# سياسة تصنيف البيانات بجامعة تبوك

**V.1.0**

## خصائص المستند

| | |
|---|---|
| اسم المستند | سياسة تصنيف البيانات |
| المؤسسة | جامعة تبوك |
| مالك الوثيقة | مكتب إدارة البيانات |
| رقم الاصدار | **1.0** |
| الحالة | اصدار |
| تاريخ الإصدار | 1 سبتمبر 2023 |
| التصنيف الأمني | داخلي |

## تاريخ التعديلات

| الاصدار | التاريخ | التعديلات | تحرير | مراجعة | موافقة |
|---|---|---|---|---|---|
| 1.0 | 1 سبتمبر 2023 | لا يوجد | د. عائشة الحكمي<br>مسؤول إدارة البيانات | د. مريم الشهري<br>مسؤول إتاحة البيانات | د. محمد متعب العتيبي<br>مشرف وحدة حوكمة البيانات |

## الموافقات

| الاسم | الوظيفة | التاريخ | التوقيع |
|---|---|---|---|
| د. محمد متعب العتيبي | مشرف وحدة حوكمة البيانات | 1 سبتمبر 2023 | |
| اللجنة التنفيذية لحوكمة البيانات | ---- | ١٦ سبتمبر 2023 | --- |

المحتويات

## جدول التعريفات

| المصطلح | التعريف |
|---|---|
| الجامعة | جامعة تبوك. |
| إدارات الجامعة | الوكالات، العمادات، الوحدات، الإدارات، الأقسام. |
| حوكمة البيانات | مجموعة من الممارسات والإجراءات التي تساعد على ضمان إدارة أصول البيانات في الجامعة، بدءً من وضع الخطة المعنية بالبيانات وتطوير المعايير والسياسات وحتى التنفيذ والامتثال. |
| إدارة البيانات | عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين الجامعة من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيمة والثمينة. |
| عنصر البيانات | عنصر البيانات هو وحدة من البيانات لها مفهوم دقيق وسمة واضحة وتمثل سمة من سمات كيان البيانات التابعة له - مثال رقم هوية العميل واسم العميل هي عناصر لبيانات العميل. |
| قاموس البيانات | قاموس البيانات عبارة عن قائمة مركزية تحتوي على السمات التفصيلية المحددة لعناصر البيانات (مثل اسم العنصر وتوصيفه ومصدره ونوع البيان الذي يحتويه هل هو تاريخ أو رقم أو حرف ...إلخ). |
| جودة البيانات | جودة البيانات هي قدرة البيانات على تلبية متطلبات العمل والنظام والمتطلبات الفنية المنصوص عليها في الجامعة، ويتم عادةً قياس جودة البيانات من حيث اكتمالها وملاءمتها وتوقيتها ودقتها، واتساقها، وارتباطها، ونزاهتها. |
| أمن البيانات | أمن البيانات يمثل العمليات والتقنيات المستخدمة لحماية البيانات من عمليات الوصول، أو العرض، أو التعديل، أو الحذف غير المصرح به سواءً كانت النية عرضية أو متعمدة أو كيدية. |
| بنية البيانات | تشتمل بنية البيانات على النماذج، أو السياسات، أو القواعد، أو المعايير التي تحكم أي بيانات يتعين جمعها وكيفية تخزينها وترتيبها واستخدامها في نظام قاعدة البيانات. |
| البيانات الوصفية | هي المعلومات التي تصف ماهية عناصر البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التقنية والتشغيلية. |
| مرجعية البيانات | مرجعية البيانات هي الموثوقية المسلم بها والتي بصددها يتم الحفاظ على تعريفات البيانات ومعايير جودة البيانات بالإضافة إلى مشاركة حقوق الوصول. |
| الإشراف على البيانات | الإشراف على البيانات هي الموثوقية المسلم بها والتي بصددها يتم وضع التوصيات وتنفيذ قرارات ممثل بيانات الأعمال. |
| قائمة مصطلحات الأعمال | هي قائمة مركزية لتوثيق مصطلحات الأعمال ومشاركتها على نطاق الجامعة. |
| مستويات تصنيف البيانات | مستويات التصنيف التالية: (سري للغاية (، (سري)، (مقيد)، (عام). |

## 1. المقدمة

تُمَثِّل هذه الوثيقة سياسة تصنيف البيانات بجامعة تبوك، والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من أقسام رئيسية لِتَشمل هذه المُقَدِمَة يلها الغَرض، والنطاق، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات.

على جَمِيع المستخدمين القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بوثيقة سياسة البيانات المفتوحة الخاصة بجامعة تبوك. وفي حالة عدم وضوح أيا من معلومات هذه الوثيقة أو لأي جزءٌ منها، فنأمل التواصل مع مكتب إدارة البيانات لشرحها وتوضيحها.

يعَدُ مكتب إدارة البيانات بالجامعة المالك لِتلك الوثيقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على مكتب إدارة البيانات مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يجوز أيضاً تحديثها فور حُدوث أي تعديلات أو تغييرات تَتَعلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأي تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ مكتب إدارة البيانات.

## 2. الغرض من الوثيقة

استجابة لمبادرة مكتب إدارة البيانات الوطنية والمبادرات ذات الصلة بضرورة وضع سياسات حوكمة البيانات في الجهات الحكومية انطلاقًا من سياسات حوكمة البيانات الوطنية التي تم تطويرها، قام مكتب إدارة البيانات في الجامعة بتطوير وثيقة سياسة تصنيف البيانات، بالتوافق مع سياسات مكتب إدارة البيانات الوطنية.

