سياسة تصنيف البيانات

نسخة 1.0

التاريخ: 2025/4/12
نوع الوثيقة: سياسة
تصنيف الوثيقة: عام
رقم الإصدار: 1.0

جدول المحتويات

المادة الأولى: الغرض والنطاق

تهدف هذه السياسة إلى الحفاظ على سرية البيانات داخل الجامعة وحمايتها من الوصول أو التعديل غير المصرح به من خلال وضع تصنيف للبيانات يقسمها-وفق درجة حساسيتها وخطورتها-إلى أربع مستويات. تنطبق أحكام هذه السياسة على كل البيانات التي تنتجها الجامعة أو تتعامل معها أو تتلقاها، 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، كما تنطبق هذه السياسة على جميع منسوبي الجامعة الذين يتعاملون مع هذه البيانات واي انتهاك لهذه السياسة قد يعرض صاحب المخالفة الى اجراء تأديبي حسب الإجراءات المتبعة في الجامعة الاسلامية.

المادة الثانية: التعريفات

- **سياسة تصنيف البيانات:** حماية سرية البيانات الوطنية وتصنيفها على أربعة مستويات.
- **البيانات:** هي أي معلومات أو معلومات مسجلة، بغض النظر عن الشكل الذي تتخذه، بما في ذلك الوثائق الورقية والبيانات الإلكترونية والصور والفيديوهات والتسجيلات الصوتية.
- **مستويات تصنيف البيانات:** مستويات التصنيف التالية: (سري للغاية). (سري)، (مقيد)، (عام).
- **مستوى تصنيف البيانات:** هو مستوى الحساسية المخصص للبيانات، والذي يحدد مستوى الحماية المطلوب للبيانات.
- **البيانات الداخلية:** هي البيانات التي يمكن مشاركتها داخل الجامعة فقط مع الموظفين أو الطلاب الذين لديهم الحاجة إليها لأداء عملهم أو دراستهم.
- **البيانات السرية:** هي البيانات التي لا يمكن مشاركتها إلا مع عدد محدود من الأشخاص الذين لديهم إذن خاص بالوصول إليها.
- **البيانات الحساسة:** هي البيانات التي قد تسبب ضرراً كبيراً للجامعة أو للأفراد إذا تم الكشف عنها بشكل غير مصرح به.
- **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 للجهة لغرض استخدامها.
- **مستوى الوصول إلى البيانات:** مستوى يعتمد على الأذونات والصلاحيات التي تقيّد الوصول إلى البيانات والموارد التقنية على الأشخاص المصرح لهم وفقاً لما هو مطلوب لإنجاز المهام والمسؤوليات المناطة بهم.
- **سريّة البيانات:** الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.
- **البيانات المحميّة:** البيانات المصنفة على أنها (سرّي للغاية، سرّي، مقيّد).
- **البيانات العامة:** البيانات بعد المعالجة-غير المحمية-التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة مهما كان مصدرها، أو شكلها أو طبيعتها ويمكن مشاركتها مع الجمهور دون قيود.

- **مسؤول تصنيف البيانات:** هو الشخص المسؤول عن تطبيق سياسة تصنيف البيانات وضمان الامتثال لها.
- **مالكي البيانات:** هم الأشخاص المسؤولون عن تحديد فئة تصنيف البيانات وإدارة الوصول إليها.
- **مستخدمو البيانات:** هم الأشخاص الذين لديهم حق الوصول إلى البيانات.

المادة الثالثة: المسؤوليات

يعتبر مكتب إدارة البيانات مسؤولا عن جميع العمليات المرتبطة بالبيانات وذلك بالتنسيق مع الجهات المالكة للبيانات داخل الجامعة، وتكون صلاحية مشاركة البيانات مع الجهات خارج الجامعة مقتصرةً على موافقة مكتب إدارة البيانات.

المادة الرابعة: المبادئ الرئيسية لتصنيف البيانات

يجب مراعاة المبادئ التالية عند التعامل مع هذه السياسة والتي حددتها السياسات المعتمدة من الجهات التنظيمية وعلى مكتب إدارة البيانات التأكد من الالتزام بهذه المبادئ:

1. **الأصل في البيانات الإتاحة:** الأصل في البيانات أن تكون متاحة (في المجال التنموي) ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية، كما أن الأصل في البيانات أن تكون سريّة للغاية (في المجال السياسي والأمني) ما لم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.
2. **الضرورة والتناسب:** يتم تصنيف البيانات إلى مستويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سرّيتها.
3. **التصنيف في الوقت المناسب:** يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى، ويكون التصنيف خلال فترة زمنية محددة.
4. **المستوى الأعلى من الحماية:** يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات مستويات مختلفة من التصنيف.
5. **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.
6. **الحاجة إلى المعرفة:** يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، ولأقل عدد ممكن من العاملين.
7. **الحد الأدنى من الامتيازات:** يتم تقييد إدارة صلاحيات العاملين على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة بهم.

