

جامعة الأميرة
نورة بنت عبد الرحمن



سياسة تصنيف البيانات

المملكة العربية السعودية

وزارة التعليم

جامعة الأميرة نورة بنت عبد الرحمن

اللجنة التوجيهية للحوكمة والالتزام وإدارة
المخاطر والطوارئ واستمرارية الأعمال



العام: ٢٠٢٥

رقم الإصدار: ١٠

جدول المحتويات

٤	١ المقدمة
٤	١,١ جدول التعريفات
٥	١,٢ الغرض
٥	١,٣ النطاق
٥	١,٤ المستند النظامي
٦	٢ بيان السياسة
٦	٢,١ المبادئ التوجيهية لتصنيف البيانات
٦	٢,٢ مستويات تصنيف البيانات
٨	٢,٣ ضوابط تصنيف البيانات
٩	٢,٤ خطوات تصنيف البيانات
١٢	٣ الأدوار والمسؤوليات
١٣	٤ المراجعة والتحديث
١٣	٥ الامتثال
١٣	٦ التواصل
١٣	٧ السياسات ذات العلاقة

معلومات الوثيقة:

اسم الوثيقة	سياسة تصنيف البيانات
نوع الوثيقة	سياسة
مالك الوثيقة	مكتب إدارة البيانات
تاريخ الإعداد	١٤٤٧/٠٤/٣٣ هـ
تصنيف الوثيقة	مقيّد - داخلي
النسخة رقم	١,٠

إصدارات الوثيقة:

تاريخ الإصدار	معد الوثيقة	الإصدار	التغييرات بالوثيقة
١٤٤٧/٨/٢٤ هـ	مكتب إدارة البيانات	١,٠	

مراجعات الوثيقة:

التاريخ	الجهة	ملاحظات
١٤٤٧/٦/١٩ هـ	إدارة الأمن السيبراني	
١٤٤٧ /٦ /١٢ هـ	الإدارة العامة للحكومة والمخاطر والالتزام	
١٤٤٧/٠٨/١٦ هـ	الإدارة القانونية	

اعتماد الوثيقة:

التاريخ	الجهة	الختم



١. المقدمة

تسعى جامعة الأميرة نورة بنت عبد الرحمن إلى حماية سرية وسلامة بياناتها، وضمان توافرها وتصنيفها وفق مبادئ ومستويات رئيسية لتصنيف البيانات، بالاستناد إلى المعايير والمتطلبات التنظيمية وذلك بناءً على الفقرة (أ) من البند (عاشراً) من قرار مجلس الوزراء رقم (٢٩٢) وتاريخ ١٤٤٧/٤/٢٧ هـ، الذي أسند إلى مكتب إدارة البيانات الوطنية مهمة وضع السياسات وآليات الحوكمة والمعايير والضوابط الخاصة بالبيانات والتحقق من مدى امتثال الجهات لها، بما يعزز النزاهة والشفافية، ويدعم التكامل مع الجهات الحكومية وتبادل البيانات بشكل آمن، ويسهم في تحسين جودة العمل وتحقيق الأهداف الاستراتيجية للجامعة.

١.١ جدول التعريفات

يقصد بالمصطلحات الواردة أدناه - أينما وردت في هذه السياسة - المعاني الموضحة أمام كل منها، ما لم يقتض سياق النص خلاف ذلك:

المصطلح	الوصف
الجامعة	جامعة الأميرة نورة بنت عبد الرحمن.
جهات الجامعة	الوحدات التنظيمية بالجامعة بما فيها مستشفى الملك عبد الله بن عبد العزيز الجامعي.
اللجنة التوجيهية لإدارة وحوكمة البيانات	هي لجنة عليا داخل الجامعة مكلفة بالإشراف الاستراتيجي على إدارة البيانات وحوكمتها.
المكتب	مكتب إدارة البيانات في جامعة الأميرة نورة بنت عبد الرحمن.
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	هي القدرة على الوصول المنطقي والمادي للبيانات والموارد التقنية التي تخص الجامعة لفرض استخدامها.
تصنيف البيانات	عملية تقسيم البيانات إلى مستويات محددة - تحدد آلية التعامل معها - بناءً على قياس شدة الأثر المترتب على الإفصاح غير المصرّح به نظاماً عن البيانات أو عن محتواها.
البيانات الوصفية	هي البيانات التي تصف وتفسر وتوضح سياق ومحتوى وهيكل البيانات وتساعد في إدارتها واستخدامها واسترجاعها بكفاءة بحيث تُمكن من فهم البيانات وتوحيدها ومشاركتها عبر مختلف الجهات.

