جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة تصنيف البيانات

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-21.CS.A.V2.0

1. جدول المحتويات

2. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة الاتصالات وتقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة الاتصالات وتقنية المعلومات.

3. الرقابة على الوثيقة

1.3 معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة تصنيف البيانات	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/12	إنشاء
V1.1	د. سامر بني عواد	2022/02/01	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/28	مراجعة وتحديث

3.3 المراجعة والتدقيق

تاريخ المراجعة القادمة
2025/01/01

4.3 قائمة التوزيع

الرقم	المستفيد
1	جميع أقسام عمادة الاتصالات وتقنية المعلومات
2	الشؤون القانونية
3	الموقع الإلكتروني
4	

5.3 الاعتماد

الاسم	الوظيفة	رقم القرار	التاريخ
د. نهاد بنت عبد الله العمير	نائب الرئيس للتطوير والشراكة المجتمعية	61945	2024/03/06

4. المقدمة

حماية الأصول المعلوماتية والتقينه أمر ضروري لنجاح الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني بتطوير وإنشاء وتنظيم العمليات الأمنية المطلوبة لحماية الأصول المعلوماتية والتقنية. وتحدد هذه الوثيقة سياسة تصنيف البيانات داخل الجامعة وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

تُدرج هذه السياسة في إطار سياسة الجامعة وتحت الصلاحيات الممنوحة من صاحب الصلاحية ابتداءً من تاريخ اعتمادها.

5. الهدف

تهدف هذه السياسة إلى تحديد المتطلبات والمعايير اللازمة لتصنيف البيانات والتعامل معها وحمايتها وفقاً للأنظمة والتشريعات ذات العلاقة.

6. قابلية التطبيق ونطاق العمل

تنطبق أحكام هذه السياسة على جميع العاملين أو المكلفين الذين يعملون في الجامعة سواء بعقود دائمة أو مؤقتة وبشكل مباشر أو غير مباشر بما في ذلك الموردين والمقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أو المؤقت إلى بيانات الجامعة مهما كان مصدرها أو شكلها أو طبيعتها وإلى أنظمة وأجهزة وقواعد بيانات الجامعة.

7. السياسة

1.7 متطلبات السياسة العامة.

1.1.7 يجب أن يعكس تصنيف البيانات والمعلومات مستوى حساسيتها وقيمتها وأهميتها لأعمال الجامعة.

2.1.7 يجب على الجامعة وضع خطة لتصنيف البيانات، على أن تشتمل الخطة على خارطة طريق بالنشاطات والأهداف المرحلية الأساسية لتصنيف بيانات الجامعة.

3.1.7 يجب على الجامعة أن يحدد ويعدّ قائمة بكل مجموعات ومصادر البيانات في الجامعة.

4.1.7 يجب على الجامعة أن تحدد أولويات مجموعات البيانات والسجلات التي يجب تصنيفها حسب الأهمية لاتباعها عند التصنيف.

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

6.1.7 يجب تصنيف جميع البيانات الهامة والحساسة الموجودة داخل الجامعة.

7.1.7 يجب تقييم بيانات الجامعة من خلال إجراء تقييم تأثير الأعمال وعلى عملية تقييم الأثر أن تشمل الخطوات التالية:

- تحديد الفئات التي يمكن أن تتأثر من الجهات، والأفراد والأشخاص، والبيئة.
- يجب اختيار مستوى تأثير الضرر المحتمل لكل فئة منها بين "لا يوجد أثر" و "منخفض" و "متوسط" و "مرتفع".
- يجب تحديد مستويات التصنيف لمجموعات البيانات والسجلات بناءً على مستوى الأثر المحدد:
  - إذا كان تقييم مستوى الأثر "مرتفع" - تصنف البيانات باعتبارها "سرية للغاية".
  - إذا كان تقييم مستوى الأثر "متوسط" - تصنف البيانات باعتبارها "سرية".
  - إذا كان تقييم مستوى الأثر "منخفض" - تصنف البيانات باعتبارها "مقيدة"
  - إذا كان تقييم مستوى الأثر "لا يوجد" - تصنف البيانات باعتبارها "عامة".

8.1.7 يجب أن يعتمد تصنيف البيانات على تقييم تأثر الأعمال الذي تم إجراؤه.

