



مكتب إدارة البيانات
Data Management Office

سياسة تصنيف البيانات

الإصدار الثاني
فبراير ٢٠٢٥ م

سعيًا لتطبيق هذه السياسات، تم تحديد معاني الكلمات والمصطلحات الرئيسية الواردة فيها، وتعني أيما وردت المعاني الموضحة أمامها، ما لم يقتض سياق النص خلاف ذلك، وهي:

1. **الجامعة:** جامعة الملك عبدالعزيز.
2. **المكتب:** مكتب إدارة البيانات بجامعة الملك عبدالعزيز.
3. **البيانات:** مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو التسجيلات المرئية أو التسجيلات الصوتية أو الرموز التعبيرية.
4. **إدارة البيانات:** عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول الإستراتيجية.
5. **الضوابط:** هي مجموعة من المبادئ والقواعد والتوجيهات التي تمكن المنظمة من الوصول إلى أهدافها بعيدة المدى.
6. **مستويات تصنيف البيانات:** مستويات التصنيف المعتمدة من مكتب إدارة البيانات الوطنية، وهي: "سري للغاية"، "سري"، "مقيد"، "عام".
7. **الوصول إلى البيانات:** القدرة على الوصول المنطقي والمادي إلى البيانات لغرض استخدامها.
8. **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 دمجها مع بيانات أخرى، ويشمل ذلك- على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد، وغير ذلك من البيانات ذات الطابع الشخصي.
9. **الامتثال:** تطبيق بنود هذه السياسة وضمان المراقبة الدورية لذلك.
10. **الإفصاح:** تمكين أي شخص - عدا جهة التحكم أو جهة المعالجة بحسب الأحوال - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.
11. **الصلاحيات:** عملية إعطاء الأفراد أو الجهات قدرات أوسع أو (سلطة) لممارسة التحكم وتحمل المسؤولية عن مهام محددة.
12. **الإجراءات:** يقصد بها تصميم خطوات العمل في الجهة وتوثيقها بحيث تتم بتسلسل واضح حسب الأنظمة واللوائح والمسؤوليات الموجودة في الهيكل التنظيمي لضمان الكفاءة المناسبة التي تخدم توجه الجهة في تحسين العمليات وتقديم الخدمات.
13. **السياسة:** وثيقة تنظيمية تقوم بتحديد السياق أو طريقة العمل لإرشاد وتحديد الخطوات الحالية والمستقبلية، كما تحدد المطلوب من الجهات داخل الجامعة أو خارجها من خلال المبادئ التي تضمنتها السياسات.
14. **التشفير:** تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر. لا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فك تشفيرها.

الهدف

تهدف هذه السياسة إلى وضع سياسات تصنيف البيانات بجامعة الملك عبدالعزيز وفق أفضل الممارسات المحلية والدولية، كما تهدف - أيضاً - إلى الالتزام بالمتطلبات التشريعية الصادرة عن مكتب إدارة البيانات الوطنية وهي سياسة وضوابط تصنيف البيانات وجميع السياسات الأخرى ذات العلاقة.

النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواء أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، 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.

ملكية هذه السياسة

تعود ملكية سياسات تصنيف البيانات إلى مكتب إدارة البيانات في جامعة الملك عبدالعزيز، وإصدار النسخ المحدث منها.

الامتثال لهذه السياسات

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسات، وعلى جهات الجامعة ضمان تطبيق هذه السياسات داخل إداراتها، علماً بأن الالتزام بنود هذه السياسات يخضع لمراجعة دورية من مكتب إدارة البيانات بالجامعة، وأي عدم التزام أو انتهاك لها سيؤدي إلى المساءلة القانونية واتخاذ الإجراءات اللازمة حسب ما يوصي به مكتب إدارة البيانات بالجامعة.

يتم تصنيف البيانات وفق المبادئ الرئيسية التالية:

المبدأ الأول: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة "عامة" ما لم تقتضي طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية.