تهدف هذه السياسة إلى وضع القواعد والإرشادات الأساسية لمكتب إدارة البيانات التابع للجامعة والوكالات، العمادات، الوحدات، الإدارات، الأقسام ذات الصلة من أجل تصنيف البيانات بطريقة تعكس احتياجات العمل في الجامعة وأفضل الممارسات من منظور تقنية المعلومات والأعمال.

## 3. نطاق عمل السياسة وتطبيقها

تنطبق سياسة تصنيف البيانات على جميع البيانات التي تنتجها أو تتلقاها أو تتعامل معها الجامعة - سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - وأيًا كان مصدرها أو طبيعتها، وتتعدد أشكال ومضامين هذه البيانات والمعلومات، التي منها على سبيل المثال لا الحصر: السجلات الورقية، ووثائق الاجتماعات، ورسائل البريد الإلكتروني، والبيانات والمعلومات المخزنة على الكمبيوتر، أو أشرطة الصوت، والفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجلة بشكل إلكتروني وغير إلكتروني والقابلة للنشر.

## 4. جدول مراجعة السياسة

يجب مراجعة هذه السياسة بشكل منتظم بحيث تكون هذه المراجعة مرة واحدة سنويًا على أقل تقدير وفقًا لما يوجه به المشرف العام على السياسة ويطلب من مكتب إدارة البيانات داخل الجامعة.

## 5. مر اقبة الامتثال

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسة، وعلى جهات الجامعة ضمان تطبيق هذه السياسة داخل مكوناتها (عمادات، وحدات، إدارات.... الخ)، علمًا بأن الالتزام ببنود هذه السياسة يخضع لمراجعة دورية من قبل مكتب إدارة البيانات بالجامعة عدم التزام أو انتهاك لأي منها لها سيؤدي إلى المساءلة القانونية واتخاذ الإجراءات اللازمة حسب ما توصي عليه اللجنة التوجيهية بالجامعة.

## 6. الأدواروالمسؤوليات

| المصطلح | التعريف |
|---|---|
| اللجنة التوجيهية | تحديد مسؤولية البيانات من خلال تحديد ممثلي بيانات الأعمال وأخصائي بيانات الأعمال، مراجعة واعتماد مستويات تصنيف البيانات واتخاذ القرارات لحل المشاكل وحالات التصعيد. |
| مكتب إدارة البيانات | مكتب إدارة البيانات هو الجهة المسؤولة عن إعداد سياسة تصنيف البيانات بما ينسجم مع ما يصدره مكتب إدارة البيانات الوطنية.<br>ويشمل ذلك:<br>- إعداد وثيقة سياسة تصنيف البيانات والتحديثات المرتبطة بها.<br>- متابعة أعمال تصنيف البيانات لضمان تصنيف كافة أصول البيانات في الجامعة.<br>- إعداد ومراجعة وتحديث واعتماد الأدلة الإجرائية لتوضيح آلية تطبيق السياسة في الجامعة.<br>- رفع التقارير المرتبطة بأعمال تصنيف البيانات وتقارير الامتثال لسياسة تصنيف البيانات في الجامعة والتصعيد بما يخص أعمال تصنيف البيانات والامتثال للسياسة.<br>- إعداد برامج توعوية لرفع مستوى الوعي وتعزيز ثقافة تصنيف البيانات. |
| إدارات الأعمال | تقوم إدارات الأعمال في الجامعة بتطبيق السياسة بحيث يتم تصنيف البيانات واعتمادها ويشمل ذلك:<br>- حصر البيانات غير الإلكترونية.<br>- إعداد ومراجعة وتحديث واعتماد أدلة البيانات.<br>- تصنيف البيانات في الجامعة بالتوافق مع مبادئ وضوابط السياسة. |
| عمادة تقنية المعلومات | تطبيق الضوابط على البيانات بحسب تصنيفاتها المعتمدة بالإضافة الى التمكين التقني والمعلوماتي للجهات ذات العلاقة بتطبيق السياسة.<br>ويشمل ذلك:<br>- حصر قواعد البيانات في الجامعة.<br>- توفير كافة المعلومات عن البيانات الإلكترونية المخزنة في قواعد بيانات لتمكين إدارات الأعمال في الجامعة من تصنيف البيانات.<br>- توفير البيانات اللازمة لإعداد أدلة البيانات لقواعد البيانات في الجامعة بناءً على النماذج المعتمدة من مكتب إدارة البيانات ومشاركتها مع الوحدات التنظيمية المعنية.<br>- تطبيق سياسات وضوابط الحماية على البيانات الالكترونية في الجامعة بناءً على تصنيفها.<br>- إبلاغ ممثلي البيانات ومكتب إدارة البيانات عن أية مخالفات أو حالات عدم التزام.<br>- تركيب وإدارة وتشغيل الأدوات والأنظمة الخاصة بكشف تسريب البيانات في الجامعة، وكشف المخالفات والانتهاكات ونقاط الضعف الأمنية والتعامل معها. |
| إدارة الأمن السيبراني | المواءمة مع السياسات والضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني والمتابعة والإشراف والرقابة على تنفيذ الضوابط على البيانات المصنفة. |
| إدارة المخاطر | مراجعة تقارير الالتزام بتطبيق السياسة وتعريف مخاطر عدم الالتزام. |
| إدارة المراجعة الداخلية | مراجعة تقارير الالتزام بأدلة السياسات والإجراءات الخاصة بتصنيف البيانات في الجامعة والمشاركة في التحقيق في أي مخالفات أو حالات عدم التزام. |

## 7. بنود السياسة

يجب تعريف وتصنيف كيانات بيانات الجامعة بالشكل المناسب وفقًا لمعايير التصنيف بما يتوافق مع الاحتياجات واللوائح والسياسات من مكتب إدارة البيانات الوطنية.