المصطلح	الوصف
ممثّل بيانات الأعمال	الشخص المسؤول عن البيانات التي تجمعها الجامعة أو تحتفظ بها داخل إدارته، وعادةً ما يكون في مستوى إداري عالٍ.
مختص بيانات الأعمال	شخص يرشحه ممثّل بيانات الأعمال، ويكون خبيرًا بمجال معين ويتولى تطبيق سياسات ومعايير إدارة البيانات داخل الإدارة الخاصة به.
تقني وفني البيانات	شخص تقني مسؤول عن تنفيذ ضوابط حوكمة البيانات وتطبيقها على قواعد البيانات والأنظمة بالتعاون مع مختصي البيانات.

١.٢. الفرض

تهدف سياسة تصنيف البيانات إلى وضع معايير موحدة لتصنيف أصول البيانات وتحديد متطلبات التعامل معها وفق مستوى حساسيتها، بما يضمن تطبيق الضوابط الأمنية المناسبة وحماية البيانات من الاستخدام أو الوصول غير المصرح به. كما تدعم السياسة الامتثال لضوابط حوكمة البيانات وحماية البيانات الشخصية الصادرة عن الجهات التنظيمية، وتمكّن من إدارة البيانات ومشاركتها بشكل آمن يميز سرية البيانات وسلامتها وتوافرها داخل الجامعة.

١.٣. النطاق

تُطبّق أحكام هذه السياسة على كافة البيانات التي تتلقاها الجامعة أو تنتجها أو تتعامل معها مهما كان مصدر هذه البيانات أو شكلها أو طبيعتها والتي تشمل السجلات الورقية والاتصالات عبر وسائل التواصل والتطبيقات ورسائل البريد الإلكتروني والبيانات المُخزّنة على وسائط إلكترونية والتسجيلات الصوتية أو المرئية والخرائط والصور الفوتوغرافية والمخطوطات والوثائق المكتوبة بخط اليد، وأي شكل آخر من أشكال البيانات.

١.٤. المستند النظامي

- ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية - إصدار ١,٥ عام ٢٠٢١م.
- سياسات حوكمة البيانات الوطنية الصادرة من مكتب إدارة البيانات الوطنية - الإصدار الأول عام ٢٠٢٠: سياسة تصنيف البيانات.

٢. بيان السياسة

٢.١ المبادئ التوجيهية لتصنيف البيانات

٢.١.١ الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة في (المجال التنموي) ، ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية وتكون سرية للغاية ما لم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف والحماية.

٢.١.٢ الضرورة والتناسب

تُصنّف البيانات وفقاً لمستوى طبيعتها وتأثيرها ومدى حساسيتها، مع الأخذ بعين الاعتبار التوازن بين قيمتها ودرجة سريتها.

٢.١.٣ التصنيف في الوقت المناسب

تُصنّف البيانات عند إنشائها أو حين تلقيها من جهات أخرى، ويُنفذ ذلك التصنيف خلال فترة زمنية محددة.

٢.١.٤ المستوى الأعلى من الحماية

يُعتمد المستوى الأعلى من التصنيف عندما يتضمن محتوى مجموعة متكاملة من البيانات ذات مستويات تصنيف مختلفة .

٢.١.٥ فصل المهام

يُفصل بين مهام ومسؤوليات منسوبي الجامعة المتعلقة بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها بما يضمن منع تداخل الاختصاصات وتفادي تشتيت المسؤوليات.

٢.١.٦ الحاجة إلى المعرفة

يُقَيّد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة ولأقل عدد ممكن من منسوبي الجامعة.

٢.١.٧ الحد الأدنى من الصلاحيات

تُقَيّد إدارة صلاحيات منسوبي الجامعة إلى الحد الأدنى من الصلاحيات اللازمة لأداء المهام والمسؤوليات المسندة إليهم.