9.1.7 على الجامعة أن يدرس إمكانية تصنيف البيانات منخفضة الأثر باعتبارها "عامة" بد لا من "مقيدة". ويجب أن يشمل التقييم ما يلي:

- دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية، مثل نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية.
- تحديد المزايا المحتملة للإفصاح عن مثل هذا البيانات والتأكد مما إذا كانت هذه المزايا ستفوق الآثار السلبية أم لا.
- إن لم يكن نشر البيانات منخفضة الأثر يمثل خرقا لأي نظام نافذ، ومنافعه تتجاوز تأثيراته السلبية، على الجهة أن تصنف البيانات منخفضة الأثر باعتبارها "عامة".

10.1.7 يجب على جميع العاملين بالجامعة استخدام البيانات المصنفة بناءً على مبدأ الحاجة الى المعرفة.

11.1.7 يجب تقييد صلاحيات وصول العاملين للبيانات المصنفة وفقًا لمبدأ الحد الأدنى من الامتيازات لأداء المهام والمسؤوليات المناطة بهم.

12.1.7 في حالة عدم اليقين عن مستوى التصنيف الذي سيتم اختياره، يجب تصنيف البيانات وفقاً لأعلى مستوى تصنيف.

13.1.7 يتم تصنيف البيانات المتراكمة أو المجمعة وفقاً لتصنيفها المحدد مسبقاً، وفي حال اختلاف مستويات التصنيف يتم تطبيق التصنيف الأعلى.

14.1.7 إذا كانت الأصول المعلوماتية والتقنية تحتفظ ببيانات ذات فئات تصنيف مختلفة، فيجب تصنيف الأصول المعلوماتية والتقنية وفق أعلى فئة تصنيف.

15.1.7 يجب تقديم التوعية والتدريب اللازمة للعاملين في الجامعة فيما يتعلق بتصنيف البيانات والتعامل معها بما يتوافق مع حساسيتها ومستوى الأثر.

16.1.7 يجب تخصيص ضوابط أمنية لحماية ومعالجة البيانات حسب تصنيفها، لضمان المعالجة والمشاركة والحذف الآمن للبيانات على أن تكون هذه الضوابط بما يتماشى مع سياسات أمن المعلومات واستمرارية الأعمال والمتطلبات التشريعية والتنظيمية ذات العلاقة ومن هذه الضوابط على سبيل المثال لا الحصر:

- إدارة الوصول
- تقييد استخدام البيانات المصنفة كـ"سري للغاية" على مواقع محددة مثل مرافق الجامعة
- التشفير

17.1.7 يجب التعامل مع جميع بيانات الجامعة الغير مصنفة على أنها مقيدة حتى يتم تصنيفها.

18.1.7 يجب ترميز جميع الأصول المعلوماتية والتقنية ومنها (المستندات والوسائط المادية) حسب تصنيف البيانات.

19.1.7 يجب تصنيف بيانات الجامعة وفقاً لمستوى تصنيف المرسل (سواءً تم إرسالها من جهة داخل المملكة أو خارجها)، وفقاً للوائح المعمول بها والاتفاقيات الدولية.

20.1.7 يجب تصنيف رسائل البريد الإلكتروني للجامعة وفقاً لمستويات التصنيف المنصوص عليها في هذه السياسة.

21.1.7 على الجامعة أن ينشر درجات التصنيف الممنوحة لمجموعات البيانات كما هي في الدليل الشامل للبيانات.

22.1.7 يجب تخزين البيانات المصنفة واستبقاءها بما يتوافق مع سياسات الجامعة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

23.1.7 في حال استخدام الأجهزة المحمولة أو الأجهزة الشخصية في الوصول للبيانات المصنفة، فيجب التأكد من تطبيق الضوابط اللازمة لحماية البيانات بما يتوافق مع سياسات الجامعة والمتطلبات التشريعية ذات العلاقة.

24.1.7 على الجامعة أن يصنّف مجموعة بياناته الرئيسية إلى مجموعات بيانات داخلية أو خارجية على النحو التالي:

- داخلية – أي مجموعة بيانات رئيسية يمتلكها الجامعة ويديرها وتمثل المصدر الأوحد للحقيقة في مختلف الجهات.
- خارجية – أي مجموعة بيانات رئيسية تمتلكها وتديرها جهات حكومية أخرى.

