جامعـــة الأمـيـــر سطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY

سياسة تصنيف البيانات

Data Classification Regulation

الإصدارات

الإصدار	التاريخ	الإعداد	التغيير	وصف التغيير	مستوى الخصوصية	الاعتماد	عدد الصفحات
١.٠	٢٠٢١-١٠-٠٧	مكتب إدارة البيانات والذكاء الاصطناعي	نسخة أولية	إعداد السياسة	☒ عام ☐ مقيد ☐ سري ☐ سري للغاية	عميد تقنية المعلومات والتعليم عن بُعد	١٩
١.١	٢٠٢٢-٠٥-٢٣	مكتب إدارة البيانات والذكاء الاصطناعي	نسخة معدلة	تعديل السياسة وتطويرها	☒ عام ☐ مقيد ☐ سري ☐ سري للغاية	عميد تقنية المعلومات والتعليم عن بُعد	١٩
١.٢	٢٠٢٣-٠٢-١٦	مكتب إدارة البيانات والذكاء الاصطناعي	نسخة معدلة	ضبط السياسة وفقاً للهوية الجديدة للجامعة	☒ عام ☐ مقيد ☐ سري ☐ سري للغاية	عميد تقنية المعلومات والتعليم عن بُعد	٢٢
١.٣	٢٠٢٣-٠٨-١٥	مكتب إدارة البيانات والذكاء الاصطناعي	نسخة معدلة	ضبط وتطوير السياسة	☒ عام ☐ مقيد ☐ سري ☐ سري للغاية	عميد تقنية المعلومات والتعليم عن بُعد	٢٣

المراجع

الوثيقة	سياسات حوكمة البيانات الوطنية
العنوان الإلكتروني	https://sdaia.gov.sa/ndmo/Files/PoliciesAr.pdf

المحتويات

الجداول

الصور

التعريفات

البيانات الشخصية: كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

البيانات: مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام، أو الحروف، أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية.

الوصول إلى البيانات: القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجامعة لغرض استخدامها.

التحقق: التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية.

توافر البيانات: ضمان إمكانية الوصول المناسب والموثوق إلى البيانات واستخدامها عند الحاجة.

البيانات المحمية: البيانات المصنفة على أنها (سري للغاية، سري، مقيد.(

المعلومات العامة: البيانات بعد المعالجة - غير المحمية - التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها.

مستويات تصنيف البيانات: مستويات التصنيف التالية: سري للغاية، سري، مقيد، عام.

الفرد: الشخص المتقدم بطلب الاطلاع أو الحصول على المعلومات العامة.

ممثل بيانات أعمال: هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الجامعة، وغالباً ما يكون في ً مستوى إداري عال، ويمكن أن يوجد في الجامعة أكثر من ممثل بيانات أعمال.

مستخدم البيانات: أي شخص يمنح صلاحية الوصول إلى البيانات بغرض الاطلاع عليها أو استخدامها أو تحديثها وفقاً للمهام المصرح بها من قبل ممثل بيانات الأعمال.

الضوابط الأمنية: الأجهزة الإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ووسائل معالجتها والوصول إليها.

الإفصاح عن البيانات: تمكين أي شخص - عدا الجامعة - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.

التسويق: نشاط تبادل، أو تداول، أو تزويد البيانات الخام، أو البيانات المعالجة مقابل مبلغ نقدي أو قيمة عينية أخرى.

الأهداف

الغرض من هذه السياسة هو توفير متطلبات مكتب إدارة البيانات الوطنية وتوعية منسوبي الجامعة بأهمية حماية البيانات التي يتم انشاؤها، وتخزينها من قبل جامعة الأمير سطام بن عبد العزيز، ولتنظيم عملية نشر وتبادل استخدام/ إعادة استخدام البيانات المحمية والمعلومات العامة وتقليل المخاطر.

النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، الاجتماعات، الاتصالات عبر وسائل التواصل والتطبيقات، رسائل البريد الإلكتروني، البيانات المخزنة على وسائط إلكترونية، أشرطة الصوت أو الفيديو، الخرائط، الصور الفوتوغرافية المخطوطات الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال البيانات المسجلة.