٢.٢ مستويات تصنيف البيانات

تُصنّف البيانات إلى مستويات مختلفة وفقاً لدرجة تأثيرها المحتمل على المصلحة الوطنية أو أنشطة الجهات أو مصالح الأفراد أو البيئة والموارد الطبيعية. ويُحدّد مستوى الأثر استناداً إلى مجموعة من المعايير، من أبرزها:

- حجم الأثر ونطاقه (وطني، إقليمي، على عدة جهات، جهة واحدة، أفراد متعددين).

- مدى خطورة الأثر وصعوبة التحكم في الضرر.

- الفترة الزمنية اللازمة لمعالجة الأضرار وإصلاحها بعد وقوعها.

وفيما يلي عرض للمستويات الرئيسية لتصنيف البيانات بما يتناسب مع مستوى الأثر:

٢,٢,١. سري للغاية: درجة الأثر (عالي)

يؤدي الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها إلى تأثيرات بالغة الخطورة وغير قابلة للإصلاح على المصلحة الوطنية أو أنشطة الجهات وأدائها أو سلامة الأفراد على نطاق واسع، أو البيئة والموارد الطبيعية ويشمل ذلك:

- 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.
- المعلومات السياسية الرسمية المتعلقة بالعلاقات الدولية والاتفاقيات أو المعاهدات وكل ما يتعلق بها من مباحثات ودراسات وأعمال تحضيرية.
- المعلومات المتعلقة بآليات ومفاتيح التشفير المستخدمة للبنى التحتية الوطنية.

٢,٢,٢. سري: درجة الأثر (متوسط)

تُصنّف البيانات على أنها "سري" إذا كان الوصول إليها غير مصرّح به ويؤدي إلى تأثير أو ضرر جسيم على المصالح الوطنية أو أنشطة الجهات أو التأثير على حياة مجموعة أفراد أو الضرر على المدى الطويل للموارد البيئية. ويشمل ذلك:

- تهديد محتمل أو فعلي للأنظمة الرقمية الحساسة داخل الجامعة.
- التسبب في أذى جسيم أو إصابة تؤثر على حياة مجموعة من الأفراد.
- التسبب في ضرر على المدى الطويل للموارد البيئية أو الطبيعية.

٢,٢,٣. مقيد: درجة الأثر (منخفض)

تُصنّف البيانات على أنها "مقيد" إذا كان الوصول إليها غير مصرّح به ويمكن أن يؤثر على الأفراد أو الجهات ضمن نطاق محدود فقط. ويشمل ذلك:

- تأثير على منسوبي الجامعة ضمن نطاق ضيق أو محدود في نطاق المصالح الشخصية أو المالية.
- فقدان البيانات أو تسريبها قد يؤثر على العمليات الداخلية في الجامعة.
- بيانات مفصلة للمعاملات الفردية للعاملين بالجامعة.
- نتائج الأبحاث والدراسات العملية قبل نشرها.
- معلومات متعلقة بالتعيينات والقرارات الإدارية المعنية داخل الجامعة.
- معلومات الملف الصحي للأفراد داخل الجامعة.
- معلومات تحديد الهوية مثل الاسم والعنوان وأرقام الهوية الوطنية وأرقام الهواتف وأرقام الحسابات والتراخيص وبيانات السمات الحيوية للطالبات ومنسوبي الجامعة.
- معلومات رواتب منسوبي الجامعة.
- سياسات وإجراءات الجامعة المعتمدة.

كما يمكن تصنيف البيانات المقيّدة إلى مستويات فرعية بناءً على نطاق الأثر على النحو الآتي:

- مقيّد مستوى (أ): لا يمكن مشاركة البيانات خارج الجامعة بدون موافقة مسبقة من صاحب الصلاحية.
- مقيّد مستوى (ب): لا يمكن مشاركة البيانات خارج الوحدة التنظيمية العامة بدون موافقة مسبقة من صاحب الصلاحية.
- مقيّد مستوى (ج): لا يمكن مشاركة البيانات خارج الوحدة التنظيمية الداخلية بدون موافقة مسبقة من صاحب الصلاحية.