25.1.7 على الجامعة أن يصنف مجموعة بياناته المرجعية إلى مجموعات داخلية أو خارجية على النحو التالي:

- داخلية – أي بيانات مرجعية يمتلكها الجامعة ويديرها وتمثل "مصدر المعلومة الصحيح" في مختلف الجهات.
- خارجية – أي بيانات مرجعية تمتلكها وتديرها جهات حكومية أخرى أو تُعتبر بيانات معيارية في القطاع تصدرها منظمات خارجية مثل ISO.

26.1.7 على الجامعة أن يوثق قائمة بكل مجموعات البيانات والسجلات المحددة، بالإضافة إلى كل النشاطات التي تم تنفيذها خلال عملية تصنيف البيانات. وينبغي أن يشمل السجل ما يلي كحدٍ أدنى:

- قائمة بكل مجموعات البيانات المحددة.
- مستويات التصنيف الممنوحة لمجموعات البيانات.
- تواريخ منح مستويات التصنيف لمجموعات البيانات.
- فترات التصنيف المفروضة على مجموعات البيانات.

- مستويات التصنيف المصدق عليها.

27.1.7 على الجامعة أن يراجع كل مجموعات البيانات المصنفة لضمان مناسبتها لدرجة التصنيف الممنوحة لها، وذلك وفقًا لسياسة تصنيف البيانات الصادرة عن مكتب إدارة البيانات الوطنية.

28.1.7 على الجامعة أن يحدد مؤشرات أداء رئيسية لقياس التقدم المتحقق في خطة تصنيف البيانات وتنفيذ عملية تصنيف البيانات الخاصة بالجامعة. على أن تشمل هذه المؤشرات ما يلي كحدٍ أدنى:

- النسبة المئوية لمجموعات البيانات المصنفة.
- النسبة المئوية لمجموعات البيانات المصنفة بمستوى تصنيف معين.
- النسبة المئوية للبيانات ذات الأثر المنخفض المصنفة بدرجة "مقيدة".
- النسبة المئوية لمجموعات البيانات المصنفة التي خضعت للمراجعة والتصديق.

2.7 مستويات تصنيف البيانات والمعلومات

1.2.7 يجب تصنيف جميع البيانات التي ينشئها الجامعة أو يستخدمها أو يقوم بصيانتها أو حيازتها ضمن واحدة من التصنيفات الأربعة التالية:

- سري للغاية: تعتبر البيانات الحساسة جداً "سرية للغاية"، وهي البيانات التي في حال الكشف عنها قد تسبب خسائر مالية كبيرة للجامعة، وتلحق أضراراً جسيمة والاستثنائية بالأمن الوطني، وأضراراً كبيرة بالمصلحة العامة، أو الضرر الجسيم والاستثنائي على الاقتصاد الوطني أو بالعلاقات الخارجية.
- سري: تعتبر البيانات الحساسة "سرية"، وهي التي في حال الكشف عنها قد تسبب خسائر مالية ويسبب ضرر جسيم بالأمن والاقتصاد الوطني.
- مقيد: هي البيانات والمعلومات التي من المتوقع أن يؤدي الإفصاح عنها إلى أي أثر سلبي على أعمال الجامعة أو نشاطاته أو العاملين فيه أو تتعلق بالبيانات الشخصية.
- متاح: تعتبر البيانات التي توافق الجامعة صراحةً على نشرها للجمهور تحت التصنيف "متاح". ولا يسبب الإفصاح لغير المصرح له عن مثل هذه المعلومات أي ضرر أو أذى للجامعة.

8. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني:

1.1.8 على مدير الأمن السيبراني اعتماد السياسة من صاحب الصلاحية والعمل على تنفيذها.

2.1.8 على مدير الأمن السيبراني اعتماد المعايير والإجراءات والتوجيهات لضمان الالتزام الضروري بمتطلبات أمن عمليات الجامعة.

3.1.8 على مدير الأمن السيبراني ضمان التوافق بين هذه السياسة وأعمال الجامعة.

4.1.8 على مدير الأمن السيبراني حل أي تعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة حيثما أمكن.