المبادئ الرئيسية لتصنيف البيانات

المبدأ الأول: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، والسرية للغاية (في المجال السياسي والأمني) ما لم 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، وأقل عدد ممكن من العاملين.

المبدأ السابع: الحد الأدنى من الامتيازات

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

مستويات تصنيف البيانات

جدول ١ يوضح المستويات الرئيسية لتصنيف البيانات بما يتوافق مع مستوى الأثر، كما يوضح بعض الأمثلة الاسترشادية لكل مستوى.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشاديه
سري للغاية	عالي	تصنف 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 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	خطط وتفصيلات العمليات العسكرية أو أي معلومات ذات علاقة بها. المعلومات السياسية الرسمية المتعلقة بالعلاقات الدولية والاتفاقيات أو المعاهدات وكل ما يتعلق بها من مباحثات ودراسات وأعمال تحضيرية. المعلومات المتعلقة بأعمال وتدابير وتشكيلات الأجهزة الأمنية والاستخباراتية وتجهيزاتها. المعلومات المتعلقة بآليات ومفاتيح التشفير المستخدمة للبنى التحتية الوطنية.

		العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية أو الأعمال الحكومية. • أداء الجهات العامة مما يلحق ضررًا بالمصلحة الوطنية. • صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين. • الموارد البيئية أو الطبيعية	معلومات القضايا الإرهابية والمخططات المهددة للأمن. المعلومات المتعلقة بالأسلحة والذخائر أو المواقع العسكرية الاستراتيجية أو أي مصدر من مصادر القوة الدفاعية والهجومية. معلومات عن تحركات القوات المسلحة أو القوات العسكرية الأخرى، أو تحركات الشخصيات الهامة. معلومات تمس سيادة الدولة.
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 أو بالعلاقات الدبلوماسية و/أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية أو الأعمال الحكومية. • يُحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها أو خسارة جسيمة للقدرة التنافسية أو كليهما معًا. • يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد.	• معلومات عن مواقع تخزين المواد اللوجستية أو المخازن الاقتصادية. • معلومات متعلقة بالمنشآت الحيوية. • مذكرات التفاهم مع الشركات الدولية لإنشاء مصالح تجارية أو اقتصادية استراتيجية بالمملكة. • معلومات متعلقة بالاتفاقيات الثنائية ومذكرات التفاهم الدبلوماسية بين المملكة والدول الأخرى.

		• تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية. • التحقيق في القضايا الكبرى المحددة نظامًا، كقضايا تمويل الإرهاب.	
مقيّد	منخفض	تُصنف البيانات على أنها "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.	• معلومات تضر بسمعة أي شخصية عامة. • بيانات مفصلة للمعاملات الفردية. • نتائج الأبحاث والدراسات العملية قبل نشرها. • المعلومات المتعلقة بالمنتجات تحت التطوير والتي قد تضر بعدالة المنافسة. • معلومات متعلقة بالتعيينات والقرارات الإدارية الحساسة. • معلومات الملف الصحي للأفراد • معلومات تحديد الهوية مثل الاسم والعنوان وأرقام الهوية الوطنية وأرقام الهواتف وأرقام الحسابات والتراخيص وبيانات السمات الحيوية. • معلومات رواتب الموظفين. • وثائق مثل خطط المستوى التخطيطي وبرامج التسويق قبل الكشف عنها للجمهور وخطط الإبداع التقني. • عقود موردين وعروض أسعارهم. • طلبات تقديم عروض. • مواصفات منتج جديد قبل طرحه للجمهور. • تفاصيل تصميم وتطبيق أنظمة أمنية (جدار الحماية

			وضوابط الوصول ومخططات الشبكة وغيرها). • سياسيات وإجراءات الجهات الداخلية - رسائل / مذكرات داخلية • قوائم هواتف داخلية وقوائم البريد الإلكتروني لبعض الجهات.
عام	لا يوجد	• تُصنف 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 أعلاه - في حال عدم وجود تأثير على ما يأتي: • المصلحة الوطنية • نشطة الجهات • مصالح الأفراد • الموارد البيئة	• توجهات استراتيجية وطنية معلنة. • الإحصائيات الوطنية حول عدد السكان والبيئة والأعمال حسب الصناعة وغيرها. • التنمية العامة والدراسات الاقتصادية. • إجراءات الحكومة وسياستها • معلومات متعلقة بالخدمات العامة التي تقدمها الحكومة للمواطنين. • جهات الاتصال في المؤسسات. • إعلانات وظائف. • إعلانات عامة. • تصريحات صحفية • نتائج مالية معلنة للجمهور. • عروض منتجات (عامة). • معلومات العلاقات العامة. • أي معلومات متاحة علنًا على مواقع أي مؤسسة. • الإعلانات.