٢,٢,٤. عام: درجة الأثر (لا يوجد)

- لا يؤدي الوصول غير المصرّح به إلى هذه البيانات أو الإفصاح عنها إلى أي من التأثيرات المذكورة أعلاه ولا يؤثر على المصلحة الوطنية أو أنشطة الجامعة أو مصالح الأفراد، أو الموارد البيئية ويشمل ذلك:
- توجهات استراتيجية معلنّة تخص الجامعة.
- سياسات وإجراءات معلنّة تخص الجامعة.
- إعلانات وظيفية أو إعلانات عامة مرتبطة بالجامعة.
- أي معلومات متاحة علنًا على مواقع الجامعة.

٢,٣. ضوابط تصنيف البيانات

تتولى جهات الجامعة المختلفة بالتعاون مع مكتب إدارة البيانات وإدارة الأمن السيبراني وإدارة تقنية المعلومات والاتصالات عملية تحديد مستويات تصنيف البيانات وتطبيق الضوابط الأمنية المناسبة لضمان حمايتها من أي اختراق أو تسريب.

٢,٣,١. علامات الحماية

يتم تطبيق علامات الحماية الواردة في ضوابط ومواصفات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني على الوثائق الورقية والإلكترونية (بما في ذلك رسائل البريد الإلكتروني) وفقًا لكل مستوى من مستويات التصنيف.

٢,٣,٢. الوصول

- يتم منح الوصول – المنطقي والمادي – للبيانات بناءً على مبدأ " الحد الأدنى من الصلاحيات " و " الحاجة إلى المعرفة " كما يجب على الجهة المعنية في الجامعة الإشراف على منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بالجامعة.
- تطبيق ضوابط الوصول عن بُعد للبيانات وفقًا لضوابط الأمن السيبراني.

٢,٣,٣. الاستخدام

يتم استخدام البيانات المصنفة وفقًا لمتطلبات المستويات الواردة في ضوابط ومواصفات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني. ويشمل ذلك على سبيل المثال لا الحصر ضرورة استخدام بيانات سري للغاية فقط في مواقع محددة، سواءً ماديًا (مثل المكاتب) أو افتراضيًا (مثل استخدام التشفير أو التطبيقات الخاصة).

٢,٤ خطوات تصنيف البيانات

٢,٤,١. حصر وتحديد جميع البيانات التي تمتلكها الجامعة، مرورًا بتقييمها وتحديد البيانات منخفضة الأثر، وانتهاءً بتطبيق ضوابط الحماية المناسبة وفقًا لمستوى التصنيف.

٢,٤,٢. يتولى مختص بيانات الأعمال مسؤولية تنفيذ عملية التصنيف في كل إدارة داخل الجامعة.

٢,٤,٣. مراجعة ترتيب أولويات البيانات المراد تصنيفها بناءً على أهميتها وحساسيتها وتأثيرها على الأعمال.

٢,٤,٤. في حال عدم تصنيف البيانات عند إنشائها أو تلقيها وفقًا لمعايير التصنيف، تُعامل هذه البيانات على أنها «مقيّدة» حتى تُصنّف على نحو صحيح من قبل الجهة المسؤولة. كما يجب تصنيف البيانات التي لم تُصنّف وقت إصدار هذه السياسة خلال فترة زمنية محددة بموجب خطة عمل يحددها مكتب إدارة البيانات بالجامعة وتُعتمد من قبل الإدارة العليا.

٢,٤,٥. تنفيذ إجراء عملية تقييم الأثر لمجموعات البيانات المراد تصنيفها من خلال تطبيق مبدأ الأصل في البيانات الإتاحة مالم تقتض طبيعتها أو تقتض حساسيتها مستويات أعلى من التصنيف والحماية.

٢,٤,٦. 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 مختص بيانات الأعمال في هذا الصدد، دراسة ما إذا كان الإفصاح عن هذه البيانات يتعارض مع أنظمة المملكة العربية السعودية على سبيل المثال لا الحصر نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية، وإذا كان الإفصاح عن البيانات مخالفًا للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيّدة".

٢,٤,٧. توفير البيانات الوصفية للمضي في تقييم الأثر ومن ثم تصنيف جميع البيانات ونشر درجات التصنيف الممنوحة لمجموعة البيانات في دليل البيانات الشامل.