6.1.8 على إدارة الأمن السيبراني مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

7.1.8 على إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

يجب على الإدارة العليا ومدراء الإدارات ورؤساء الوحدات والمستشارين ما يلي:

8.1.8 التأكد من مشاركة هذه السياسة لجميع العاملين داخل الجامعة أو الملف.

9.1.8 إبلاغ إدارة الأمن السيبراني عن أي تجاوزات أو عدم التزام بهذه السياسة.

يتحمل مستخدمي أصول الجامعة المعلوماتية والتقنية مسؤولية الالتزام بهذه السياسة بالإضافة إلى الإبلاغ عن أي حادثة أمنية أو عدم الالتزام بهذه السياسة إلى إدارة الأمن السيبراني.

9. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

10. تغييرات السياسة

يجب مراجعة السياسة سنويًا على الأقل أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الجامعة.

11. الالتزام

يجب على جميع العاملين في الجامعة والأطراف (الخارجية/المتعاقد معهم) الالتزام بأحكام هذه السياسة، ويجب على مدير الأمن السيبراني في الجامعة ضمان المراقبة المستمرة للالتزام، ورفع التقارير اللازمة بهذا الشأن لصاحب الصلاحية بشكل دوري.

يجب اتخاذ الإجراءات اللازمة لضمان الالتزام بأحكام هذه السياسة، وذلك من خلال قيام إدارة الأمن السيبراني أو الإدارات ذات العلاقة بمراجعة دورية، واتخاذ إجراءات تصحيحية من قبل صاحب الصلاحية في الجامعة وفقاً للتوصيات المقدمة من قبل مدير الأمن السيبراني حيال أي انتهاك لأي من أحكام هذه السياسة، على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يسفر عنه التحقيق بهذا الخصوص، وتتضمن الإجراءات التأديبية على سبيل المثال لا الحصر الآتي:

- سحب صلاحية الوصول إلى البيانات وأصول تقنية المعلومات وأنظمة الجامعة المتصلة بها.
- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما يراه الجامعة من إجراءات مناسبة.

يستوجب عدم الالتزام بأي من أحكام هذه السياسة -دون الحصول على استثناء مسبق من إدارة الأمن السيبراني - اتخاذ الإجراءات المناسبة وفقًا للسياسات واللوائح المعمول بها في الجامعة، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية مع أي أشخاص أو جهات متعاقد معهم.

12. السياسات والمعايير والإجراءات ذات العلاقة

- DICT.I.06-01.CS.A.V.2.0– السياسة العامة للأمن السيبراني وحوكمة البيانات
- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- DICT.I.06-03.CS.A. V2.0- سياسة حماية البيانات
- DICT.I.06-20.CS.A. V2.0- سياسة تخزين واستبقاء البيانات
- DICT.I.06-13.CS.A. V2.0- سياسة حماية البيانات الشخصية
- DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- DICT.I.06-42.CS.A. V2.0- سياسة أمن الأجهزة المحمولة والأجهزة الشخصية
- DICT.I.06-11.CS.A. V2.0- سياسة مشاركة البيانات
- DICT.I.06-53.CS.A.V2.0- معايير الحماية من فقدان البيانات
- DICT.I.06-56.CS.A.V2.0- معايير أمن البيانات
- DICT.I.06-58.CS.A.V2.0- معايير أمن قواعد البيانات
- DICT.I.06-61.CS.A.V2.0- معايير حماية البيانات
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.06-79.CS.A.V2.0- معايير أمن الأجهزة المحمولة والأجهزة الشخصية

13. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات	ضوابط الأمن السيبراني للحوسبة السحابية	الأيزو 27001: 2013	مكتب إدارة البيانات الوطنية	المعهد الوطني للمعايير والتقنية
متطلبات السياسة العامة	3-2-7-2	2-1-6-2	1-6-2	1-1-5-2	-	A.8.2	سياسات حوكمة البيانات الوطنية وضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16
مستويات تصنيف البيانات والمعلومات	3-2-7-2	2-1-6-2	1-6-2	1-1-5-2	-	A.8.2	سياسات حوكمة البيانات الوطنية وضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16

14. ملحق1: تصنيف البيانات

تم العمل على مواءمة درجات تصنيف البيانات حسب الجدول الموضح أدناه بناءً على التصنيفات الصادرة من المركز الوطني للوثائق والمحفوظات الموافق عليه بقرار مجلس الوزراء رقم (595/م) بتاريخ 1421/5/10هـ، والتصنيفات الصادرة من مكتب إدارة البيانات الوطنية التي سيتم استصدارها كنظام موحد لتصنيف البيانات بمرسوم ملكي.