جدول ١ مستويات تصنيف البيانات

كما يمكن تصنيف البيانات المصنفة على مستوى، مقيد إلى مستويات فرعية بناءً على نطاق الأثر على النحو التالي:

مقيد -مستوى (أ): إذا كان نطاق الأثر على مستوى قطاع كامل أو نشاط اقتصادي عام.

مقيد - مستوى (ب): إذا كان نطاق الأثر على مستوى أنشطة عدة جهات أو على مصالح مجموعة من الأفراد.

مقيد: مستوى (ج): إذا كان نطاق الأثر على مستوى أنشطة جهة واحدة أو مصالح فرد معين.

وفي الجدول ٢ أدناه توضيح وتحديد لمستوى التصنيف الصحيح الذي يمكن الجامعة 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 الجامعة 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	سمعه المملكة		
الاعتبارات	هل ستخضع المعلومات لاهتمام وسائل الإعلام المحلية والدولية؟ هل ستعطي انطباع سلبي؟		
مستوى الأثر			
سري للغاية	سري	مقيد	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 الرئيسة	المصلحة الوطنية		
فئة الأثر الفرعية	العلاقات الدبلوماسية		
الاعتبارات	هل تشكل المعلومات خطرًا على العلاقات مع الدول الصديقة؟ هل تزيد من حدة التوتر الدولي؟ هل يمكن أن تؤدي إلى احتجاجات أو عقوبات من دول أخرى؟		
مستوى الأثر			
سري للغاية	سري	مقيد	عام
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 أو يحدث تأثير بسيط على المدى القصير.	لا يوجد تأثير على المصالح الحيوية الوطنية.

جدول ٢ فئات ودرجات تقييم الأثر وفقا لمستويات تصنيف البيانات

فئة الأثر الرئيسة	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	مقيد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تتأثر الكفاءة التشغيلية لحفظ النظام العام والأمن الوطني أو العمليات الاستخبارية 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 يُذكر 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 الرئيسة	المصلحة الوطنية
فئة الأثر الفرعية	الاقتصاد الوطني
الاعتبارات	هل يؤدي الكشف عن المعلومات إلى خسائر اقتصادية على المستوى الوطني؟

مستوى الأثر			
سري للغاية	سري	مقيد	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 سلبا على جميع القطاعات في المملكة .	تأثير طويل المدى على الاقتصاد الوطني مع انخفاض يمكن تداركه في الناتج المحلي الإجمالي ونسبة البطالة وأسعار الأسواق المالية أو القوة الشرائية مما ينعكس سلبا على قطاع واحد أو أكثر.	تأثير بسيط على الاقتصاد الوطني مع انخفاض يمكن تداركه في وقت قصير في الناتج المحلي والإجمالي ومعدل العمالة وأسعار الأسواق المالية أو القوة الشرائية مما ينعكس سلبا على قطاع واحد فقط.	

فئة الأثر الرئيسة	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 ستضل الخدمات الأساسية بالمملكة متاحة؟

مستوى الأثر			
سري للغاية	سري	مقيد	عام
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 الرئيسة	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	مقيد	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 .	

فئة الأثر الرئيسة	أنشطة الجهات
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	مقيد	عام
عالي	متوسط	منخفض	لا يوجد أثر
تأثير سلبي كبير على الجهات الخاصة إلى الحد الذي يتسبب في الإضرار بالمصالح الحيوية الوطنية .	تكبد خسائر مالية فادحة مما قد يؤدي إلى الإفلاس .	ضرر محدود يتمثل في خسارة مالية محدودة للجهة أو لأي من أصولها .	لا يوجد تأثير على أنشطة الجهات .

