



جامعة الأمير سّطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

سياسة تصنيف البيانات

مكتب إدارة البيانات والذكاء الاصطناعي

الإصدار: ٧١,٤

تاريخ الإصدار: ١٧ / ٧ / ٢٠٢٥

التصنيف: عام

المحتويات

١.	المراجع	٣
٢.	المصطلحات والتعريفات	٣
٣.	الفرض	٤
٤.	النطاق	٤
٥.	بيان السياسة	٥
٥-١	ضوابط تصنيف البيانات	٥
٥-٢	مستويات تصنيف البيانات	٧
٥-٣	تصنيف المقيّد إلى المستويات الفرعية	٨
٥-٤	فئات ودرجات تقييم الأثر	٨
٦.	الاستثناءات	١١
٧.	ملكية السياسة	١١

١. المراجع

رقم المرجع	عنوان المرجع	المصدر	التاريخ
١	سياسات حوكمة البيانات الوطنية مكتب إدارة البيانات الوطنية. (الإصدار الثاني)	مكتب إدارة البيانات الوطنية	٢٠٢١
٢	ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية (الإصدار ١,٥)	مكتب إدارة البيانات الوطنية	٢٠٢١
٣	وثيقة ضوابط الأمن السيبراني للبيانات	الهيئة الوطنية للأمن السيبراني	٢٠٢٢

٢. المصطلحات والتعريفات

المصطلح	التعريف
الجامعة	جامعة الأمير سلطان بن عبد العزيز
المكتب	مكتب إدارة البيانات والذكاء الاصطناعي.
الوحدة التنظيمية	الكلية، أو الإدارة، أو القسم المعتمد في هيكل الجامعة التنظيمي.
الموظف	الشخص الطبيعي الذي يعمل لمصلحة الجامعة وتحت إدارتها أو إشرافها مقابل أجر.
ممثّل بيانات الأعمال	الموظف المعيّن من قبل الوحدة التنظيمية - بحسب الحال - الذي لا يقل مسماه الوظيفي عن مدير إدارة، ليكون المسؤول عن الإشراف على تطبيق سياسات وضوابط ومعايير وإجراءات إدارة البيانات فيما يُمثّل والتي تشمل البيانات التي تم جمعها والاحتفاظ بها من قبل الوحدة التنظيمية التي يرجع إليها، والتحقق من امتثالها للضوابط والسياسات المتعلقة بالبيانات، كذلك متابعة مؤشرات الأداء الرئيسية ومستوى نضج الممارسات المرتبطة بإدارة وحوكمة البيانات داخل الوحدة التنظيمية. أو هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الوحدة التنظيمية التي يعمل بها، وغالباً ما يكون في مستوى إداري عالٍ، ويمكن أن يوجد في الجامعة أكثر من ممثّل بيانات أعمال.
مختص بيانات الأعمال	الموظف الذي يتم تعيينه من قبل الوحدة التنظيمية في الجامعة لتنفيذ الأعمال الخاصة بتطبيق سياسات وضوابط ومعايير البيانات داخل الوحدة التنظيمية وتحديد وإدارة المشاكل والمخاطر المتعلقة بإدارة البيانات ورفعها إلى ممثّل بيانات الأعمال.
تقني وفني بيانات	الموظف المسؤول عن إنشاء وإدارة قواعد البيانات الخاصة بمنصة البيانات/ذكاء الأعمال ونحوه، وبأنظمة الجامعة الرقمية، وتخزين البيانات وضمان توفرها، وتطبيق ضوابط ومعايير هذه السياسة على البيانات المخزنة في قواعد بيانات الجامعة. وكذلك يقدم المساعدة والدعم فيما يخص عمليات وأنشطة إدارة البيانات ذات العلاقة بتقنية المعلومات أو التحول الرقمي.
المستشار القانوني	موظف للشؤون القانونية الذي يقوم بتقديم الاستشارات للمكتب حول المسائل التنظيمية والقانونية المتعلقة بالبيانات.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظّمة مثل الأرقام، أو الصوتية، أو الرموز التعبيرية. الحروف، أو الصور الثابتة، أو الفيديو، أو التسجيلات

