
# سياسة تصنيف البيانات بجامعة الباحة

الإصدار ١,٠

## إعداد الوثيقة :

| الدور | الاسم | التاريخ | التوقيع |
|---|---|---|---|
| المالك | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات بجامعة الباحة | أبريل ٢٠٢٣ | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات |
| المُراجع | فريق مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات | أبريل ٢٠٢٣ | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات |
| المصرّح | فريق مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات | أبريل ٢٠٢٣ | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات |
| المعمِّد | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات | أبريل ٢٠٢٣ | مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات |

## جدول الاصدارات

| النسخة | التاريخ | المساهم | التعديل |
|---|---|---|---|
| ١,٠ | أبريل ٢٠٢٣ | فريق مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات | الإصدار الأول |

# قائمة المحتويات

# المصطلحات والتعاريف

| المصطلح | التعريف |
|---|---|
| الجامعة | جامعة الباحة |
| الخطة الاستراتيجية "واعد" | الخطة الاستراتيجية لجامعة الباحة ٢٠٢٠_٢٠٢٥ |
| العمادة | عمادة التعلم الإلكتروني وتقنية المعلومات بكافة وكالاتها وأقسامها |
| المكتب | مكتب إدارة البيانات بجامعة الباحة |
| مكتب إدارة البيانات الوطنية | الجهة المختصة بكل ما يتعلق بإدارة البيانات في المملكة العربية السعودية، وتعد المرجع الوطني في شؤونها. |
| منسوبي الجامعة | يقصد به الطلاب والطالبات وأعضاء هيئة التدريس ومن في حكمهم والإداريين. |
| منسوبي العمادة | يقصد به أعضاء إدارة العمادة وموظفي وموظفات العمادة ويشمل محللي الأعمال، ومطوري الخدمات، ومشغلي مركز البيانات وفرق التعلم الإلكتروني والدعم الفني والشؤون الإدارية والأمن السيبراني. |
| البيانات | مجموعة من الحقائق في صورتها الأولي أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصور الثابتة أو الفيديو أو التسجيلات الصوتية أو الرموز التعبيرية. |
| سرية البيانات | الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها |
| سلامة البيانات | حماية البيانات من أي تعديل أو إتلاف غير مصرّح به نظاماً |
| البيانات المحمية | البيانات المصنّفة على أنها (سري للغاية ،سري، مقيّ) |
| توافر البيانات | ضمان إمكانية الوصول المناسب والموثوق إلى البيانات واستخدامها عند الحاجة. |
| التحقق | التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية. |
| البيانات الشخصية | كل بيان – مهما كان مصدره أو شكله -من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابل للتعرف ا 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. |

| | |
|---|---|
| التصريح | تعريف حقوق وصلاحيات الوصول إلى البيانات والموارد التقنية لأي مستخدم أو برنامج أو عملية، والتحكم بمستويات الوصول إليها. |
| الوصول | القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجهة لغرض استخدامها. |
| مستويات تصنيف البيانات | مستويات التصنيف التالية: (سري للغاية)،(سري ) (مقيّد) (عام.). |
| البيانات الوصفية | هي المعلومات التي تصف البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التقنية والتشغيلية. |
| مستخدم البيانات | أي شخص يمنح صلاحية الوصول إلى البيانات بغرض الاطلاع عليها أو استخدامها ا أو تحديثها وفقاً للمهام المصرح بها من قبل ممثل بيانات الأعمال. |

## مقدمة

تهدف سياسات حوكمة البيانات الوطنية إلى فهم وتطبيق المبادئ الرئيسية التي تنظم عملية التعامل مع البيانات وذلك ببيان كيفية حمايتها وطرق مشاركتها او إتاحتها للعموم ومعايير العمل بها مما يؤدي للاستفادة من قيمة البيانات باعتبارها موردا اقتصاديًا يساعد على الابتكار ويساهم في دعم التحولات الاقتصادية وتعزيز المقومات التنافسية للدول.