المبدأ الثاني: الضرورة والتناسب

يتم تصنيف البيانات بما يتناسب مع طبيعتها ومستوى حساسيتها، مع الأخذ بعين الاعتبار الأهمية للبيانات والحاجة إلى حمايتها من ثم 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، وذلك لضمان معالجتها وحمايتها بشكل مناسب منذ البداية.

المبدأ الرابع: المستوى الأعلى من الحماية

في حال تضمين مجموعة من البيانات مستويات مختلفة من التصنيف، يتم اعتماد مستوى التصنيف الأعلى لضمان الحماية الكاملة لجميع البيانات ذات الصلة.

المبدأ الخامس: فصل المهام

يتكفل مكتب إدارة البيانات بالجامعة بالمهام والمسؤوليات حصرياً فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها ولا يحق لأي جهة من جهات الجامعة القيام بها أو عدم الخضوع لها.

المبدأ السادس: الحاجة إلى المعرفة

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، بحيث تمنح الصلاحيات لمنسوبي الجامعة في الوصول للبيانات بقدر حاجة مهامهم الوظيفية لذلك.

المبدأ السابع: الحد الأدنى من الامتيازات

يتم تقييد إدارة صلاحيات الوصول على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناط به للمنسوين.

هذه المبادئ تضمن تطبيق سياسة تصنيف البيانات بطريقة تراعي الاحتياجات الخاصة للبيئة الأكاديمية والإدارية للجامعة، مع الحفاظ على الأمان والخصوصية لجميع البيانات ذات الصلة.