المصطلح	التعريف
حوكمة البيانات	مجموعة من الممارسات والإجراءات التي تساعد على ضمان إدارة أصول البيانات في الجامعة، بدء من وضع الخطة المعنية بالبيانات وتطوير الضوابط والسياسات وحتى التنفيذ والامتثال. يتم تحقيق ذلك من خلال إطار حوكمي يوضح الأدوار والمسؤوليات بين ذوي العلاقة.
الوصول الى البيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجامعة لغرض استخدامها.
تصنيف البيانات	إطار موحد يهدف إلى تقسيم البيانات إلى مستويات محددة - تحدد آلية التعامل معها - بناءً على قياس شدة الأثر المترتب على الإفصاح غير المصرح به نظاماً عن البيانات أو عن محتواها.
مستويات تصنيف البيانات	مستويات التصنيف التالية: (سري للغاية، سري، مقيد، عام)
البيانات المحمية	البيانات المصنفة على أنها (سري للغاية، سري، مقيد)
القواعد الاسترشادية	مجموعة من المبادئ الأساسية المستندة لضوابط إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية. وتساعد هذه المبادئ في فهم منظومة إدارة البيانات وحوكمتها بأكملها.
سرية البيانات	الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.
مستوى الوصول إلى البيانات	مستوى يعتمد على الأذونات والصلاحيات التي تقيد الوصول إلى البيانات والموارد التقنية على الأشخاص المصرح لهم وفقاً لما هو مطلوب لإنجاز المهام والمسؤوليات المناطة بهم.
التحقق	التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية.
التصريح	تعريف حقوق وصلاحيات الوصول إلى البيانات والموارد التقنية لأي مستخدم أو برنامج أو عملية، والتحكم بمستويات الوصول إليها.

٣. الغرض

تهدف هذه السياسة إلى وضع المبادئ الأساسية وضوابط تصنيف البيانات في الجامعة مهما كان مصدرها أو شكلها أو طبيعتها. وكذلك وضع إطار موحد لتصنيف البيانات إلى أربعة مستويات بناءً على نتائج تقييم الأثر المترتب على الإفصاح غير المصرح به نظاماً عن البيانات أو عن محتواها، بحيث يحدد هذا الإطار آلية الاطلاع على البيانات والتعامل معها وفقاً لمستوى تصنيفها.

٤. النطاق

تنطبق أحكام السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ومحاضر الاجتماعات والاتصالات عبر وسائل التواصل والتطبيقات ورسائل البريد الإلكتروني والبيانات المخزنة على وسائط إلكترونية وأشرطة الصوت أو الفيديو والخرائط، والصور الفوتوغرافية والمخطوطات والوثائق المكتوبة بخط اليد وأي شكل آخر من أشكال البيانات المسجلة. ويجب الالتزام بهذه السياسة من قبل جميع منسوبي الجامعة، بما في ذلك الموظفين الرسميين، هيئة التدريس، المتقاعدين، المستشارين، وجميع الجهات ذات العلاقة.

٥. بيان السياسة

١-٥-١ ضوابط تصنيف البيانات

يتم تحديد وتطبيق الضوابط الأمنية المناسبة لحماية البيانات بناءً على مستويات التصنيف من قبل مكتب إدارة البيانات والذكاء الاصطناعي بالتعاون مع إدارة الأمن السيبراني؛ وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن. في حال عدم تصنيف البيانات عند إنشائها وفقاً لمعايير التصنيف، تُعامل هذه البيانات على أنها "مقيّدة" حتى يتم تصنيفها بشكل صحيح، مع مراعاة الالتزام بالضوابط والتشريعات والتعاميم الصادرة من المركز الوطني للوثائق والمحفوظات، والهيئة الوطنية للأمن السيبراني ذات العلاقة بحماية البيانات. ويكون تصنيف البيانات وفقاً للضوابط الآتية:

١-٥-١-١ علامات الحماية

- تطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقاً لكل مستوى من مستويات التصنيف.

١-٥-٢ الوصول

- يُمنح الوصول -المنطقي والمادي- للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة".
- يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين في الجامعة.

١-٥-٣ الاستخدام

- تُستخدم البيانات المصنفة وفقاً 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.

١-٥-٤ التخزين

- لا تُترك البيانات المصنفة على أنها "سرية للغاية" و"سري" و"مقيّد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.
- يجب حماية البيانات ذات تصنيف "سري للغاية" و"سري" و"مقيّد" الغير المراقبة أثناء تخزينها مادياً أو إلكترونياً باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

١-٥-٥ مشاركة البيانات

- يقوم تقنيي وفنيي البيانات بالتعاون مع إدارة الأمن السيبراني بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
- يجب الاتفاق على آلية تبادل البيانات من قبل تقنيي وفنيي البيانات، سواء كانت الجهات تستخدم الوسائل المستخدمة حالياً 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.