### 1.1 المبادئ الرئيسية لتصنيف البيانات

- المبدأ الأول: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة (في المجال التنموي) مالم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي والأمني) مالم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

- المبدأ الثاني: الضرورة والتناسب

يتم تصنيف البيانات إلى مستويات وفقًا لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها.

- المبدأ الثالث: التصنيف في الوقت المناسب.

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

- المبدأ الرابع: المستوى الأعلى من الحماية

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

- المبدأ الخامس: فصل المهام

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

- المبدأ السادس: الحاجة إلى المعرفة

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين داخل الجامعة.

- المبدأ السابع: الحد الأدنى من الامتيازات

يتم تقييد إدارة صلاحيات العاملين داخل الجامعة على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المنوطة بهم.

## 8. ضوابط عامة لتصنيف البيانات

بناءً على مستويات التصنيف، تقوم إدارة الأمن السيبراني بتحديد وتطبيق الضوابط الأمنية المناسبة لحماية البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن. وفي حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقًا لمعايير التصنيف، تعامل هذه البيانات على أنها «مقيدة» حتى يتم تصنيفها بشكل صحيح. كما يجب تصنيف البيانات التي لم يتم تصنيفها وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل يعدها مكتب إدارة البيانات ويتم اعتمادها من اللجنة التنفيذية، أدناه بعض 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 :

- علامات الحماية
  - تُطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقًا لكل مستوى من مستويات التصنيف.
- الوصول
  - يمنح الوصول - المنطقي والمادي - إلى البيانات بناءً على مبدئي «الحد الأدنى من الامتيازات» و «الحاجة إلى المعرفة».
  - يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو انهاء الخدمة المهنية للعاملين بالجامعة.
- الاستخدام

- تستخدم البيانات المصنفة وفقًا لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة «سري للغاية» على مواقع محددة سواءً مادية - كالمكاتب - أو - افتراضية - باستخدام ترميز الأجهزة أو تطبيقات خاصة.

- التخزين
  - لا تترك البيانات المصنفة على أنها «سري للغاية» و «سري» و «مقيد» وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة حثيثة داخل الجامعة.
  - يجب حماية البيانات المصنفة على أنها «سري للغاية» و «سري» و «مقيد» غير المراقبة أثناء تخزينها ماديًا أو إلكترونيًا باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
- مشاركة البيانات
  - تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
  - يجب الاتفاق على آلية تبادل البيانات، سواءً كانت الجهات (مقدمي الطلب) 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.
- الاحتفاظ بالبيانات
  - يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
  - يتم تحديد فترة الاحتفاظ بناءً على ما تحدده المتطلبات التعاقدية والتنظيمية والقانونية ذات العلاقة.
  - يتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.
- التخلص من البيانات
  - يتم التخلص من جميع البيانات بشكل آمن وفقًا للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
  - يتم التخلص من البيانات التي تم تصنيفها على أنها «سري للغاية» و «سري» التي يتم التحكم بها الكترونيًا باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
  - يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
  - يتم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.
- الأرشفة
  - يتم أرشفة البيانات في مواقع تخزين آمنة وفقًا للطريقة التي يوصي بها ممثل بيانات الأعمال.
  - يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
  - يتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها «سري للغاية» و «سري» باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
  - يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.
- إلغاء التصنيف (رفع السرية)
  - 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.
  - في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
  - 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:
    - فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (على سبيل المثال، عامين بعد الإنشاء).
    - فترة زمنية محددة بعد اتخاذ آخر إجراء على البيانات (على سبيل المثال، ستة أشهر من تاريخ آخر استخدام)
    - بعد انقضاء تاريخ محدد (على سبيل المثال، من المقرر مراجعتها في 1 يناير 2024).

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

– 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.

1.2 تحديد جميع بيانات الجامعة ومصادرها

- يحدد ممثلي بيانات الأعمال جميع بيانات الجامعة كما تقوم الجهات المشاركة مع الجامعة بتحديد وتوثيق بياناتها التي تمتلكها.
- ينبغي تعريف مصادر بيانات الجامعة كما يلي:
  - مصادر البيانات الداخلية: إدارات الأعمال والنظم الداخلية التي تولّد البيانات للجامعة من خلال تنفيذ إجراءات وخدمات العمل. وتشمل تلك المصادر، على سبيل المثال لا الحصر، النسخ الورقية أو الرقمية للتقارير التي تعمل عليها والإدارات الداخلية أو البيانات المعرفة من خلال الأنظمة المستخدمة.
  - مصادر البيانات الخارجية: الجهات الخارجية التي تقدم البيانات المتفق عليها للجامعة لتنفيذ إجراءات وخدمات العمل. وتشمل هذه المصادر: مقدمي بيانات الطلاب (سهل)، الجهات الحكومية ذات العلاقة (البيانات الإلكترونية أو الورقية) والهيئات الرقابية الأخرى
- يجب تحديد قنوات تبادل البيانات كما يلي:
  - القنوات الآلية: وتشمل كافة القنوات الآلية وشبه الآلية مثل: الرسائل القصيرة والبريد الإلكتروني، تكامل النظم التقنية ونظم الأعمال.
  - القنوات اليدوية: وهي القنوات غير التقنية مثل الأقراص المدمجة ووحدات التخزين USB والأقراص الصلبة الخارجية والوثائق الورقية.
- يتعاون مكتب إدارة البيانات مع إدارات الأعمال في الجامعة ذات العلاقة لإدراج ووصف مصادر البيانات الداخلية والخارجية إضافة إلى قنوات تبادل البيانات ذات العلاقة.
- يتوّلى مكتب إدارة البيانات تسجيل وإدراج ووصف مصدر البيانات وقنواته ذات العلاقة والحفاظ عليها.
- عند تحديد مصادر البيانات الداخلية، ينبغي تسجيل وصف مكان تخزين البيانات ومكان إدارتها.
- عند تحديد مصادر البيانات الخارجية، ينبغي تحديد المعلومات التالية:
  - ما إذا كان هناك اتفاقية مشاركة بيانات رسمية و/ أو اتفاقية مستوى خدمة مع الجامعة.
  - ما إذا كانت الجهة الخارجية ستوفر البيانات للجامعة بشكل كامل أو على أجزاء.
  - قنوات الاتصال المستخدمة لتبادل البيانات.
  - آليات الأمن المطبقة.
  - المستوى المتوقع لجودة البيانات (بحسب سياسة جودة البيانات واحتياجات العمل).
  - توافق حلول تقنية المعلومات الخارجية مع معايير ولوائح الجامعة لحماية وتأمين البيانات.
  - توافق الجهة الخارجية مع معايير ومبادئ إدارة البيانات المعتمدة في الجامعة ومكتب إدارة البيانات الوطنية.