واستناداً إلى الامر السامي الكريم رقم (٣٧١٢٦) وتاريخ ١٤٤٣/٠٦/١٥هـ ، والمتضمن ضرورة قيام الجهات الحكومية بتطبيق تصنيف البيانات الوارد في سياسات حوكمة البيانات الوطنية، قام مكتب إدارة البيانات بعمادة التعلم الالكتروني وتقنية المعلومات بالجامعة بإعداد النسخة الأولى من سياسة تصنيف البيانات لتحقيق أعلى مستويات الالتزام.

## الهدف

تهدف هذه السياسة إلى وضع إطار موحد لتصنيف البيانات إلى أربعة مستويات ( **سري للغاية ، سري ،مقيد، عام** ) وذلك بناء على نتائج تقييم الأثر المترتب على الإفصاح غير المصرح به نظاماً أو الوصول غير المصرح به نظاماً عن البيانات أو عن محتواها ، بحيث يحدد هذا الإطار آلية الاطلاع على البيانات والتعامل معها وفقاً لمستوى تصنيفها. وكذلك الالتزام بمتطلبات مكتب إدارة البيانات الوطنية والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي من الضابط رقم DC.1 إلى DC.٥ من ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية الإصدار ١,٥ (٢٠٢١) الصادرة من مكتب إدارة البيانات الوطنية.

## النطاق

تنطبق أحكام هذة السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها. وتتواءم هذة السياسة مع سياسات حوكمة البيانات الوطنية الصادرة من مكتب إدارة البيانات الوطنية وسياسات الهيئة الوطنية للأمن السيبراني ذات العلاقة، وبما لا يتعارض مع هذة السياسات ومع الأنظمة المرعية وما يصدر بشأنها من تعديلات.

## المستهدفين

جميع البيانات التي تنتجها الجامعة، أو تتلقاها، أو تتعامل معها.

## نظام تصنيف البيانات

يهدف تصنيف البيانات إلى حماية **سرية وسلامة وتوافر البيانات** التي تنتجها الجامعة، أو تتلقاها، أو تتعامل معها بأي وسيلة كانت.

- **سرية البيانات:** تقييد الوصول إلى البيانات، أو الافصاح عنها.
- **سلامة البيانات:** ضمان دقة وصحة البيانات من التعديل أو الإتلاف غير المصرح به نظاماً.
- **توافر البيانات:** ضمان الوصول إلى البيانات أو استخدامها في الوقت المناسب وبشكل مستدام.

## المبادئ الأساسية لتصنيف البيانات

### المبدأ الأول: الأصل في البيانات الإتاحة

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

### المبدأ الثاني: الضرورة والتناسب

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

### المبدأ الثالث: التصنيف في الوقت المناسب

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

### المبدأ الرابع: المستوى الأعلى من الحماية

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

### المبدأ الخامس: فصل المهام

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

### المبدأ السادس: الحاجة إلى المعرفة

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

### 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

يعد تصنيف البيانات خطوة أساسية في خطة حوكمة البيانات بجامعة الباحة ويشمل تحديد مستويات البيانات التي تتعامل معها الجامعة، كما يتضمن أيضاً تحديد مدى حساسية البيانات والأثر المحتمل الناتج عن تعرضها للخطر أو الفقد أو إساءة الاستخدام أو الإفصاح غير المصرح به نظاماً عن تلك البيانات

**بيانات سرية للغاية**: بيانات تشارك مع أشخاص محددين وغير قابلة لإعادة التوجيه أو النشر للأشخاص غير المصرح لهم، والكشف عنها له تأثير عالٍ على صورة الجامعة.

**بيانات سرية**: بيانات يكشف عنها داخل قسم واحد أو مشروع واحد وهي بيانات متوسطة الحساسية وقد يضر الجامعة الكشف عنها.

**بيانات مقيدة**: بيانات قابلة للمشاركة داخل الجامعة فقط وليس خارجها، والكشف عنها لا يؤثر سلبيا على الجامعة.

**بيانات عامة**: بيانات قابلة للمشاركة داخل وخارج الجامعة، وتاثير الكشف عنها محايد أو إيجابي على الجامعة.

ويوضح الجدول أدناه مستويات تصنيف البيانات:

| مستوى التصنيف | درجة الأثر | الوصف |
|---|---|---|
| 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 لا يمكن تداركه أو إصلاحه على :<br>• مصالح الجامعة فيما يتعلق بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة الجامعة أو بالعلاقات الجامعية أو الكفاءة التشغيلية للعمليات البنية التحتية الوطنية أو أعمال الجامعة.<br>• أداء جامعة الباحة مما يُلحق ضرراً بمصلحة الجامعة<br>• صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين .<br>الموارد البيئية أو الطبيعية . |
| 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 واستثنائي لا يمكن تداركه أو إصلاحه على :<br>• المصالح الوطنية مثل إلحاق ضرر جزئي بسمعة الجامعة والكفاءة التشغيلية للعمليات البنية التحتية الوطنية وأعمال الجامعة.<br>• يحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجامعة عن أداء مهامها.<br>يتسبب في حدوث أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد . |
| مقيد | منخفض | • تُصنف البيانات على أنها »بيانات مقيدة«، 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 :<br>• تأثير سلبي محدود على عمل الجامعة أو على أنشطتها أو على عمل شخص معين .<br>• ضرر محدود على أصول الجامعة وخسارة محدودة على وضعها المالي والتنافسي .<br>ضرر محدود على المدى القريب للموارد البيئية أو الطبيعية . |
| عام | لا يوجد | 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 لا يمكن تداركه أو إصلاحه على :<br>• مصالح الجامعة فيما يتعلق بالاتفاقيات والمعاهدات أو إلحاق الضرر بسمعة الجامعة أو بالعلاقات الجامعية أو الكفاءة التشغيلية للعمليات البنية التحتية الوطنية أو أعمال الجامعة.<br>• أداء جامعة الباحة مما يُلحق ضرراً بمصلحة الجامعة<br>• صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين .<br>الموارد البيئية أو الطبيعية . |

جدول :مستويات تصنيف البيانات

كما يمكن تصنيف البيانات المصنفة على مستوى مقيد إلى مستويات فرعية بناء 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.

## الخطوات المتبعة لتقييم الأثر

تعتمد الإجراءات التفصيلية لتصنيف البيانات على طبيعة أنشطة الجامعة والبيانات التي تتعامل معها، ويمكن للجامعة الرجوع أو الاستفادة من الممارسات العالمية والمواصفات القياسية لتقييم الآثار والمخاطر – ومنها على سبيل المثال: ISO NIST – عند إعداد الإجراءات الخاصة بها والمتعلقة بتقييم الآثار المحتملة.

- ومن الخطوات المساعدة على تقييم الأثر (على سبيل المثال لا الحصر) . تحديد نطاق تقييم الآثار والمخاطر (على سبيل المثال، يكون نطاق تقييم الأثر هو: محاضر الاجتماعات التي سيتم مشاركتها عبر البريد الالكتروني مع جهات أخرى).
- توصيف محتوى ونوع البيانات ( على سبيل المثال، بيانات ائتمانية، بيانات صحية، الخ ) وتوصيف المستخدمين لهذه البيانات ومهامهم ومسئولياتهم، وكذلك الأنظمة والتشريعات ذات العلاقة.
- تحديد مصادر التهديد المتوقع استغلالها لهذه الثغرات وتحليل الامكانيات الممكن استخدامها من قبل هذه المصادر.
- تحديد الآثار المحتملة من استغلال هذه الثغرات على شكل درجات وتقييمها بناء على قياس شدة أثرها ( على سبيل المثال، أن يكون الاثر المترتب هو الإساءة لسمعة الجامعة ، ودرجة هذا الأثر "عالي"، وذلك من خلال تحليل استفادة مصادر.
- تحليل الضوابط الأمنية المستخدمة لضمان المحافظة على سرية وسلامة وتوافر هذه البيانات، وتحديد نقاط الضعف والثغرات الأمنية والتي من المحتمل استغلالها من قبل مصادر التهديد .
- التهديد من البيانات في حال الوصول إليها، أو الافصاح عنها أو استخدامها أو التعديل عليها أو إتلافها بطريقة غير مصرح بها نظاماً.
- بناء على قياس شدة الأثر الذي تم تقييمه بالخطوات السابقة، يتم الرجوع إلى مستويات تصنيف البيانات، وتحديد التصنيف الملائم وفقاً للمعايير الموضحة لكل مستوى.