١-٥-٦ الاحتفاظ بالبيانات

- يقوم ممثلي بيانات الأعمال بإعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات بناءً على الضوابط الأساسية وضوابط الأنظمة الحساسة للأمن السيبراني (وعلى المتطلبات التجارية والتعاقدية والتنظيمية والقانونية...) ووفقاً لتصنيف البيانات ومشاركته مع مكتب إدارة البيانات وإدارة الأمن السيبراني في الجامعة، وذلك بناءً

على ما تحدده متطلبات الأعمال والمتطلبات التعاقدية والتنظيمية والقانونية ذات العلاقة.

- تتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري (سنوي) أو إذا طرأت تغييرات على المتطلبات ذات العلاقة من قبل ممثلي بيانات الأعمال بالتعاون مع مكتب إدارة البيانات والذكاء الاصطناعي.

٧-١-٥ التلخيص من البيانات

- يتم التلخيص من جميع البيانات من قبل الإدارة الممثلة للبيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة من ممثل بيانات الأعمال.
- يتم التلخيص من البيانات التي تم تصنيفها على أنها "سرية للغاية" و"سري" التي يتم التحكم بها إلكترونياً باستخدام أحدث طرق التلخيص من الوسائط الإلكترونية.
- يتم التلخيص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
- يتم إعداد سجل مفضل عن جميع البيانات التي تم التلخيص منها.

٨-١-٥ الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يوصي بها ممثل بيانات الأعمال.
- يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
- تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و"سري" باستخدام إحدى طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
- يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

٩-١-٥ إلغاء التصنيف (رفع السرية)

٩-١-٥-١ يجب إلغاء تصنيف البيانات أو خفض مستوى تصنيفها من قبل مختص بيانات الأعمال إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.

٩-١-٥-٢ في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال ليقوم بتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.

٩-١-٥-٣ يجب تحديد عوامل التي 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.
- بعد ظروف أو أحداث معينة تؤثر تأثيراً مباشراً على البيانات (على سبيل المثال: إحداث تغيير في الأولويات الاستراتيجية أو تغيير في موظفي الجامعة).

١٠-١-٥ يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

٢-٥ مستويات تصنيف البيانات

الجدول أدناه يوضح المستويات الرئيسة لتصنيف البيانات بما يتوافق مع مستوى الأثر، كما يوضح بعض الأمثلة الاسترشادية لكل مستوى:

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	عالي	- تُصنف البيانات على أنها "بيانات سرية للغاية"، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم واستثنائي يصعب تداركه أو إصلاحه على ما يلي: - 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 الجامعة أو الجهات العامة الأخرى مما يلحق ضرراً بالمصلحة الوطنية. - صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين. - الموارد البيئية أو الطبيعية.	- المعلومات السياسية الرسمية المتعلقة بالعلاقات الدولية والاتفاقيات أو المعاهدات وكل ما يتعلق بها من مباحثات ودراسات وأعمال تحضيرية. - معلومات القضايا الإرهابية والمخططات المهددة للأمن - المعلومات المتعلقة بآليات ومفاتيح التشفير المستخدمة للبنى التحتية الوطنية. - معلومات عن تحركات الشخصيات الهامة. - معلومات تمس سيادة الدولة.
سري	متوسط	- تُصنف 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 إفلاس أو عجز الجهات في القطاعين العام والخاص عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معاً. - 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 نظاماً.	- معلومات عن مواقع تخزين المواد اللوجستية أو المخازن الاقتصادية. - مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو اقتصادية استراتيجية بالمملكة. - معلومات متعلقة بالاتفاقيات الثنائية ومذكرات التفاهم الدبلوماسية بين المملكة والدول الأخرى. - معلومات متعلقة بالمنشآت الحيوية.
مقيّد	منخفض	- تُصنف البيانات على أنها "مقيّدة"، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى: - تأثير سلبي على عمل الجامعة أو الجهات العامة الأخرى 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.	- معلومات تضر بسمعة أي شخصية عامة - بيانات مفصلة للمعاملات الفردية - نتائج الأبحاث والدراسات قبل نشرها. - معلومات متعلقة بالتعيينات والقرارات الإدارية الحساسة. - معلومات تحديد الهوية مثل الاسم والعنوان وأرقام الهوية الوطنية وأرقام الهواتف وأرقام الحسابات والتراخيص وبيانات السمات الحيوية. - وثائق مثل الخطط للبرامج والخدمات قبل الكشف عنها للجمهور. - معلومات رواتب الموظفين. - عقود موردين وعروض أسعارهم. - طلبات تقديم عروض. - مواصفات خدمة جديد قبل طرحها للمستفيدين من خدمات الجامعة - تفاصيل تصميم وتطبيق أنظمة أمنية (جدار الحماية وضوابط الوصول ومخططات الشبكة وغيرها). - السياسات والإجراءات الداخلية في الجامعة. - قوائم هواتف داخلية وقوائم البريد الإلكتروني لبعض الموظفين في الجامعة.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
عام	لا يوجد	- تُصنف البيانات على أنها "بيانات عامة" عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أي من الآثار المذكورة أعلاه - وفي حال عدم وجود تأثير على ما يأتي: - المصلحة الوطنية - أنشطة الجامعة - مصالح الموظفين والأفراد - مصالح الكادر التعليمي - الموارد البيئية	- إجراءات الحكومة وسياساتها المتعلقة بالجامعة. - معلومات متعلقة بالخدمات العامة التي تقدمها الجامعة. - جهات الاتصال في الجامعة. - إعلانات التوظيف في الجامعة. - الإعلانات العامة. - تصريحات صحفية من ممثلي الجامعة. - معلومات المخولين بالتصريح الصحفي. - عروض وخدمات تقدمها الجامعة. - معلومات العلاقات العامة.