المادة الخامسة: مستويات تصنيف البيانات

يتم تصنيف البيانات في الجامعة إلى أربع مستويات:

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	**عالي**	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: • 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 يُلحق ضررًا بالمصلحة الوطنية. • صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين.	• 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 • معلومات القضايا الإرهابية والمخططات المهددة للأمن • المعلومات المتعلقة بالأسلحة والذخائر أو المواقع العسكرية الإستراتيجية 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

		• الموارد البيئية أو الطبيعية.	
سري	**متوسط**	تُصنف 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: • 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. • 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. • تؤدي إلى ضرر على المدى الطويل للموارد البيئية أو الطبيعية. • التحقيق في القضايا الكبرى المحددة نظاما، كقضايا تمويل الإرهاب.	• 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

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 محدود على عمل الجهات العامة أو الانشطة 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 • أنشطة 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

الجدول 1: مستويات تصنيف البيانات

كما يمكن تصنيف البيانات المصنّفة على مستوى مقيّد 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.

فئة الاثر	المصلحة الوطنية
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 الاثر			
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 سلباً على المدى الطويل	لن يحدث تأثير على العلاقات الدبلوماسية أو يحدث تأثير بسيط على المدى القصير	لا يوجد تأثير على المصالح الحيوية الوطنية.

فئة الاثر	المصلحة الوطنية
الاعتبارات	هل المعلومات - في حال نشرها - تساعد على تنظيم أعمال إرهابية أو ارتكاب جرائم خطيرة؟ هل تُشكل مصدر ذعر للجميع؟

مستوى الاثر			
سري للغاية	سري	مقيد	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 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 الاثر	أنشطة الجهات
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 الاثر			
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 الجهة 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 الاثر	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 الاثر			
سري للغاية	سري	مقيد	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

الجدول 2: فئات ودرجات تقييم الأثر وفقاً لمستويات تصنيف البيانات

المادة السادسة: ضوابط تصنيف البيانات

- بناءً على مستويات التصنيف، يقوم مكتب إدارة البيانات 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، تُعامل هذه البيانات على أنها "مقيّدة" 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 المسؤول الأول بمكتب إدارة البيانات.
- فيما يلي بعض الأمثلة على بعض الضوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرجوع إلى ما يصدر عن الهيئة الوطنية للأمن السيبراني من ضوابط وإرشادات تتعلق بحماية البيانات:

1. **علامات الحماية:**

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

2. **الوصول:**

- يمنح الوصول -المنطقي والمادي- للبيانات بناءً على مبدأ" الحد الأدنى من الامتيازات" الحاجة إلى المعرفة".
- يجب منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة للعاملين بالجهة.

3. **الاستخدام:**

تستخدم البيانات المصنفة وفقا لمتطلبات مستويات التصنيف، مثلا، يتم تقييد استخدام البيانات التي تكون مصنفة على أنها" سرية للغاية" ماديا على أناس ومكاتب معينين أو افتراضيا باستخدام ترميز للأجهزة أو تطبيقات خاصة.

4. **التخزين:**

- يجب ألا تترك البيانات التي تصنف على أنها" سرّي للغاية "أو" سرّي "أو" مقيّد "وكذلك الأجهزة التي تخزن هذه البيانات أو تعالجها بما في ذلك الأجهزة المحمولة دون مراقبة.
- يجب حماية البيانات غير المراقبة والمصنفة على أنها "سرّي للغاية" أو "سرّي" أو "مقيّد" أثناء تخزينها ماديّاً أو إلكترونياً باستخدام أحد طريق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

5. **مشاركة البيانات:**

- يقوم مكتب إدارة البيانات بتحديد الوسائل المناسبة لتبادل البيانات بشكل آمن سواءً كانت ماديّة أو رقميّة، وبما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات.
- يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجهات ستستخدم الوسائل المستخدمة حاليا لتبادل البيانات أم لا، على سبيل المثال قناة التكامل الحكومية وشبكة مركز المعلومات الوطني والشبكة الحكومية الآمنة.

