٠٢٣/١٠/١٠ م	

المحتويات

مقدمة

يهدف هذا الدليل الإجرائي إلى مساعدة جامعة تبوك على الالتزام بسياسات حوكمة البيانات التي يصدرها مكتب إدارة البيانات بالجامعة والمشتقة من مكتب إدارة البيانات الوطنية[1] والتي تضع الضوابط المنظمة للتعامل مع البيانات الوطنية، بما في ذلك تصنيفها ومشاركتها مع الأطراف الخارجية المتعاقدة مع جامعة تبوك بما يتوافق مع ضوابط الأمن السيبراني للبيانات.

نطاق التطبيق

ينطبق هذا الدليل على بيانات الجامعة[2], مهما كان شكلها أو طبيعتها, التي يتم مشاركتها مع الأطراف الخارجية لتنفيذ الأعمال والمشاريع.

الأهداف

يساعد الدليل الإجرائي على تحقيق الأهداف التالية:

- **المحافظة على بيانات الجامعة وشركائها**

يساعد على تقييد الوصول للبيانات المصنفة للحد اللازم لتنفيذ متطلبات المشروع.

- **تحسين الكفاءة والأمان**

من خلال تطبيق أفضل الممارسات في رفع التوعية وتطبيق الضوابط الأمنية والسيبرانية والتأكد من فعاليتها.

- **ضمان الإلتزام**

يساعد في تسهيل الالتزام بالمتطلبات الأخرى مثل سياسات حوكمة البيانات الوطنية والقواعد واللوائح ذات الصلة بتقنيات الذكاء الاصطناعي والتي يصدرها مكتب إدارة البيانات بجامعة تبوك تطبيقيا لما تصدره الهيئة السعودية للبيانات والذكاء الاصطناعي وضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني.

[1] ملحق (٣) الدليل الإجرائي لحوكمة بيانات المشاريع من مكتب إدارة البيانات الوطنية

[2] بيانات الجامعة: هي جميع البيانات - مهما كان شكلها أو مصدرها أو طبيعتها- التي يتم إنشاؤها او الحصول عليها من قبل جامعة تبوك في سياق ممارسة اختصاصها المقررة نظاما.

خطوات مشاركة البيانات مع الأطراف الخارجية لأغراض تنفيذ المشاريع

أولا: تشكيل فريق عمل

على جامعة تبوك القيام بتشكيل فريق عمل يتكون من: (مالك المشروع, مدير المشروع من إدارة المشاريع, ممثل إدارة المخاطر/المراجعة, ممثل مكتب إدارة البيانات في الجامعة, ممثل الأمن السيبراني في الجامعة) ومن تراه الجامعة ملائماً. ويتولى الفريق المشكل المساهمه في حماية البيانات والحد من تسربها عند مشاركتها مع الأطراف الخارجية وضمان الالتزام بسياسات حوكمة البيانات الوطنية وضوابط الأمن السيبراني للبيانات أثناء مراحل المشروع.

مهام فريق العمل

1. تحديد درجة تصنيف المشروع.
2. تحديد الحد الأدنى من البيانات التي يجب مشاركتها مع الأطراف الخارجية.
3. مراجعة تصنيف البيانات المطلوبة قبل مشاركتها مع الأطراف الخارجية.
4. دراسة و تقييم أثر البيانات المطلوبة من قبل الأطراف الخارجية.
5. تحديد واقتراح البنود التعاقدية النظامية التي تكفل حماية البيانات وإدارجها ضمن النصوص المتغيرة وفق نماذج العقود المعتمدة لوزارة المالية - المتصلة بنظام المنافسات والمشتريات الحكومية.
6. تحديد الضوابط المناسبة لضمان حماية البيانات الحكومية وفقا لمستوى التصنيف.

ثانياً: تقييم ودراسة أثر المشروع ووثائقه

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

- تحديد فئة الأثر وقد تشمل واحدة أو أكثر:
  - المصلحة الوطنية
  - أنشطة الجهات
  - صحة وسلامة الأفراد
  - الموارد البيئية

- تحديد مستوى الأثر (حسب دليل سياسة تصنيف الأصول وترميزها لجامعة تبوك) ويشمل :

  - 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[3]

ثالثاً: آلية التعامل مع المشروع حسب التصنيف

1. **في حال كان تصنيف المشروع سري فأعلى:**

- يقوم الفريق المشكل بتحديد الآلية النظامية المناسبة لطرح المشاريع المصنفة على أنها سري فأعلى.
- يقوم الفريق المشكل بتحديد الضوابط اللازمة لحماية البيانات عند مشاركتها.

الحد الأدنى من الضوابط للمشاريع المصنفة سري فأعلى:

(ا) تعهد الأطراف الخارجية بعدم استخدام تطبيقات التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية أو الخاصة بالطرف الخارجي لإنشاء أو تخزين أو مشاركة البيانات الخاصة بجامعة تبوك باستثناء التطبيقات الآمنة المعتمدة من الجهات ذات العلاقة.

(ب) تخصيص موقع ملائم لموظفي الطرف الخارجي لأداء أعمالهم، مع توفير أجهزة مخصصة مملوكة للجهة يتم من خلالها مشاركة البيانات ومعالجتها للبيانات التي يحددها الفريق.