تصنيف المركز الوطني للوثائق والمحفوظات		تصنيف مكتب إدارة البيانات الوطنية	
سري للغاية	الوثائق والمحفوظات التي تؤدي معرفة بيانتها للغير إلى الإضرار بأمن الدولة.	سري للغاية	الوصول الغير مصرح به لهذه البيانات أو الإفصاح عنها أو عن محتواها قد يسبب خسائر مالية كبيرة أو إلحاق أضراراً جسيمة بالأمن الوطني وأضراراً كبيرة بالمصلحة الوطنية.
سري جداً	الوثائق والمحفوظات التي يؤدي إفشاء بيانتها إلى الإضرار بالمصالح العامة أو الخاصة.	سري	الوصول الغير مصرح به لهذه البيانات أو الإفصاح عنها أو عن محتواها قد يسبب خسائر مالية أو إلحاق ضرر جزئي بسمعة الجامعة أو المصلحة الوطنية.
سري	الوثائق والمحفوظات التي تتعلق بمواضيع أو قضايا فرديه يترتب على إفشائها أو الاطلاع عليها تأثيرات سيئة على الحياة الاجتماعية للجماعات والأفراد.	مقيّد	الوصول الغير مصرح به لهذه البيانات أو الإفصاح عنها أو عن محتواها قد يؤدي إلى أثر سلبي على أعمال الجامعة أو نشاطاته أو العاملين فيه أو تتعلق بالبيانات الشخصية.
متاح أو عام	الوثائق والمحفوظات التي تتعلق بمواضيع عامة غير سرية تم نشرها أو إبلاغها للجهات والأشخاص الاعتبارين أو الطبيعيين.	متاح أو عام	عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الآثار السلبية على أعمال الجامعة أو المصلحة الوطنية.

مستوى التصنيف	درجة الأثر	الوصف
سري للغاية	عالي	تصنف البيانات على أنها "بيانات سرية للغاية" إذا كان الوصول غير المصرح به إلى هذه البيانات والإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم واستثنائي لا يمكن تداركه أو إصلاحه على: - 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. - 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 أنها "بيانات سرية" إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى 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. - يحدث خسارة مالية على المستوى التنظيمي تؤدي إلى افلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كلهما معًا. - يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد. - تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية. - التحقيق في القضايا الكبرى المحددة نظامًا، كقضايا تمويل الإرهاب.
مقيّد	منخفض	تصنف البيانات على أنها "بيانات مقيدة" إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها 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 والتنافسي. - ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية.
متاح	لا يوجد	تصنف البيانات على أنها "بيانات عامة/متاح" عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي من الاثار المذكورة أعلاه –في حال عدم وجود تأثير على ما يأتي: - المصلحة الوطنية - أنشطة الجهات - مصالح الأفراد - الموارد البيئية

فئة الأثر الرئيسية	المصلحة الوطنية		
فئة الأثر الفرعية	سمعة المملكة		
الاعتبارات	هل ستخضع المعلومات لاهتمام وسائل الأعلام المحلية أو الدولية؟ هل ستعطي انطباع سلبي؟		
مستوى الأثر			
سري للغاية	سري	مقيّد	متاح
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 تشكّل المعلومات خطرًا 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	متاح
عالي	متوسط	منخفض	لا يوجد أثر
قطع العلاقات الدبلوماسية والانتماءات السياسية أو تهديد الاتفاقيات وشروط المعاهدات أو كليهما	تتأثر العلاقات الدبلوماسية سلبًا على المدى الطويل	لن يحدث تأثير على العلاقات الدبلوماسية ويحدث 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 تشكل مصدر ذعر للجميع؟		
مستوى الأثر			
سري للغاية	سري	مقيّد	متاح
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 الداخل.	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	متاح
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 سلبًا على جميع القطاعات في المملكة	تأثير طويل المدى على الاقتصاد الوطني مع انخفاض يمكن تداركه في الناتج المحلي الإجمالي نسبة البطالة أو أسعار الأسواق المالية أو القوة الشرائية، مما ينعكس سلبًا على قطاع واحد أو أكثر	تأثير بسيط على الاقتصاد الوطني مع انخفاض يمكن تداركه في الناتج المحلي الإجمالي ومعدل العمالة أو أسعار الأسواق المالية أو القوة الشرائية، مما ينعكس سلبًا على قطاع واحد فقط	-