## 9. مسؤوليات تعريف وتصنيف البيانات

يعمل مكتب إدارة البيانات على تسهيل تصنيف كيانات البيانات المحددة بالتنسيق مع ممثلي بيانات الأعمال داخل الجامعة و يحدد الجدول أدناه مصفوفة الأدوار والمسؤوليات عن تعريف وتصنيف البيانات:

| # | الإجراء | ممثل بيانات الأعمال | مختص بيانات الأعمال | تقنيين وفنيين البيانات |
|---|---|---|---|---|
| 1 | تحديد مصادر عناصر البيانات | A | R | C |
| 2 | تعريف قيم قاموس البيانات | A | R | R |
| 3 | تطبيق معايير تصنيف البيانات | A | R | R |
| 4 | التحقق من نتائج تصنيف البيانات | A | R | R |
| 5 | تعميم نتائج التصنيف | A | R | R |
| 6 | الحفاظ على تعريف وتصنيف البيانات | A | R | R |

- R (الجهة المسؤولة): واحد أو أكثر من الأدوار التي تقوم بالعمل المطلوب لإنجاز المهمة.
- A (الجهة الخاضعة للمحاسبة): الدور الذي يخضع للمحاسبة في النهاية عن إنجاز المهمة بشكل صحيح وتام
- C (الجهة المستشارة): واحد أو أكثر من الأدوار التي تستشار بالعمل المطلوب.

- ينبغي تصعيد أي اختلاف في التصنيف بحسب "إجراء تصعيد المشاكل".
- ينبغي توثيق كافة كيانات البيانات باستخدام النماذج المعتمدة.
- ينبغي تعريف وتصنيف كافة جهات البيانات والخصائص ذات العلاقة.

## 10. مستويات تصنيف عناصر البيانات

ينبغي تصنيف عناصر بيانات الجامعة من منظور المستوى المؤسسي ومنظور المستوى التنفيذي.

### 10.1 تصنيف كيانات البيانات حسب المستوى المؤسسي

ينبغي تصنيف عناصر بيانات الجامعة من منظور المستوى المؤسسي إلى الفئات التالية:

- كيانات البيانات الإدارية: وتشمل كافة عناصر بيانات ووظائف وأنشطة أعمال الحوكمة في الجامعة (مثال: التخطيط الاستراتيجي، إدارة المشاريع، إدارة الأداء)
- عناصر بيانات الأعمال الرئيسية: وتشمل كيانات البيانات ذات العلاقة بوظائف "سلسلة قيمة الأعمال الرئيسية في الجامعة".
- كيانات البيانات المساندة: وتشمل كيانات البيانات ذات العلاقة بوظائف وأنشطة الأعمال المساندة في الجامعة (مثل، تقنية المعلومات، الموارد البشرية، الخدمات اللوجستية، وغيرها)

### 10.2 .تصنيف كيانات البيانات حسب المستوى التنفيذي

ينبغي تصنيف عناصر بيانات الجامعة من منظور المستوى التنفيذي باستخدام الفئات التالية:

- الأهمية: تصنيف البيانات من حيث أهميتها للأعمال اليومية داخل الجامعة بالمقارنة مع قدرة الجامعة على الاستمرار بالأعمال في حال عدم توافر هذه البيانات.
- الخصوصية وأمن البيانات: تصنيف البيانات بناءً على حقوق وقواعد الوصول لأصحاب المصلحة ونتائج تقييم الأثر المترتب على الوصول الى البيانات أو نشرها.
- هيكلية البيانات: تصنيف البيانات بناء على هيكليتها (ورقية، رقمية، ...) وصيغ معلوماتها عند تخزينها.
- وظائف الأعمال: تصنيف البيانات بناءً على وظائف الأعمال "سلسلة قيمة الأعمال" الأساسية وربطها بالوظائف التي قامت بإنشاء البيانات في الأصل
- التخزين: تصنيف البيانات بناءً على مكان تخزين البيانات داخل أو خارج مباني الجامعة.