فئة الأثر الرئيسة	أنشطة الجهات
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 عدد كبير من الموظفين؟ هل سيؤثر على القدرة التنافسية للجهة الخاصة؟

مستوى الأثر			
سري للغاية	سري	مقيد	عام
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 الرئيسة	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: أسماء ومواقع العملاء السريين والأشخاص الخاضعين لأنظمة حماية خاصة)

مستوى الأثر			
سري للغاية	سري	مقيد	عام
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.

فئة الأثر الرئيسة	الأفراد
فئة الأثر الفرعية	الخصوصية
الاعتبارات	هل سيؤدي الكشف عن المعلومات إلى انتهاك خصوصية الأفراد؟

مستوى الأثر			
سري للغاية	سري	مقيد	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 الرئيسة	الأفراد
الاعتبارات	سيؤدي ذلك إلى انتهاك أي حقوق ملكية فكرية؟

مستوى الأثر			
سري للغاية	سري	مقيد	عام
عالي	متوسط	منخفض	لا يوجد أثر
مما يؤثر على المصلحة الوطنية.			

فئة الأثر الرئيسة	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	مقيد	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 أو محدودة على البيئة أو الموارد الطبيعية.	لا يوجد تأثير على البيئة.

ضوابط تصنيف البيانات

بناءً على مستويات التصنيف، تقوم الجامعة 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 وفقا 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 تعدها الجامعة ويتم اعتمادها من المسؤول الأول بالجامعة.

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 :

الأول: علامات الحماية

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

الثاني: الوصول

١. يمنح الوصول - المنطقي والمادي - إلى البيانات بناءً على مبدأ «الحد الأدنى من الامتيازات» و «الحاجة إلى المعرفة».
٢. يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بالجامعة.

الثالث: الاستخدام

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

الرابع: التخزين

١. لا تُترك البيانات المصنفة على أنها «سري للغاية» و «سري» و «مقيد» وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات دون مراقبة.
٢. يجب حماية البيانات المصنفة على أنها «سري للغاية» و «سري» و «مقيد» الغير المراقبة أثناء تخزينها ماديًا وإلكترونيا باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

الخامس: مشاركة البيانات

١. تقوم الجامعة بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
٢. يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجامعة 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 بُعد، أو الشبكة الخاصة الافتراضية...إلخ.

السادس: الاحتفاظ بالبيانات

١. يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
٢. يتم تحديد فترة الاحتفاظ بناء على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة .
٣. يتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

السابع: التخلص من البيانات

١. يتم التخلص من جميع البيانات بشكل آمن وفقا للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
٢. يتم التخلص من البيانات التي تم تصنيفها على أنها «سرية للغاية» و «سري» التي يتم التحكم بها إلكترونيًا باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
٣. يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
٤. يتم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.

الثامن: الأرشفة

١. يتم أرشفة البيانات في مواقع تخزين آمنة وفقًا للطريقة التي يوصي بها ممثل بيانات الأعمال.
٢. يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
٣. يتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها «سري للغاية» و «سري» باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
٤. يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

التاسع: إلغاء التصنيف (رفع السرية)

١. 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.
٢. في حال تم تصنيف البيانات بشكل خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
٣. 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 أخر إجراء على البيانات (على سبيل المثال، ستة أشهر من تاريخ آخر استخدام).
   - بعد انقضاء تاريخ محدد (على سبيل المثال، من المقرر مراجعتها في ١ يناير ٢٠٢١).
   - بعد ظروف أو أحداث معينة تؤثر تأثيرًا مباشرًا على البيانات (على سبيل المثال، إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجامعة).
٤. يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيدًا عن العوامل المساعدة على إلغاء التصنيف الواضحة تماما، فهمًا سليمًا لمحتوى البيانات السرية والسياق الذي وردت فيه.

الخطوات اللازمة لتصنيف البيانات

الخطوة ١- تحديد جميع بيانات الجامعة:

تتمثل الخطوة الأولى التي تتخذها الجامعة في جرد وتحديد جميع البيانات التي تمتلكها.

الخطوة ٢- تعيين مسؤول تصنيف البيانات:

على الجامعة تفويض شخص يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات، غالبًا ما يكون ممثل بيانات الأعمال - أحد منسوبي مكتب إدارة البيانات والذكاء الاصطناعي - هو الشخص الذي يفهم طبيعة البيانات وقيمتها داخل الجامعة، وهو الشخص الذي يجب أن يتحمل المسؤولية حيال إجراء التصنيف الأولي، ونظرًا لوجود أكثر من مسؤول بيانات داخل الجامعة، فقد يوجد أكثر من شخص مسؤول عن تصنيف البيانات.