٣-٥ تصنيف المقيّد إلى المستويات الفرعية

يمكن تصنيف البيانات المصنّفة على مستوى مقيّد إلى 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.

٤-٥ فئات ودرجات تقييم الأثر

الجدول أدناه يمكن الاسترشاد به (ولا يعتبر شامل) لتوضيح فئات ودرجات تقييم الأثر وفقاً لمستويات تصنيف البيانات:

مستوى تصنيف البيانات				الاعتبارات	فئة الأثر الفرعية	فئة الأثر الرئيسية
عام	مقيّد	سري	سري للغاية			
لا يوجد	منخفض	متوسط	عالي			
لا يوجد تأثير على المصالح الحيوية الوطنية	لا تتأثر السمعة	تتأثر السمعة إلى حد ما	تتأثر السمعة بشكل كبير	هل ستخضع المعلومات لاهتمام وسائل الإعلام المحلية أو الدولية؟ هل ستغطي انطباعات سلبية؟	سمعة المملكة	المصلحة الوطنية
	لن يحدث تأثير على العلاقات الدبلوماسية أو سيحدث تأثير بسيط على المدى القصير	تتأثر العلاقات الدبلوماسية سلباً على المدى الطويل	قطع العلاقات الدبلوماسية والانتماءات السياسية أو تهديد الاتفاقيات وشروط المعاهدات أو كليهما	هل تشكل المعلومات خطراً على العلاقات مع الدول الصديقة؟ هل ستزيد من حدة التوتر الدولي؟ هل يمكن أن تؤدي إلى احتجاجات أو	العلاقات الدبلوماسية	

مستوى تصنيف البيانات				الاعتبارات	فئة الأثر الفرعية	فئة الأثر الرئيسية
عام	مقدّم	سري	سري للغاية			
لا يوجد	منخفض	متوسط	عالي	عقوبات من دول أخرى؟	الاقتصاد الوطني	
	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	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 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	هل يؤدي الكشف عن المعلومات إلى خسائر اقتصادية على المستوى الوطني؟		
	يحدث ضرر أو تأثير قصير المدى على أمن وعمليات البنى التحتية المحلية/ الإقليمية	التوقف والتعطيل - لفترة قصيرة - في أمن وعمليات البنى التحتية الوطنية الحيوية، كما يتأثر قطاع واحد أو أكثر	التوقف والتعطيل في أمن وعمليات البنى التحتية الوطنية الحيوية، كما تتأثر العديد من القطاعات وتتعرض الحياة الطبيعية	هل الوصول إلى المعلومات يؤدي إلى تعطيل البنى التحتية الحيوية الوطنية (مثل الطاقة، النقل، التجارة، الاتصالات)؟ في حال التعرض لهجمات إلكترونية، هل ستظل الخدمات الأساسية بالمملكة متاحة؟	البنى التحتية الوطنية	
	عدم قدرة الجامعة أو أكثر من جهة حكومية أخرى من أداء مهمة واحدة أو أكثر من المهام غير الرئيسية لفترة قصيرة	عدم قدرة الجامعة أو أكثر من جهة حكومية أخرى على أداء واحدة أو أكثر من مهامها الرئيسية لفترة قصيرة	عدم قدرة جميع الجهات الحكومية من أداء مهامها وعملياتها الرئيسية لفترة طويلة	هل سيؤدى الكشف عن المعلومات إلى الحد من إمكانية الجهات الحكومية من تنفيذ عملياتها ومهامها اليومية؟	مهام الجهات الحكومية	
	ضرر محدود يتمثل في خسارة مالية		تأثير سلبي كبير على الجهات	هل سيؤدى الكشف عن المعلومات	أرباح الجهات الخاصة	