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	متاح	
عالي	متوسط	منخفض	لا يوجد أثر	
التوقف والتعطل في أمن وعمليات البنى التحتية الوطنية الحيوية، كما 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	-	

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	متاح	
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 على أداء واحدة أو أكثر من المهام غير الرئيسية لفترة قصيرة	-	

فئة الأثر الرئيسية	المصلحة الوطنية			
فئة الأثر الفرعية	أرباح الجهات الخاصة			
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى خسائر مالية أو إفلاس الجهات الخاصة التي تقوم بإدارة مرافق العامة؟ على سبيل المثال، احتمالية الاحتيال، وتحويلات الأموال غير القانونية، والمصادرة غير القانونية للأصول.			
مستوى الأثر				
سري للغاية	سري	مقيّد	متاح	
عالي	متوسط	منخفض	لا يوجد أثر	
تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية	تكبد الجهة خسائر مالية فادحة مما قد يؤدي إلى الإفلاس	ضرر محدود يتمثل في خسارة مالية محدودة للجهة أو لأيٍ من أصولها	لا يوجد تأثير على أنشطة الجهات	

فئة الأثر الرئيسية	المصلحة الوطنية			
فئة الأثر الفرعية	مهام الجهات الخاصة			
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى حدوث أضرار على الجهات الخاصة التي تقوم بإدارة المرافق العامة؟ هل سيؤدي ذلك إلى فقدان الدور الريادي التي تتمتع به الجهة أو خسارة أي من أصولها؟ هل سيؤدي ذلك إلى إنهاء عقود عددٍ كبيرٍ من العاملين؟ هل سيؤثر على القدرة التنافسية للجهة الخاصة؟			
مستوى الأثر				
سري للغاية	سري	مقيّد	متاح	
عالي	متوسط	منخفض	لا يوجد أثر	
تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية	عدم إمكانية الجهة من القيام بمهامها الرئيسية، وفقدان القدرة على التنافسية إلى حد كبير	عدم إمكانية الجهة من أداء إحدى مهامها الرئيسية، وفقدان القدرة على التنافسية بشكل محدود	لا يوجد تأثير على أنشطة الجهات	

فئة الأثر الرئيسية	الأفراد		
فئة الأثر الفرعية	الخصوصية		
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى انتهاك خصوصية الأفراد؟		
مستوى الأثر			
سري للغاية	سري	مقيّد	متاح
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	البيئة		
فئة الأثر الفرعية	الموارد البيئية		
الاعتبارات	هل سيتم استخدام هذه المعلومات لتطوير خدمة أو منتج يمكن أن يؤدي إلى تدمير الموارد البيئية أو الطبيعية للمملكة؟		
مستوى الأثر			
سري للغاية	سري	مقيّد	متاح
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 أو محدود على البيئة أو الموارد الطبيعية	لا يوجد تأثير على البيئة

فئة الأثر الرئيسية	الأفراد		
فئة الأثر الفرعية	الخصوصية		
الاعتبارات	سيؤدي ذلك إلى انتهاك أي حقوق ملكية فكرية؟		
مستوى الأثر			
سري للغاية	سري	مقيّد	متاح
عالي	متوسط	منخفض	لا يوجد أثر
مما يؤثر على المصلحة الوطنية	-	-	-

فئة الأثر الرئيسية	الأفراد			
فئة الأثر الفرعية	صحة/سلامة الأفراد			
الاعتبارات	سيؤدي ذلك إلى الكشف عن المعلومات الى إفشاء أسماء أو مواقع أشخاص وما الى ذلك (مثل، أسماء أو مواقع عملاء، اشخاص خاضعين لأنظمة الحماية الخاصة)؟			
مستوى الأثر				
سري للغاية	سري	مقيّد	متاح	
عالي	متوسط	منخفض	لا يوجد أثر	
خسارة عامة أو فادحة في الأرواح، وفقدان 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	

---------- نهاية الوثيقة ----------