٢,٤,٨. تُصنّف جميع البيانات التي تمتلكها الجامعة وفقًا لمعايير التصنيف المعتمدة، مع التحقق من دقة مستويات التصنيف من قبل مكتب إدارة البيانات. تُعتمد نتائج التصنيف من ممثلي البيانات ثم تُوجّه إلى الجهات المعنية لتطبيق الضوابط والإجراءات المناسبة بناءً على مستوى التصنيف المحدد.

٢,٤,٩. يتولى مكتب إدارة البيانات بالاشتراك مع ممثلي البيانات مراجعة جميع البيانات المصنفة للتأكد من أن مستوى التصنيف المحدد من قبل مختص البيانات هو الأنسب، ويجب مراجعتها خلال شهر واحد من التصنيف الأولي.

٢,٤,١٠. ينشئ مكتب إدارة البيانات بالجامعة سجلًا لمؤشرات الأداء الرئيسية لتصنيف البيانات لقياس التقدم المتحقق في خطة تصنيف البيانات.

٢,٤,١١. ينشئ مكتب إدارة البيانات بالجامعة سجلًا للاحتفاظ بمجموعات البيانات المصنفة حسب متطلبات مكتب إدارة البيانات الوطنية.

٢,٤,١٢. التخزين

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

٢,٤,١٣. الاحتفاظ بالبيانات

- يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات كما ورد في سياسة التخزين والاستبقاء داخل الجامعة.
- يتم تحديد فترة الاحتفاظ بناء على ما تحدده المتطلبات التجارية والتعاقدية والتنظيمية والقانونية ذات العلاقة.
- يتم مراجعة الجدول الزمني لفترة الاحتفاظ بصورة دورية - سنوياً أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

٢,٤,١٤. الأرشفة

- يتم أرشفة البيانات في مواقع تخزين آمنة وفقاً للطريقة التي يُوصي بها ممثل بيانات الأعمال.
- يتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
- يتم حماية البيانات المؤرشفة التي ضُفّت على أنها "سري للغاية" و"سري" باستخدام أحد طرق التشفير المعتمدة من قبل إدارة الأمن السيبراني.
- يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرّح لهم بالوصول إلى البيانات المؤرشفة.
- يتم الالتزام بما ورد بسياسة المحتوى والوثائق داخل الجامعة فيما يخص عملية أرشفة البيانات.

٢,٤,١٥. التخلص من البيانات

- يتم التخلص من جميع البيانات بطريقة آمنة وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
- يتم التخلص من البيانات التي ضُفّت على أنها "سرية للغاية" و"سري" والتي يجري 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 جرى التخلص منها.
- يتم الالتزام بما ورد بسياسة التخزين والاستبقاء بالجامعة فيما يخص عملية التخلص من البيانات.

٢,٤,١٦. مشاركة البيانات

- على الجامعة إنشاء وسائل آمنة مناسبة لتبادل البيانات المادية والرقمية للحد من المخاطر وضمان الامتثال لأنظمة مشاركة البيانات.
- يجب اتباع آلية تبادل البيانات المذكورة في سياسة مشاركة البيانات داخل الجامعة سواء باستخدام الوسائل الحالية المعتمدة في الجامعة أو عبر إنشاء اتصال مباشر جديد أو استخدام وسائط تخزين قابلة للإزالة أو الشبكات اللاسلكية أو الوصول عن بعد أو الشبكات الافتراضية الخاصة، وغيرها من الوسائل المناسبة.

٢,٤,١٧. المراجعة الدورية للبيانات المصنفة

يجب على ممثلي بيانات الأعمال، بالتعاون مع مكتب إدارة البيانات، إجراء مراجعة دورية لتصنيف البيانات التي تقع ضمن نطاق مسؤولياتهم للتأكد من أن مستوى التصنيف المحدد لا يزال مناسبًا، بحيث تكون دورية المراجعة كالاتي:

- سري للغاية: كل ٣ أشهر من تاريخ التصنيف.
- سري: كل ٦ أشهر من تاريخ التصنيف.
- مقيد: كل ١٢ شهرًا من تاريخ التصنيف.
- عام: كل ١٢ شهرًا من تاريخ التصنيف.