الخطوة ٣ - إجراء عملية تقييم الأثر:

يجب على ممثل بيانات الأعمال اتباع الخطوات اللازمة لعملية تقييم الأثر المحتمل الذي يترتب على:

- الإفصاح عن هذه البيانات أو الوصول غير المصرح به لها.
- إجراء تعديل على هذه البيانات أو إتلافها أو كليهما.
- عدم الوصول إلى هذه البيانات في الوقت المناسب.

تبدأ عملية تقييم الأثر بتطبيق مبدأ «الأصل في البيانات الإتاحة» (في المجال التنموي) ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية وسرية للغاية (في المجال السياسي والأمني) ما لم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف.

الخطوة ٣-أ تحديد فئة الأثر:

يتمثل العنصر الأول من عملية تقييم الأثر في تحديد الفئة الرئيسية والفرعية للأثر المحتمل في أي من الفئات الرئيسية التالية:

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

الخطوة ٣-ب - تحديد مستوى الأثر:

يشير العنصر الثاني إلى أنه يتعين على ممثل بيانات الأعمال أن يحدد لكل أثر محتمل مستوى معين يعتمد تحديد المستوى على الآتي:

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

تحدد هذه المعايير مستويات الأثر الأربعة:

- **عالي:** يؤدي الوصول إلى 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 أي ضرر على المدى الطويل أو القصير.

يجب أن تكون جميع الأضرار المحتملة والمحددة خلال عملية تقييم الأثر محددة وقائمة على أدلة، في محاولة للحد من التقديرات الشخصية للمكلف بإجراء تصنيف البيانات.

يحدد ممثل بيانات الأعمال مستوى تصنيف البيانات بناء على الآثار المحددة ومستوياتها:

- **عالي:** تصنف البيانات باعتبارها (سرية للغاية).
- **متوسط:** تصنف البيانات على أنها (سرية).
- **منخفض:** يلزم إجراء مزيد من التقييمات (يرجى الاطلاع على الخطوة ٤ وه).
- **لا يوجد أثر:** تصنف البيانات على أنها بيانات "عامة."

ويوجد وصف مفصل للاعتبارات الرئيسية لكل فئة من فئات الأثر ومستواه في الجدول ٢ " فئات ومستويات تقييم أثر تصنيف البيانات".

يجب الأخذ بعين الاعتبار الخطوتين ٤ و٥ عندما يكون مستوى الأثر المحدد منخفض يتم الانتقال إلى الخطوة ٦ عندما تصنف البيانات باعتبارها «سرية للغاية» أو «سرية» أو «عامة».

الخطوة ٤ - تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفض):

يجب إجراء تقييمات إضافية إذا كان مستوى الأثر المحدد «منخفض» وذلك بهدف زيادة مستوى تصنيف البيانات المصنفة على أنها بيانات «عامة» إلى الحد الأقصى.

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 مخالفا لأنظمة فيجب حينها تصنيف البيانات على أنها بيانات «مقيدة»، بخلاف ذلك يتعين على ممثل بيانات الأعمال مواصلة تنفيذ الخطوة ٥.

الخطوة ٥ - الموازنة بين مزايا الإفصاح عن البيانات والآثار السلبية (فقط إذا كانت الإجابة على الخطوة ٤ "لا"):

بعد التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكا لأي نظام نافذ، يجب أيضا تقييم المزايا المحتملة للإفصاح عن مثل هذا 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 شفافية العمليات الحكومية 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"

الخطوة ٦ - مراجعة مستوى التصنيف:

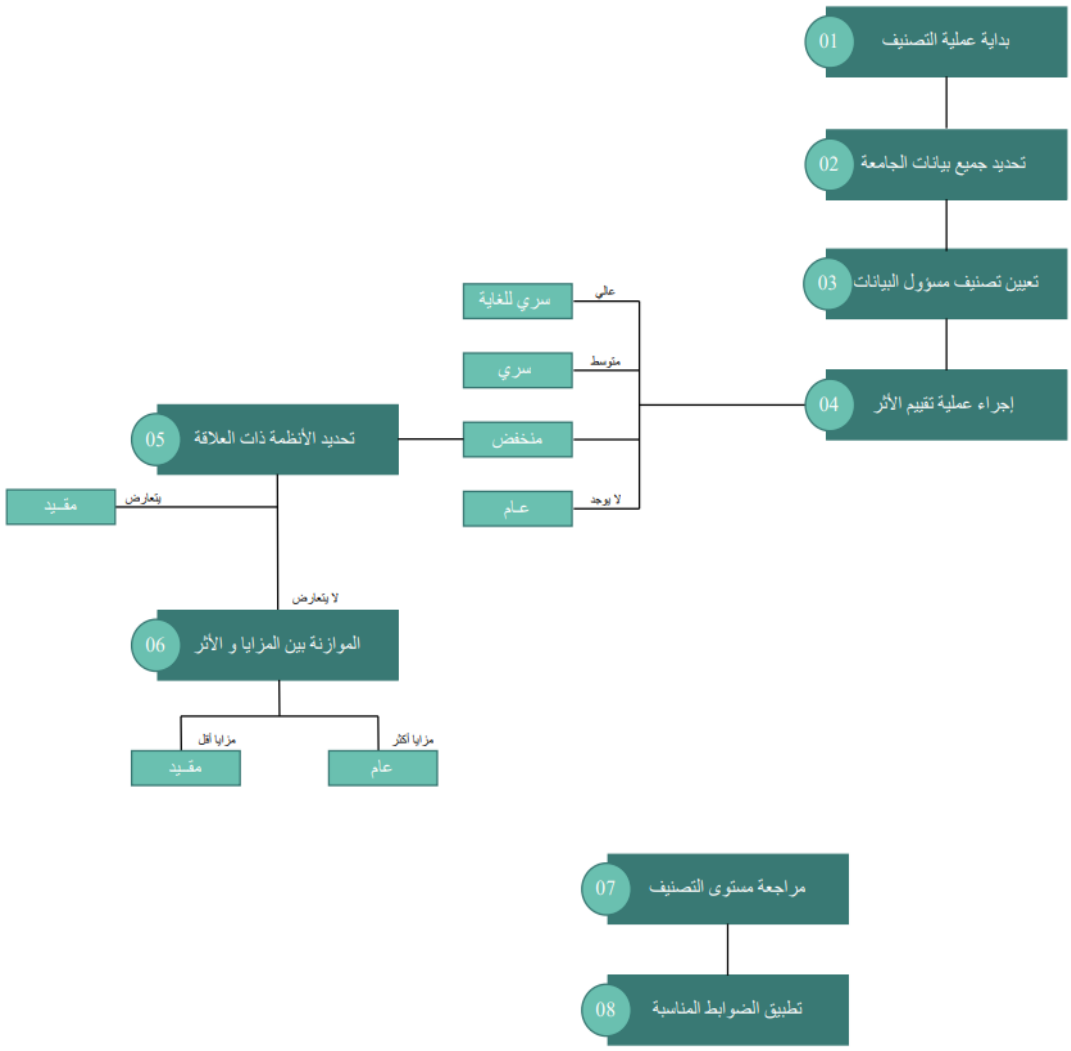
يجب أن يفحص مراجع تصنيف البيانات - أحد منسوبي مكتب إدارة البيانات والذكاء الاصطناعي - جميع البيانات المصنفة لضمان أن يكون مستوى التصنيف المحدد من جانب ممثل بيانات الأعمال هو الأنسب، وتتم مراجعته خلال شهر واحد من التصنيف الأولي.

الخطوة ٧- تطبيق الضوابط المناسب:

تتمثل الخطوة الأخيرة من عملية تصنيف البيانات في حماية جميع البيانات وفقا لمستوى التصنيف من خلال تطبيق عناصر التحكم ذات الصلة (راجع «ضوابط تصنيف البيانات») .

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

بعد تصنيف البيانات على نحو صحيح، يمكن للجامعة مشاركتها مع جهات أخرى، أو إتاحتها ونشرها كبيانات مفتوحة عند تصنيفها كبيانات (عامة).