يتم تصنيف البيانات إلى أحد المستويات التالية: **سري للغاية، سري، مقيد، عام**. يوضح الجدول التالي مستويات التصنيف بناءً على الأثر.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	عالي	البيانات التي تصنف على أنها "سري للغاية" هي تلك التي تحتوي على معلومات حساسة جدًا، والتي إذا تم الوصول إليها أو الكشف عنها بطريقة غير مصرح بها، يمكن أن تؤدي إلى أضرار جسيمة وغير قابلة للإصلاح بالنسبة للأمن والسمعة والوضع التشغيلي للجامعة والمصالح الوطنية والشؤون المتعلقة بالتعليم والبحث العلمي. هذه الفئة من البيانات تتطلب أعلى درجات السرية والحماية نظرًا للعواقب الوخيمة المحتملة على الجامعة والأفراد المرتبطين بها في حالة إساءة استخدامها أو تسريبها.	• بيانات حول البحوث السرية أو غير المنشورة التي تحمل القدرة على إحداث تغيير كبير في مجال معين. • تفاصيل حول التقنيات الناشئة أو الملكية الفكرية التي لم يتم توثيقها بعد والتي يمكن أن تعطي ميزة تنافسية كبيرة. • السجلات المتعلقة بالموظفين أو الطلاب التي تحتوي على معلومات شخصية حساسة مثل السجلات الطبية أو المعلومات المالية. • تفاصيل البروتوكولات الأمنية الخاصة بال الحرم الجامعي، بما في ذلك أنظمة المراقبة وإجراءات الاستجابة للحوادث. • تفاصيل حول بنية تقنية المعلومات والاتصالات الحساسة وأنظمة الشبكات التي تدعم عمليات الجامعة الحيوية. • مستندات تحتوي على قرارات إدارية كبرى، مثل التعيينات الجديدة أو الخطط الاستراتيجية. هذه الأمثلة تعكس نوعية البيانات التي يجب أن تعالج بأقصى درجات الحذر والسرية في الجامعة، ويجب حمايتها من أي وصول غير مصرح به لضمان الحفاظ على سلامة وأمان الجامعة ومجتمعها.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري	متوسط	مستوى التصنيف "سري" يشمل البيانات التي تعتبر حساسة والتي يمكن أن يؤدي الوصول غير المصرح به إليها أو الإفصاح عنها إلى ضرر ملموس لكن يمكن تداركه على الوضع التشغيلي، السمعة، أو الأصول للجامعة. هذه البيانات تتطلب إجراءات حماية مهمة لكنها لا تحتاج إلى مستوى الحماية الشديد الذي تتطلبه البيانات المصنفة كـ "سري للغاية". يتوقع أن يكون الوصول إليها محدوداً لأفراد معينين ضمن الجامعة ويطلب منهم التعامل مع هذه البيانات بمسؤولية وسرية.	• تقارير حول تقييم البرامج أو تقييمات الأقسام التي تحلل الأداء والتي قد تؤثر على سمعة الجامعة. • تفاصيل حول المنح البحثية الجديدة أو التمويلات التي لم يتم الإعلان عنها بعد، والتي يمكن أن تعطي الجامعة ميزة تنافسية. • الدرجات الطلابية والسجلات الأكاديمية التي لم يتم إتاحتها علناً، والتي تحتوي على معلومات شخصية وأكاديمية حساسة. • مراسلات بين أعضاء الهيئة الإدارية تتضمن مناقشات حول تغييرات سياسات الجامعة أو قرارات مهمة تؤثر على العمليات الداخلية. • معلومات مفصلة حول الميزانيات، والتخطيط المالي، والتي يمكن أن تؤثر على العمليات التشغيلية والمالية للجامعة. • بيانات حول برامج التطوير التي لم يتم الإعلان عنها، والتي قد تؤثر على المسارات المهنية للمعنيين. كل هذه الأمثلة تتطلب مستوى عالٍ من الحماية لضمان عدم تسريب المعلومات الحساسة التي قد تؤثر سلباً على الجامعة إذا تم الكشف عنها دون تخطيط.
مقيد	منخفض	مستوى التصنيف "مقيد" يشير إلى البيانات التي تكون حساسة لكنها ليست بالدرجة العالية من الحساسية كما في المستويات "سري للغاية" أو "سري". الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها قد يؤدي إلى ضرر محدود قد يؤثر على العمليات الداخلية للجامعة أو على الخصوصية الشخصية، لكنه لا يصل إلى مستوى الضرر الجسيم الذي يتطلب مستويات التصنيف الأعلى.	• جداول العمل الخاصة بالموظفين، تقارير الحضور والغياب، ومعلومات الجدولة الدورية للمحاضرات والفعاليات الجامعية. • الاتصالات اليومية بين الأقسام والمراسلات التي لا تحتوي على معلومات استراتيجية، مثل الإشعارات الداخلية والتحديثات الإدارية. • تقارير المصروفات والميزانيات التشغيلية الصغيرة التي لا تحتوي على بيانات شديدة الحساسية.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
مقيّد	منخفض	هذه الفئة من البيانات تتطلب تدابير حماية لضمان الخصوصية والأمان، لكن متطلبات الحماية ليست بالغة كما في الفئات الأعلى من التصنيفات. يعتبر التعامل مع هذه البيانات جزءاً من إجراءات الحفاظ على السرية الروتينية في الجامعة.	- توزيعات الدرجات والتقييمات الفردية للطلاب التي يتم التعامل معها ضمن الأقسام الأكاديمية. - البيانات الأولية للأبحاث التي لا تحمل قيمة استراتيجية كبيرة أو لم تتم مراجعتها بعد لنشرها. كل هذه الأمثلة تعتبر حساسة وتتطلب مستوى من الحماية لضمان الخصوصية ومنع الإفصاح، ولكنها لا تصل إلى درجة الحماية الشديدة اللازمة للبيانات ذات التصنيف الأعلى. يتوجب تقييد وصول الأشخاص إلى هذه البيانات بناءً على الحاجة إلى المعرفة والدور الوظيفي.
عام	لا يوجد	مستوى التصنيف "عام" يطبق على البيانات التي لا تعتبر حساسة ويمكن مشاركتها مع العامة دون أن يسبب ذلك ضرراً للمصالح الجامعية أو الفردية. هذه البيانات عادةً ما تكون معلومات مصممة للنشر العام ولا تتطلب إجراءات حماية مشددة. هذه الفئة من البيانات لا تتطلب تدابير حماية خاصة وعادةً ما تكون متاحة بشكل عام على الموقع الإلكتروني للجامعة أو من خلال المنشورات والوسائل الإعلامية الأخرى.	- كتيبات الجامعة، الخرائط، معلومات عن المرافق والخدمات الطلابية التي تقدم للعموم. - تقويم الأحداث الجامعية الذي يعلن عن الندوات، الفعاليات والأنشطة. - الأوراق البحثية والمقالات التي تم نشرها وهي متاحة للعامة. - اللوائح الأكاديمية وسياسات الجامعة. - الخدمات التي تقدمها الجامعة للمجتمع، مثل العيادات الصحية أو المراكز الاستشارية. هذه الأمثلة تظهر نوعية المعلومات التي يمكن مشاركتها بحرية مع الجمهور العام دون الحاجة إلى تدابير أمنية مشددة، حيث إنها تصمم للنشر ولا تحمل مخاطر أمنية.