6. **الاحتفاظ بالبيانات:**

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

7. **التخلص من البيانات:**

- يتم التخلص من جميع البيانات بشكل آمن وفقا للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
- يتم التخلص من البيانات الي تُصنف على أنها" سرّي للغاية "أو" سرّي "والتي يتحكم بها إلكترونيا باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
- يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
- يُعد سجل مفصل عن جميع البيانات التي تم التخلص منها.

8. **الأرشفة:**

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

9. **إلغاء التصنيف (رفع السرّية):**

- يتم إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد 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.
- يتم تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، كما يجب تسجيلها في سجل أصول البيانات، وقد تتضمن هذه العوامل ما يلي:
  - فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (مثلا: عامين بعد الإنشاء).

- فترة زمنية محددة بعد اتخاذ آخر إجراء على البيانات (مثلا: ستة أشهر من تاريخ آخر استخدام).
- بعد انقضاء تاريخ محدد (مثلا، من المقرر مراجعتها في ١ يناير ٢٠٢١).
- بعد ظروف أو أحداث معّينة تؤثر تأثيرا مباشرا على البيانات (مثلا، إحداث تغيير في الأولويات والاستراتيجيات أو تغيير موظفي الجهات الحكومية (الجامعة).

- يتطلب إلغاء التصنيف -رفع السرّية-أو خفض مستويات التصنيف، بعيدا عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرّية والسياق الذي وردت فيه.
- لا يتم تغيير درجة السرّية إلا بموافقة مكتوبة من الجهة المختصة التي هي مصدر البيانات وتحت إشراف مكتب إدارة البيانات.

المادة السابعة: الخطوات اللازمة لتصنيف البيانات

الخطوة 1 - تحديد جميع بيانات الجامعة

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

الخطوة 2 - 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 - 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 3 - 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) مالم تقتضِ طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية؛ وسرية للغاية (في المجال السياسي والأمني) مالم تقتضِ طبيعتها أو حساسيتها مستويات أدنى من التصنيف.

الخطوة 3-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 3-ب - تحديد مستوى الأثر:

يُشير 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 أضرارٍ 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 أضرارٍ 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 محاولةٍ للحد من التقديرات الشخصية للمكلف بإجراء تصنيف البيانات.

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

- عالي - تُصنف البيانات باعتبارها "سرية للغاية".
- متوسط - تُصنف البيانات على أنها "سرية".
- منخفض - يلزم إجراء مزيدٍ من التقييمات.
- لا يوجد أثر- تُصنف البيانات على أنها بياناتٍ "عامة".

الخطوة 4 – 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 الالكترونية ... الخ، وإذا كان الإفصاح عن البيانات مخالفًا للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيّدة"، بخلاف ذلك يتعين على ممثل بيانات الأعمال مواصلة تنفيذ الخطوة 5.

بعد التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكًا لأي نظام نافذ، يجب أيضًا 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 الافراد 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 "مقيّدة"

الخطوة 6 - مراجعة مستوى التصنيف

يجب أن يفحص مراجع تصنيف البيانات - أحد منسوبي مكتب الجهة - 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 7 - تطبيق الضوابط المناسبة

تتمثل الخطوة الأخيرة من عملية تصنيف البيانات في حماية جميع البيانات وفقًا لمستوى التصنيف من خلال تطبيق عناصر التحكم ذات الصلة.

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

بعد تصنيف البيانات على نحوٍ صحيح، يمكن للجهات مشاركتها مع جهات أخرى، أو اتاحتها ونشرها كبيانات مفتوحة عند تصنيفها كبيانات "عامة"

المادة الثامنة: الأدوار والمسؤوليات داخل الجهة

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

ممثل بيانات الأعمال - الشخص المسؤول عن البيانات التي تجمعها الجهة أو تحتفظ بها، وعادةً ما يكون في مستوى إداري عالٍ، ويكون ممثل بيانات الأعمال مسؤول عن:

- تصنيف البيانات - تصنيف البيانات التي تجمعها الجهة أو الجهات التابعة لها.
- تجميع البيانات - التأكد من تصنيف البيانات المجمعة من مصادرٍ 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 عالٍ.

مختص بيانات الأعمال - عادةً ما يكون مختص بيانات الأعمال من أعضاء إدارات تقنية المعلومات أو أمن المعلومات 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 وفقًا 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 الجهة وحمايتها بعد العملية الموضحة في هذه السياسة ووفقًا للضوابط المحددة.

مستخدم البيانات - الموظف الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدّثها 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، ويُكلف المسؤول الأول بالجهة من يراه من ذوي الاختصاص لأداء هذه الأدوار.