### 10.3.تفاصيل تصنيف كيانات البيانات حسب المستوى التنفيذي

بالنسبة للتصنيف حسب المستوى التنفيذي، ينبغي تصنيف كيانات البيانات وفقًا لمعايير الاختيار التالية:

| # | فئة التصنيف | القيمة | معايير الاختيار |
|---|---|---|---|
| 1 | الأهمية (قيمة واحدة فقط) | كيانات البيانات الحرجة | في حال استخدام كيان البيانات في إجراءات العمل الهامة وعدم إمكانية توليدها في حال ضياعها. |
| | | كيانات البيانات غير الحرجة | في حال عدم استخدام كيان البيانات في إجراءات العمل الهامة أو إمكانية توليدها في حال ضياعها. |
| 2 | الخصوصية وأمن البيانات (قيمة واحدة فقط) | عالي الأثر: سري للغاية | تصنف البيانات على أنها «بيانات سرية للغاية»، إذا كان الوصول غير المصرح به الى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي الى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على:<br>- المصالح الوطنية بما في ذلك الإخلال بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة المملكة أو بالعلاقات الدبلوماسية والانتماءات السياسية أو الكفاءة التشغيلية للعمليات الأمنية، أو العسكرية، أو الاقتصاد الوطني، أو البنية التحتية الوطنية، أو الأعمال الحكومية.<br>- أداء الجامعة مما يلحق ضرر بالمصلحة الوطنية.<br>- صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين.<br>- الموارد البيئية أو الطبيعية. |
| | | متوسط الأثر: سري | تصنف البيانات على أنها «بيانات سرية» إذا كان الوصول غير المصرح به الى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي الى ضرر جسيم على:<br>- 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.<br>- حدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معا<br>- يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد. |

| | | | |
|---|---|---|---|
| | | | - تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية.<br>- التحقيق في القضايا الكبرى المحددة نظاما، كقضايا تمويل الإرهاب. |
| | | منخفض الأثر: مقيّد | تصنف البيانات على أنها «مقيدة» إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى:<br>- تأثير سلبي محدود على عمل الجهات العامة أو الانشطة الاقتصادية في المملكة أو على عمل شخص معين.<br>- ضرر محدود على أصول أي جهة وخسارة محدودة على وضعها المالي والتنافسي.<br>- ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية.<br>تصنف البيانات المقيدة الى ثلاث فئات<br>● مقيد – مستوى أ: إذا كان الأثر على مستوى قطاع العمل كاملًا أو أي من الأنشطة الاقتصادية.<br>● مقيد – مستوى ب: إذا كان نطاق الأثر على مستوى أنشطة مجموعة محددة من قطاع العمل.<br>● مقيد – مستوى ج: إذا كان نطاق الأثر على مستوى أنشطة الجامعة أو جهة تابعة محددة. |
| | | لا يوجد أثر: عام | 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 الآثار المذكورة. |
| 3 | هيكلية البيانات (واحدة أو أكثر من القيم) | الورقية | في حال حفظ كيانات البيانات أو أحد خصائصه بصورة ورقية. |
| | | الملفات الرقمية، الفيديو، الصور، الصوت، الوثائق (غير منظمة، شبه منظمة) | في حال حفظ كيانات البيانات أو أحد خصائصه بأحد صيغ الملفات الرقمية التالية:<br>الفيديو، الصور، الصوت، الوثائق. |
| | | قاعدة البيانات المنظمة | في حال حفظ كيانات البيانات أو أحد خصائصه بصيغة قاعدة بيانات منظمة. |
| | | الهيكل الخاص (مثلا، بيانات بيومترية) | في حال حفظ كيانات البيانات أو أحد خصائصه بصيغة مقاييس بيانات بيومترية غير مشمولة بقيم تصنيف سابقة. |
| 4 | وظائف الأعمال (قيمة واحدة فقط) | وفقًا للوظائف المعرفة ضمن سلسلة قيمة الأعمال الخاصة بالجامعة | في أي وظيفة أعمال تم إنشاء كيان البيانات أولاً (قيمة واحدة فقط من سلسلة قيمة الأعمال الرئيسية المحددة). |
| 5 | التخزين (واحدة أو أكثر من القيم) | التخزين الورقي في المبنى الرئيسي | في حال تخزين كيانات البيانات أو أحد خصائصه ضمن مباني الجامعة بصورة ورقية. |
| | | التخزين الرقمي في المباني (الأقراص | في حال تخزين كيانات البيانات أو أحد خصائصه ضمن مباني الجامعة بصورة إلكترونية باستخدام الأقراص المدمجة ووحدات التخزين USB والأقراص الصلبة الخارجية. |

| | | | |
|---|---|---|---|
| | | المدمجة ووحدات التخزين USB والأقراص الصلبة الخارجية) | |
| | | مركز البيانات المحلي (server) | في حال تخزين كيان البيانات أو أحد خصائصه ضمن مباني الجامعة بصورة إلكترونية باستخدام قاعدة بيانات منظمة ضمن مركز البيانات المحلي (server). |
| | | مساحة تخزين آمنة على السحابة عبر الإنترنت (cloud) | في حال تخزين كيانات البيانات أو أحد خصائصه على خدمة تخزين آمنة على السحابة عبر الإنترنت خارج مباني الجامعة. |

## 11. اعتبارات التصنيف

ينبغي أن يأخذ التصنيف على المستوى المؤسسي للجامعة بعين الاعتبار الأسئلة والدلالات التالية عند تصنيف عناصر البيانات.