جدول 1 : مستويات تصنيف البيانات

الضابط الأول: البيانات غير المصنفة

- تعامل هذه البيانات على أنها "مقيدة" حتى يتم تصنيفها بشكل صحيح.
- يتم تصنيف البيانات التي لم يتم تصنيفها خلال فترة زمنية محددة بموجب خطة عمل يحددها مكتب إدارة البيانات.

الضابط الثاني: علامات الحماية

- تطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية بما فيها رسائل البريد الإلكتروني وفقاً لمستويات التصنيف.
- تتضمن علامات الحماية اسم التصنيف (عام، مقيد، سري، سري للغاية) وتاريخ انتهاء التصنيف، وتطبق على كل الصفحات، بما في ذلك الصفحة الأولى.

الضابط الثالث: حق الوصول

- يمنح الوصول (المنطقي والمادي) للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و "الحاجة إلى المعرفة".
- يمنع الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للمنسوب بالجامعة.

الضابط الرابع: 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.

الضابط الخامس: التخزين

- تكون البيانات المصنفة على أنها "سري للغاية" و "سري" و "مقيد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات تحت المراقبة بشكل دائم.
- تتم 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.

الضابط السادس: مشاركة البيانات

- يتم تحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتنثال لأنظمة وسياسات مشاركة البيانات وآلية تبادل البيانات.
- يتم التحقق من مستوى تصنيف البيانات قبل مشاركتها داخلياً أو خارجياً.

الضابط السابع: الاحتفاظ بالبيانات

- يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
- يتم تحديد فترة الاحتفاظ بالبيانات بناءً على ما تحدده المتطلبات الإدارية والتشغيلية والتعاقدية والتنظيمية والقانونية ذات العلاقة.
- يتم مراجعة الجدول الزمني لفترة الاحتفاظ بالبيانات بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

الضابط الثامن: التخلص من البيانات

- يتم التخلص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة رئيس قسم حوكمة وحماية البيانات.
- يتم التخلص من البيانات التي تم تصنيفها على أنها "سري للغاية" و "سري" 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.

الضابط التاسع: الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يوصي بها مكتب إدارة البيانات، ويتم 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.

الضابط العاشر: إلغاء التصنيف (رفع السرية)

- 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، يتم تحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
- يتم تحديد عوامل إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، وتسجيلها في سجل أصول البيانات.
- يتم دراسة طلب إلغاء التصنيف (رفع السرية) أو خفض مستويات التصنيف جيداً ليُكوّن فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.
- يتم الحصول على موافقة رئيس قسم حوكمة وحماية البيانات لإلغاء التصنيف أو خفضه.

يتولى مكتب إدارة البيانات بجامعة الملك عبدالعزيز مسؤولية الإشراف وتنفيذ كافة المهام المتعلقة بتصنيف البيانات، بما يضمن الالتزام بالسياسات والإجراءات المعتمدة من مكتب إدارة البيانات الوطنية. ويعمل المكتب على توجيه عمليات تصنيف البيانات والإشراف عليها لضمان توافقها مع اللوائح الوطنية ومتطلبات الجامعة، مع تحقيق التوازن بين حماية البيانات وإتاحتها بما يخدم أهداف الجامعة الأكاديمية والإدارية. كما يَنَاط بمدير مكتب إدارة البيانات مراجعة واعتماد مستويات التصنيف بما يتماشى مع أفضل الممارسات والمعايير الوطنية.