مستوى تصنيف البيانات				الاعتبارات	فئة الأثر الفرعية	فئة الأثر الرئيسية
عام	مقيّد	سري	سري للغاية			
لا يوجد	منخفض	متوسط	عالي			
لا يوجد تأثير على أنشطة الجهات	محدودة للجهة أو لأي من أصولها	تكبد الجهة خسائر مالية فادحة مما قد يؤدي إلى الإفلاس	الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية	إلى خسائر مالية أو إفلاس الجهات الخاصة التي تقوم بإدارة مرافق عامة؟ على سبيل المثال، الاحتمالية، الاحتمالات وتحويلات الأموال غير القانونية، والمصادرة غير القانونية للأصول.		أنشطة الجهات
	عدم إمكانية الجهة من أداء إحدى مهامها الرئيسية، وفقدان القدرة على التنافسية بشكل محدود	عدم إمكانية الجهة من القيام بمهامها الرئيسية، وفقدان القدرة على حد كبير	تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية	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 عدد كبير من الموظفين؟ هل سيؤثر على القدرة التنافسية للجهة الخاصة؟	مهام الجهات الخاصة	
لا يوجد تأثير على الأفراد	إصابة بسيطة دون أي خطر يهدد حياة أو صحة الفرد	ضرر جسيم أو إصابة تهدد حياة الفرد	خسارة عامة أو أرواح وفقدان حياة فرد أو مجموعة من الأفراد	هل سيؤدي الكشف عن المعلومات إلى إفشاء أسماء أو مواقع أشخاص وما إلى ذلك؟ (على سبيل المثال، أسماء ومواقع العملاء السريين،	صحة/ سلامة الأفراد	الأفراد

مستوى تصنيف البيانات				الاعتبارات	فئة الأثر الفرعية	فئة الأثر الرئيسية
عام	مقتد	سري	سري للغاية			
لا يوجد	منخفض	متوسط	عالي			
				والأشخاص الخاضعين لأنظمة حماية خاصة)		
	الكشف عن البيانات الشخصية للفرد	الكشف عن البيانات الشخصية لشخصية مهمة	الكشف عن البيانات الشخصية لشخصية مهمة	هل سيؤدي الكشف عن المعلومات الى انتهاك خصوصية الأفراد؟	الخصوصية	
لا يوجد تأثير على البيئة.	تأثير قصير المدى أو محدود على البيئة أو الموارد الطبيعية.	تأثير طويل المدى على البيئة أو الموارد الطبيعية.	تأثير كارثي لا يمكن تداركه على البيئة أو الموارد الطبيعية.	هل سيتم استخدام هذه المعلومات لتطوير خدمة أو منتج يمكن أن يؤدي الى تدمير الموارد البيئية أو الطبيعية في المملكة؟	الموارد البيئية	البيئة

6. الاستثناءات

أي استثناء لأي ضابط ذكر في هذه السياسة يجب أن يتم الموافقة عليه من قبل مكتب إدارة البيانات والذكاء الاصطناعي.

7. ملكية السياسة

تعود ملكية هذه السياسة لمكتب إدارة البيانات والذكاء الاصطناعي في جامعة الأمير سكام بن عبد العزيز ويتولى إصدار النسخ المحدث منها، ويجب الحصول على موافقة مكتب إدارة البيانات والذكاء الاصطناعي على أي تغييرات أو تحديثات على هذه الوثيقة.

في حال عدم الامتثال لضوابط السياسة، يخضع منسوبي الجامعة المعنيين للمساءلة حيث يقوم المكتب بتحديد الضرر الناجم عن عدم الامتثال لاتخاذ الإجراء النظامي المناسب.