| # | فئة التصنيف | الاعتبارات | الأثر |
|---|---|---|---|
| 1 | الأهمية | • ما هي جهات البيانات المطلوبة لتنفيذ إجراءات العمل الرئيسية الهامة؟<br>• هل تستطيع الجامعة إعادة توليد البيانات في حال ضياعها بالكامل؟<br>• هل يتم استخدام البيانات في اتخاذ القرارات الاستراتيجية؟ | - ينبغي أخذ جهات البيانات الهامة بعين الاعتبار في خطة التعافي من الكوارث.<br>- ينبغي أخذ جهات البيانات الهامة بعين الاعتبار في إجراءات النسخ الاحتياطية للبيانات. |
| 2 | الخصوصية وأمن البيانات | • هل هناك أي سياسة أو قانون أو لائحة تتعلق بقدرة مشاركة المعلومات؟<br>• دراسة الأثر المترتب على الوصول غير المصرح به للبيانات.<br>• هل يحتوي كيانات البيانات على معلومات حساسة (على سبيل المثال، شخصية أو مالية)؟<br>• ما هي قواعد إخفاء البيانات المستخدمة حاليًا؟<br>• ما هي كيانات البيانات المشفرة حاليًا؟ | - يجب تعريف تصنيفات لمشاركة البيانات أو استخدامها بناءً على السياسة الوطنية<br>- يجب تنفيذ آلية التشفير على مستوى التطبيق وقاعدة البيانات لكيانات البيانات الحساسة<br>- تعديل / تكوين امتيازات الوصول لمستخدمي التطبيقات وفقًا لتصنيف خصوصية البيانات |
| 3 | هيكلية البيانات | • ما هي طريقة العرض النهائية للتخزين في كيانات البيانات؟<br>• كيف تقوم الجامعة بتخزين البيانات؟<br>• ما هو مصدر البيانات؟ | - يجب أرشفة جميع جهات البيانات الورقية رقمياً.<br>- يجب أن تحتوي كافة البيانات الوصفية للبيانات على معلومات مفيدة تصف كيانات البيانات المنظمة وشبه المنظمة.<br>- الحفاظ على توثيق حديث لكافة قواعد البيانات التي تستضيف جهات البيانات. |

| | | | |
|---|---|---|---|
| 4 | وظائف الأعمال | • متى تم إنشاء كيانات البيانات لأول مرة؟<br>• هل كيانات البيانات مرحلية؟ | - يجب توزيع جهات البيانات على أدوار العمل المعنية (إذا أمكن).<br>- التركيز على دعم وظائف الأعمال بالأدوات والضوابط المطلوبة لإدارة جهات البيانات. |
| 5 | التخزين | • كيف يسترجع المستخدمون البيانات؟<br>• ما هي الأدوات والتطبيقات المستخدمة لعرض كيانات البيانات؟<br>• هل كيانات البيانات موزعة على العديد من الأجزاء؟<br>• هل هناك خدمات محددة تستخدمها الجامعة لتنفيذ إجراءات العمل أو معالجة البيانات؟ | - وضع وتنفيذ استراتيجية شاملة للنُسخ الاحتياطية للبيانات لتشمل كافة أنواع التخزين. |

## 12. آلية تصنيف البيانات على محور الخصوصية وأمن البيانات

- تحديد جميع بيانات الجامعة: تتمثل الخطوة الأولى في جرد وتحديد جميع البيانات التي تمتلكها الجامعة.
- تعيين مسؤول تصنيف البيانات: على الجامعة تفويض شخص يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات، غالبًا ما يكون ممثل بيانات الأعمال هو الشخص الذي يفهم طبيعة البيانات وقيمتها داخل إدارات الأعمال.
- ويتحمل المسؤولية حيال إجراء التصنيف الأولي، ونظرًا لوجود أكثر من مسؤول بيانات داخل الجامعة فقد يوجد أكثر من شخص مسؤول عن تصنيف البيانات.
    - يقوم ممثل بيانات الأعمال بتقييم الأثر المحتمل الذي يترتب على:
        - الافصاح عن هذه البيانات أو الوصول غير المصرح به اليها.
        - اجراء تعديل على هذه البيانات او اتلافها او كليهما.
        - عدم الوصول الى هذه البيانات في الوقت المناسب.
- تبدأ عملية تقييم الأثر بتطبيق مبدأ " الأصل في البيانات الإتاحة" (في المجال التنموي) مالم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، وسرية للغاية (في المجال السياسي والأمني) مالم تقتض حساسيتها مستويات أدنى من التصنيف.
- تحديد فئة الاثر:

يحدد ممثل بيانات الأعمال الفئة الرئيسية والفرعية للأثر المحتمل في أي من الفئات الرئيسية التالية:

- المصلحة الوطنية
- أنشطة الجهات
- صحة أو سلامة الأفراد
- الموارد البيئية

- تحديد مستوى الاثر

- يحدد ممثل بيانات الأعمال لكل أثر محتمل مستوى معين. يعتمد تحديد المستوى على الآتي:
    - مدة الأثر وصعوبة السيطرة على الضرر.
    - فترة تدارك وإصلاح الأضرار بعد وقوعها.
    - حجم الاثر (على المستوى الوطني، مناطقي، عدة جهات، جهة واحدة، عدة أفراد ... الخ).