(ج) توفير عناوين بريد إلكتروني من قبل الجامعة لموظفي الطرف الخارجي، وحصر مشاركة البيانات من خلالها، مع التزام موظفي الطرف الخارجي بعدم استخدام عناوين البريد الإلكتروني الخاصة بالطرف الخارجي في الأعمال المتعلقة بالمشروع.

(د) تفعيل أنظمة التحكم بالدخول والخروج من الموقع المخصص على أن يكون للمصرح لهم فقط.

(ه) منع خروج الأجهزة ووحدات التخزين والبيانات ، ومنع إدخال أي أجهزة إلكترونية للقاعة.

(و) يتم تقييد الوصول إلى البيانات واستخدامها للغرض المطلوب لأقل عدد من العاملين.

(ز) استخدام طرق وخوارزميات آمنة للتشفير عند الانشاء والتخزين والمشاركة.

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

[3] ملحق (٢) أداة تصنيف البيانات

2. **في حال كان تصنيف المشروع مقيد**

يلتزم الفريق بتطبيق الضوابط التالية كحد أدنى:

(ا) تعهد الأطراف الخارجية بعدم استخدام تطبيقات التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجامعة بإستثناء التطبيقات الآمنة المعتمدة من الجهات ذات العلاقة.

(ب) يتم تقييد الوصول إلى البيانات واستخدامها للغرض المطلوب لأقل عدد من العالمين.

(ج) استخدام طرق وخوارزميات آمنة للتشفير عند الإنشاء والتخزين والمشاركة.

(د) يتم التدرج في مشاركة البيانات وفقاً لسياسة مشاركة البيانات.

ويمكن للجامعة 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 مصنفة على درجات السرية أثناء تنفيذ مشاريع مصنفة على مستوى مقيد أو عام، على الفريق المشكل القيام بالمراجعة الدورية للوثائق والمتطلبات التي يتم مشاركتها مع الأطراف الخارجية أثناء مرحلة التنفيذ. على أن يتم دراسة أثر ذلك وتطبيق ما يلزم من الضوابط لحماية تلك البيانات. مع مراعاة الحاجة للمعالجة المسبقة في حال تطلب الأمر ذلك، على سبيل المثال: الحجب وإخفاء الهوية والتجميع. بالإضافة إلى ذلك، اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات بمستويات تصنيف مختلفة.

خامساً: تقييم الأثر للمخرجات

على جامعة تبوك عند استلامها لمخرجات المشروع وبياناته القيام بتصنيفها وفقاً لسياسة تصنيف البيانات بجامعة تبوك، وفي حال صُنفت البيانات من قبل الجهة المنفذة يتم مراجعة تصنيفها، وعلى الجامعة تطبيق ضوابط الأرشفة والتخزين الآمن للمخرجات التي تم استلامها من قبل الأطراف الخارجية والتحقق من تطبيق الضوابط الآتية للأطراف الخارجية مثل: تنفيذ عمليات الاتلاف أو الحذف الآمن للبيانات، ومنع حق الوصول إلى البيانات بمجرد انتهاء المشروع.

ضوابط عامة يجب مراعاتها

- توازن جامعة تبوك 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[4] من سياسة تصنيف البيانات.

- في المراحل الأولية من المشروع تقوم جامعة تبوك بتضمين البنود اللازمة للتأكد من التزام المتعاقد معه بحماية البيانات والمحافظة عليها وفق الالتزامات النظامية المحددة. على أن تشمل:

1. وثيقة من الجهة المنفذة تتضمن التأكيد على أنه تم تسليم جميع وثائق المشروع أو اتلافها حسب سياسات اتلاف البيانات في جامعة تبوك -تعتمده جامعة تبوك بموافقة خطية- دون الإخلال بسياسات حوكمة البيانات الوطنية وضوابط الأمن السيبراني المتعلقة بالإتلاف.
2. تطبيق علامات الحماية النصية على البيانات سواء بالصيغة الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات تصنيف البيانات.
3. تصميم وثيقة Non-disclosure agreement (NDA) اتفاقية عدم الإفشاء ملائمة لاختصاصات المشروع وتوقيع الأطراف عليها.
4. التوقيع على اتفاقية مشاركة البيانات في الأحوال التي تتطلب ذلك وفق سياسة مشاركة البيانات بالجامعة.
5. تحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.
6. تعهد موظفي الجهات المنفذة بعدم استخدام تطبيقات المراسلة أو التواصل الاجتماعي أو خدمات التخزين السحابية الشخصية أو تقنيات الذكاء الإصطناعي لإنشاء أو تخزين أو مشاركة البيانات الخاصة بالجهة، بإستثناء تطبيقات المراسلة الآمنة المعتمدة من الجهات ذات العلاقة ووفقاً للأنظمة واللوائح والقواعد ذات الصلة.

[4] ملحق (٢): الخطوة 0 من الخطوات اللازمة لتصنيف البيانات

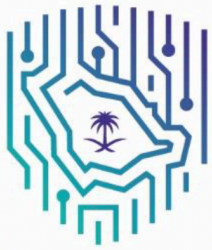
ملحق ١

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

ملحق ٢

وثيقة ضوابط الآمن السيبراني للبيانات



الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ضوابط الأمن السيبراني

للبيانات

Data Cybersecurity Controls
(DCC -1: 2022)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

ملحق ٣

الدليل الإجرائي لحوكمة بيانات المشاريع من مكتب إدارة البيانات الوطنية