وتأتي أدوار ومسؤوليات المكتب فيما يلي:

- **إعداد السياسات والإجراءات:**
يتولى مكتب إدارة البيانات إعداد وتطوير سياسات وإجراءات تصنيف البيانات بما يتماشى مع المعايير الوطنية والدولية، ويعمل على تحديثها بشكل دوري لضمان مواكبتها للتطورات التقنية والقانونية.
- **تصنيف البيانات:**
يعمل المكتب على تصنيف البيانات التي تجمعها الجامعة أو الجهات التابعة لها وفقاً للسياسات والإجراءات المعتمدة في هذه السياسة.
- **مواظمة تصنيف البيانات:**
يتولى المكتب مسؤولية التأكد من تصنيف البيانات المجمعة من مصادر متعددة بدقة، مع ضمان حماية البيانات وفقاً لأعلى مستوى من السرية المطلوبة لأي جزء منها.
- **المراجعة والإشراف:**
يقوم المكتب بمراجعة عمليات تصنيف البيانات بشكل دوري للتأكد من الالتزام بالضوابط والمعايير المعتمدة، مع الإشراف على تنفيذ مهام التصنيف لجميع البيانات التي تتعامل معها الجامعة.
- **إدارة أصول البيانات:**
يتولى المكتب مسؤولية تسجيل جميع أصول البيانات الخاصة بالجامعة وتصنيفها وفق السياسات المعتمدة، مع التأكد من توثيق عمليات التصنيف في السجلات الرسمية.
- **معالجة الاستثناءات:**
يتولى المكتب مسؤولية مراجعة طلبات الاستثناء المتعلقة بتصنيف البيانات، مثل طلبات رفع أو خفض مستوى التصنيف، واتخاذ القرارات المناسبة بالتنسيق مع الجهات ذات العلاقة.
- **التنسيق مع الجهات الداخلية والخارجية:**
يعمل المكتب كجهة تنسيقية لضمان الالتزام بتصنيفات البيانات عند التعامل مع الجهات الخارجية أو الداخلية، وضمان التوافق مع الأنظمة الوطنية المتعلقة بتصنيف البيانات.

- **إعطاء الصلاحيات:**
يمنح المكتب الصلاحيات وفق مبدأ "الحاجة إلى المعرفة" بحسب تصنيف البيانات، بحيث يقتصر الوصول إلى البيانات على الأشخاص الذين تتطلب مهامهم الوظيفية ذلك.
- **مراجعة الصلاحيات:**
يقوم المكتب بمراجعة وتحديث صلاحيات الوصول بشكل دوري أو عند حدوث تغييرات في المناصب الوظيفية لضمان توافقها مع المتطلبات الوظيفية وتصنيف البيانات
- **التحكم في الوصول:**
التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقاً لمستويات تصنيف البيانات.
- **نشاط المراقبة:**
يقوم المكتب بمراقبة الأنشطة التي تتم على البيانات وتسجيلها لضمان توافق الاستخدام مع مستوى التصنيف الخاص بالبيانات المستخدمة، بما في ذلك بيانات المستخدم.
- **التعامل مع الانتهاكات:**
يتولى المكتب مسؤولية التحقيق مع البلاغات عن أي انتهاكات لسياسات تصنيف البيانات، واتخاذ الإجراءات التصحيحية لذلك بالتنسيق مع الإدارات المعنية.
- **متابعة التنفيذ والتطوير:**
يضمن المكتب متابعة تنفيذ السياسة بجميع مراحلها وتطوير أدوات تقنية داعمة تساهم في تحسين عمليات التصنيف وضمان دقتها.

الوثائق المرتبطة بسياسة تصنيف البيانات

ترتبط هذه السياسة بالوثائق التالية:

1. إجراء تصنيف البيانات.
2. سجل حصر البيانات.
3. سجل تصنيف البيانات.



مكتب إدارة البيانات

Data Management Office

DMO@kau.edu.sa