- تحدد هذه المعايير مستويات الأثر الأربعة:
  - عالي يؤدي الوصول الى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها.
  - متوسط يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى حدوث أضرار جسيمة أو خطيرة يصعب السيطرة عليها.
  - منخفض يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى أضرار محدودة يمكن السيطرة عليها أو أضرار متقطعة على المدى القصير يمكن السيطرة عليها.
  - لا يوجد أثر، لا يؤدي الوصول إلى البيانات أو الإفصاح عنها إلى اي ضرر على المدى الطويل أو القصير.
- يجب ان تكون جميع الاضرار المحتملة والمحددة خلال عملية تقييم الأثر محددة وقائمة على أدلة، في محاولة للحد من التقديرات الشخصية للمكلف بإجراء تصنيف البيانات.
- يحدد ممثل بيانات الاعمال مستوى تصنيف البيانات بناءً على الأثار المحددة ومستوياتها:
  - عالي، تصنف البيانات باعتبارها "سرية للغاية".
  - متوسط، تصنف البيانات على انها "سرية".
  - منخفض، يلزم إجراء المزيد من التقييمات (يرجى الاطلاع على خطوة (4,5).
  - لا يوجد أثر، تصنف البيانات على أنّها بيانات "عامة".
- ويوجد وصف مفصل للاعتبارات الرئيسية لكل فئة من فئات الأثر ومستواه في الجدول 2 "فئات ومستويات تقييم أثر تصنيف البيانات" في الملحقات.
- يجب إجراء تقييمات إضافية إذا كان مستوى الأثر المحدد "منخفض" وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنّها بيانات "عامة" الى الحد الاقصى. يجب على ممثل بيانات الأعمال في هذا الصدد، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية ... الخ، وإذا كان الإفصاح عن البيانات مخالفًا للأنظمة، فيجب حينها تصنيف البيانات على أنّها بيانات "مقيدة".
- بعد التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكًا لأي نظام نافذ، يجب أيضًا تقييم المزايا المحتملة للإفصاح عن مثل هذه البيانات والتأكد مما إذا كانت هذه المزايا ستفوق الآثار السلبية أم لا. وتشمل المزايا المحتملة استخدام البيانات لتطوير خدمات جديدة ذات قيمة مضافة، أو زيادة مشاركة الأفراد مع الحكومة.
  - إذا كانت المزايا أكبر من الآثار السلبية، تصنف البيانات على أنها "عامة".
  - إذا كانت المزايا أقل من الآثار السلبية، تصنف البيانات على أنها "مقيدة".

الشكل ادناه في الملحقات يوضح الخطوات اللازمة لإجراء تصنيف البيانات.

1.1. مراجعة مستوى التصنيف

1.1.1. يجب ان يفحص مسؤول حوكمة البيانات جميع البيانات المصنفة لضمان أن يكون مستوى التصنيف المحدد من جانب ممثل بيانات الأعمال هو الأنسب، وتتم مراجعته خلال شهر واحد من التصنيف الأولي.

1.2. تطبيق الضوابط المناسبة

1.2.1. يتم تعميم نتائج التصنيف وتطبيق ضوابط تصنيف البيانات.

1.2.2. يتم الانتهاء من عملية التصنيف عند تصنيف جميع البيانات التي تملكها الجامعة والتحقق من مستويات التصنيف وتطبيق الضوابط ذات الصلة.

## 13. فئات ومستويات تقييم أثر تصنيف البيانات

كما يمكن تصنيف البيانات المصنّفة على مستوى مقيّد الى مستويات فرعية بناءً على نطاق الأثر على النحو التالي:

- مقيّد - مستوى (أ): إذا كان نطاق الأثر على مستوى قطاع كامل أو نشاط اقتصادي عام.
- مقيّد - مستوى (ب): إذا كان نطاق الأثر على مستوى أنشطة عدة جهات أو على مصالح مجموعة من الأفراد.
- مقيّد – مستوى (ج): إذا كان نطاق الأثر على مستوى أنشطة جهة واحدة أو مصالح فرد معين.

وفي الجدول أدناه توضيح وتحديد لمستوى التصنيف الصحيح الذي يمكّن الجهات من تقييم درجة الأثر المترتبة على الوصول غير المصرح به إلى البيانات أو الإفصاح عنها أو عن محتواها (ولمزيد من المعلومات حول عملية تقييم الأثر، يمكن الاطلاع على "الخطوات اللازمة لتصنيف البيانات").

يجب على كل جهة -على حدى – أن تقوم بإجراء تقييم الآثار المترتبة على عملية الوصول أو الإفصاح غير المصرح به، كما تعتبر هذه القائمة غير شمولية.

| | | | |
|---|---|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية | | |
| فئة الأثر الفرعية | سمعة المملكة | | |
| الاعتبارات | هل ستخضع المعلومات لاهتمام وسائل الإعلام المحلية أو الدولية؟ هل ستعطي انطباع سلبي؟ | | |
| مستوى الأثر | | | |
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تتأثر السمعة بشكل كبير. | تتأثر السمعة إلى حد ما. | لا تتأثر السمعة. | لا يوجد تأثير على المصالح الحيوية الوطنية. |

| | | | |
|---|---|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية | | |
| فئة الأثر الفرعية | - | | |
| الاعتبارات | هل تُشكّل المعلومات خطراً على العلاقات مع الدول الصديقة؟ هل ستزيد من حدة التوتر الدولي؟ هل يمكن أن تؤدي إلى احتجاجات أو عقوبات من دول أخرى؟ | | |
| مستوى الأثر | | | |
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| قطع العلاقات الدبلوماسية والانتماءات السياسية أو تهديد الاتفاقيات وشروط المعاهدات أو كليهما. | تتأثر العلاقات الدبلوماسية سلبياً على المدى الطويل | لن يحدث تأثير على العلاقات الدبلوماسية أو يحدث تأثير بسيط على المدى القصير | لا يوجد تأثير على المصالح الحيوية الوطنية. |

| | |
|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية |

| | |
|---|---|
| فئة الأثر الفرعية | الأمن الوطني/ النظام العام |
| الاعتبارات | هل المعلومات - في حال نشرها- تساعد على تنظيم أعمال إرهابية أو ارتكاب جرائم خطيرة؟ هل تُشكّل مصدر ذعر للجميع؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تتأثر الكفاءة التشغيلية لحفظ النظام العام والأمن الوطني أو العمليات الاستخباراتية للقوات العسكرية والأمنية بشكل كبير. | تأثير طويل المدى على قدرة وكفاءة الجهات الأمنية بالتحقيق والترافع في الجرائم المنظمة الخطيرة التي تسبب عدم الاستقرار الداخلي. | تأثير لا يذكر على الكفاءة التشغيلية للعمليات الأمنية على مستوى إقليمي أو محلي، والحيلولة دون اكتشاف الجرائم البسيطة على المدى القصير | لا يوجد تأثير على المصالح الحيوية الوطنية. |