## السياسات التنفيذية والإجراءات:

١. مسؤولية تصنيف البيانات تقع على عاتق المسؤول عن هذه البيانات (ممثل بيانات الأعمال)، كل في مجال عمله، ويتعين على المستخدمين المخولين بدخول نظم الجامعة الأكاديمية أو الإدارية أن يتحققوا من تصنيف البيانات التي يدخلون إليها من ممثل بيانات الأعمال في الجهة التي يعمل بها قبل أن يشاركوا الآخرين هذه البيانات داخلياً أو خارجياً.

٢. ممثلوا بيانات الأعمال مسؤولون عن مراجعة وتقييم البيانات التي تقع تحت مسؤوليتهم وكذلك عن تصنيفها وفق الفئات الآنف ذكرها والرفع بها لاعتماد تصنيفها.

٣. ممثلوا بيانات الأعمال مسؤولون عن تطبيق كافة إجراءات الضبط اللازمة لضمان تأمين الحماية الكافية لبيانات الجامعة وذلك ضمن المسؤوليات المنوطة بهم.

٤. مكتب إدارة البيانات هو المسؤول عن تطبيق هذه السياسة بالتعاون مع وكالة عمادة التعلم الالكتروني وتقنية المعلومات لشؤون تقنية المعلومات ..

٥. مدير مكتب إدارة البيانات مسؤول عن التنسيق والعمل مع ممثلوا البيانات في الجامعة وذلك للمساعدة في تطبيق إجراءات ضبط البيانات وفق تعريفها ومسمياتها التي وضعها ممثلوا البيانات.

٦. جميع الموظفين الذين لديهم صلاحية على أنظمة وخدمات الجامعة والبيانات بجميع أنواعها مسؤولون عن استخدام البيانات تبعاً للتعريفات والتصنيفات التي يحددها ممثلوا بيانات الأعمال.

## ضوابط تصنيف البيانات

تقوم وكالة عمادة التعلم الالكتروني وتقنية المعلومات للتحول الرقمي والأمن السيبراني بتحديد وتطبيق الضوابط الأمنية المناسبة لحماية بناء البيانات وذلك لضمان التعامل معها ومعالجتها ومشاركتها والتخلص منها بشكل آمن، وفي حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقاً 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 الجهة ويتم اعتمادها من رئيس الجامعة .

## آلية الاحتفاظ وإتلاف البيانات وفقاً لمستوى تصنيفها:

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

### علامات الحماية

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

### الوصول

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

### الاستخدام

- تستخدم 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.

### التخزين

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

## مشاركة البيانات

- تقوم الجهات بتحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة مشاركة البيانات
- يجب الاتفاق على آلية تبادل البيانات، سواء كانت الجهات ستستخدم 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 .

## الاحتفاظ بالبيانات

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

## 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 التي تم تصنيفها على أنها "سرية للغاية " وسري" التي يتم التحكم بها إلكترونياً باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
- يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق .
- يتم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.

## الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقا 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.

### إلغاء التصنيف (رفع السرية)

- يجب 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 .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 على البيانات (على سبيل المثال إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية .)
- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيدا عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

## الالتزام بالسياسة

- يجب على مكتب إدارة البيانات بعمادة التعلم الإلكتروني وتقنية المعلومات تطبيق وضمان التزام جامعة الباحة بهذه السياسة.
- يجب على جميع منسوبي جامعة الباحة من أعضاء هيئة تدريس وموظفين ومن في حكمهم الالتزام بهذه السياسة وفق أدوارهم.
- قد يتعرض من ينتهك هذه السياسة إلى المسائلة النظامية المتبعة في هذا الشأن.

## التشريعات ذات الصلة

الهيئة السعودية للبيانات والذكاء الاصطناعي- مكتب إدارة البيانات الوطنية.

https://sdaia.gov.sa/ar/Sectors/Ndmo/Pages/default.aspx

نهاية المستند،