رسم توضيحي ١ - لإجراءات تصنيف البيانات

الأدوار والمسؤوليات داخل الجامعة

على الجامعة تكليف أشخاص يتولون مسؤولية أداء الالتزامات المسندة لكل دور من الأدوار الوظيفية المرتبطة بعملية تصنيف البيانات وشروط حمايتها على النحو المنصوص عليه أدناه.

ممثل بيانات الأعمال - الشخص المسؤول عن البيانات التي تجمعها الجامعة أو تحتفظ بها، وعادة ما يكون في مستوى إداري عالي، ويكون ممثل بيانات الأعمال مسؤول عن:

- تصنيف البيانات - تصنيف البيانات التي تجمعها الجامعة أو الجهات التابعة لها.
- تجميع البيانات - التأكد من تصنيف البيانات المجمعة من مصادر متعددة من خلال أعلى مستويات التصنيف المستخدمة في تصنيف أي بيانات بشكل فردي.
- تنسيق تصنيف البيانات - التأكد من أن البيانات المتبادلة بين الإدارات أو الجهات مصنفة ومحمية بصورة متسقة.
- الامتثال لتصنيف البيانات (بالتنسيق مع مختصي بيانات الأعمال) - التأكد من أن البيانات محمية وفقًا للضوابط المحددة.

مراجع تصنيف البيانات - الشخص المسؤول عن مراجعة واعتماد مستويات تصنيف البيانات التي يحددها

ممثل بيانات الأعمال وعادة ما يكون في مستوى إداري عال.

مختص بيانات الأعمال -عادة ما يكون مختص بيانات الأعمال من أعضاء الإدارة العامة لتقنية المعلومات أو إدارة الأمن السيبراني أو كليهما ويتحمل مسؤولية حماية البيانات من خلال تطبيق الضوابط المعتمدة المحددة في قسم «ضوابط تصنيف البيانات» بالإضافة إلى ذلك، الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها. تتألف مسؤوليات مختص بيانات الأعمال:

- التحكم في الوصول - التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقا لمستويات تصنيف البيانات التي يحددها ممثل بيانات الأعمال.
- تقارير المراجعة - إرسال تقرير سنوي إلى مسؤولي البيانات يتناول توافر البيانات المصنفة وسلامتها وسريتها.
- النسخ الاحتياطي للبيانات - إجراء نسخ احتياطية منتظمة للبيانات.
- التحقق من صحة البيانات - التحقق من صحة البيانات بشكل دوري.
- استعادة البيانات - استعادة البيانات من وسائط النسخ الاحتياطي.
- نشاط المراقبة - مراقبة الأنشطة التي تتم على البيانات وتسجيلها، بما في ذلك البيانات المتعلقة بالشخص الذي يصل إلى هذه البيانات.
- الامتثال لتصنيف البيانات (بالاشتراك مع مسؤولي البيانات) - التأكد من تصنيف بيانات الجامعة وحمايتها بعد العملية الموضحة في هذه السياسة ووفقا للضوابط المحددة.

- مستخدم البيانات - الموظف الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدثها بغرض أداء مهمة يخولها له ممثل بيانات الأعمال، ويستغل المستخدمون البيانات بطريقة تتوافق مع الغرض المحدد وكذلك الامتثال لهذه السياسة وجميع السياسات المتعلقة باستخدام البيانات في المملكة العربية السعودية، ويكلف المسؤول الأول بالجامعة من يراه من ذوي الاختصاص لأداء هذه الأدوار.

الالتزام بالسياسة

١. راعي ومالك وثيقة السياسة: مدير مكتب إدارة البيانات والذكاء الاصطناعي.
٢. مراجعة السياسة وتحديثها: مكتب إدارة البيانات والذكاء الاصطناعي
٣. تنفيذ السياسة وتطبيقها: مكتب إدارة البيانات والذكاء الاصطناعي والإدارة العامة لتقنية المعلومات.
٤. يجب على مدير مكتب إدارة البيانات والذكاء الاصطناعي ضمان التزام جامعة الأمير سطام بن عبد العزيز بهذه السياسة دوريا ً.
٥. يجب على كافة العاملين في جامعة الأمير سطام بن عبد العزيز الالتزام بهذه السياسة .
٦. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة الأمير سطام بن عبد العزيز.