| | |
|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية |
| فئة الأثر الفرعية | الاقتصاد الوطني |
| الاعتبارات | هل يؤدي الكشف عن المعلومات إلى خسائر اقتصادية على المستوى الوطني؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير طويل المدى على الاقتصاد الوطني مع انخفاض لا يمكن تداركه في الناتج المحلي الإجمالي، أو أسعار الأسواق المالية، أو نسبة البطالة، أو القوة الشرائية، أو المؤشرات الأخرى ذات الصلة مما ينعكس سلباً على جميع القطاعات في المملكة. | تأثير طويل المدى على الاقتصاد الوطني مع انخفاض يمكن تداركه في الناتج المحلي الإجمالي ونسبة البطالة أو أسعار الأسواق المالية أو القوة الشرائية، مما ينعكس سلباً على قطاع واحد أو أكثر. | تأثير بسيط على الاقتصاد الوطني مع انخفاض يمكن تداركه في وقت قصير في الناتج المحلي الإجمالي ومعدل العمالة أو أسعار الأسواق المالية أو القوة الشرائية، مما ينعكس سلباً على قطاع واحد فقط. | لا يوجد تأثير على الاقتصاد الوطني. |

| | |
|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية |
| فئة الأثر الفرعية | البنى التحتية الوطنية |
| الاعتبارات | هل الوصول إلى المعلومات يؤدي إلى تعطيل البنى التحتية الحيوية الوطنية (مثل الطاقة، النقل، الاتصالات)؟ في حال التعرض لهجمات إلكترونية، هل ستظل الخدمات الأساسية بالمملكة متاحة؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| التوقف والتعطل في أمن وعمليات البنى التحتية الوطنية الحيوية تتأثر العديد من القطاعات وتتعطل الحياة الطبيعية | التوقف والتعطل - لفترة قصيرة في أمن وعمليات البنى التحتية الوطنية الحيوية، كما يتأثر قطاع واحد أو أكثر | يحدث ضرر أو تأثير قصير المدى على أمن وعمليات البنى التحتية المحلية / الإقليمية | لا يوجد تأثير على البنى التحتية الوطنية. |

| | |
|---|---|
| فئة الأثر الرئيسية | المصلحة الوطنية |
| فئة الأثر الفرعية | مهام الجهات الحكومية |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى الحد من إمكانية الجهات الحكومية من تنفيذ عملياتها ومهامها اليومية؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| عدم قدرة جميع الجهات الحكومية من أداء مهامها وعملياتها الرئيسية لفترة طويلة | عدم قدرة جهة حكومية واحدة أو أكثر على أداء واحدة أو أكثر من مهامها الرئيسية لفترة قصيرة. | عدم قدرة جهة حكومية أو أكثر من أداء مهمة واحدة أو أكثر من المهام غير الرئيسية لفترة قصيرة. | لا يوجد تأثير على مهام الجهات الحكومية. |

| | |
|---|---|
| فئة الأثر الرئيسية | الأفراد |
| فئة الأثر الفرعية | صحة / سلامة الأفراد |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟ (على سبيل المثال، اسماء ومواقع العملاء السريين، والأشخاص الخاضعين لأنظمة حماية خاصة) |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| خسارة عامة أو فادحة في الأرواح، فقدان حياة فرد أو مجموعة من الأفراد. | ضرر جسيم أو إصابة تهدد حياة الفرد. | إصابة بسيطة دون أي خطر يهدد حياة أو صحة الفرد. | لا يوجد تأثير على الأفراد. |

| | |
|---|---|
| فئة الأثر الرئيسية | الأفراد |
| فئة الأثر الفرعية | الخصوصية |
| الاعتبارات | هل سيؤدي الكشف عن المعلومات إلى انتهاك خصوصية الأفراد؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| الكشف عن البيانات الشخصية لشخصية مهمة. | الكشف عن البيانات الشخصية لشخصية مهمة. | الكشف عن البيانات الشخصية للفرد. | لا يوجد تأثير على الأفراد. |

| | |
|---|---|
| فئة الأثر الرئيسية | الأفراد |
| فئة الأثر الفرعية | |
| الاعتبارات | سيؤدي ذلك إلى انتهاك أي حقوق ملكية فكرية؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| مما يؤثر على المصلحة الوطنية | | | لا يوجد تأثير على حقوق ملكية فكرية. |

| | |
|---|---|
| فئة الأثر الرئيسية | البيئة |
| فئة الأثر الفرعية | الموارد البيئية |
| الاعتبارات | هل سيتم هذه المعلومات بتطوير خدمة أو منتج يمكن أن يؤدى إلى تدمير الموارد البيئية أو الطبيعية للمملكة؟ |

| مستوى الأثر | | | |
|---|---|---|---|
| سري للغاية | سري | مقيّد | عام |
| عالي | متوسط | منخفض | لا يوجد أثر |
| تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعية. | تأثير طويل المدى على البيئة أو الموارد الطبيعية. | تأثير قصير المدى على البيئة أو الموارد الطبيعية. | لا يوجد تأثير على البيئة. |

## 14. الوثائق ذات العلاقة

- وثيقة قاموس البيانات
- وثيقة سياسات حوكمة البيانات الوطنية.
- الدليل التنظيمي والنموذج التشغيلي لمكتب إدارة البيانات الوطنية.

- سابق خبرة لشركة الحلول الشاملة.

## المصادر

1- مكتب إدارة البيانات الوطنية (سياسات حوكمة البيانات الوطنية).
2- الضوابط الأساسية للأمن السيبراني.