٢,٤,١٨. إلغاء التصنيف

- 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.
- إذا جرى تصنيف البيانات على نحو خاطئ، يجب على مستخدم البيانات إشعار ممثل بيانات الأعمال لتحديد مدى الحاجة إلى إعادة تصنيفها تصنيفًا مناسبًا ونظاميًا.
- يجب تحديد عوامل تساعد على إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، تتضمن هذه العوامل ما يلي:
- فترة زمنية محددة بعد إنشاء البيانات أو تلقيها (مثال: عامين بعد الإنشاء).
- فترة زمنية محددة بعد اتخاذ آخر إجراء على البيانات (مثال: ستة أشهر من تاريخ آخر استخدام).
- بعد انقضاء تاريخ محدد (مثال: من المقرر مراجعتها بداية كل عام ميلادي).
- بعد ظروف أو أحداث معينة تؤثر تأثيرًا مباشرًا على البيانات.
- يتطلب إلغاء التصنيف سواء رفع السرية أو خفض مستويات التصنيف، بعيدًا عن العوامل المساعدة على إلغاء التصنيف الواضحة تمامًا، فهمًا سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

٣. الأدوار والمسؤوليات

الدور	المسؤولية
اللجنة التوجيهية لإدارة وحوكمة البيانات	- التوصية باعتماد السياسة.
اللجنة التوجيهية للحوكمة والالتزام وإدارة المخاطر والطوارئ واستمرارية الأعمال	- اعتماد السياسة.
مكتب إدارة البيانات	- الإشراف على تنفيذ السياسة عبر مختلف جهات الجامعة. - دعم برنامج تصنيف البيانات وضمان مواعيدته مع استراتيجيات الجامعة ومتطلبات الجهات التنظيمية. - مراقبة الامتثال على مستوى جهات الجامعة لعملية تصنيف البيانات ومدى فاعليتها. - الإشراف على منع حق الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للعاملين بالجامعة.
إدارة الأمن السبراني	- الموازنة مع السياسات والضوابط الصادرة عن الهيئة الوطنية للأمن السبراني ومتابعة تنفيذ الضوابط فيما يخص البيانات المصنفة والإشراف على تلك الضوابط ومراقبتها.
إدارة تقنية المعلومات والاتصالات	- ضمان توفير ودعم البنية التحتية التقنية اللازمة لتطبيق ضوابط تصنيف البيانات والتحكم في الوصول إليها.
ممثّل بيانات الأعمال	- تحمل المسؤولية الكاملة عن البيانات داخل القطاع والإشراف على عملية تصنيفها وفق مبادئ وضوابط السياسة، بما يشمل مراجعة ترتيب الأولويات واعتماد التصنيف. - ضمان تصنيف كل مجموعة بيانات بمستوى الأمان الأكثر حماية وتوجيه مختص بيانات الأعمال في تنفيذ التصنيف بما يتوافق مع مكتب إدارة البيانات.
مختص بيانات الأعمال	- ضمان تصنيف مجموعات البيانات بشكل صحيح وتطبيق ضوابط التحكم في الوصول وفق مستويات التصنيف المعتمدة.

٤. المراجعة والتحديث

- ٤.١. يجب مراجعة هذه السياسة من قبل المكتب دوريًا، أو عند وجود متطلبات جديدة تستوجب التعديل.
- ٤.٢. يجب مشاركة التحديثات المقترحة مع الجهات المعنية داخل الجامعة لأغراض المراجعة.
- ٤.٣. يجب تنفيذ التعديلات من قبل المكتب ورفع النسخة النهائية إلى اللجنة التوجيهية للحكومة والالتزام وإدارة المخاطر والطوارئ واستمرارية الأعمال لاعتمادها.

٥. الامتثال

- ٥.١. يجب على جميع جهات الجامعة ضمان تطبيق هذه السياسة والالتزام بنودها حيث يقوم المكتب بمراجعة دورية أو عشوائية للتحقق من الامتثال لها.
- ٥.٢. عند مراجعة حالات عدم الامتثال، يتبع المكتب منهجية تدريجية لتحليل سبب عدم الامتثال ومدى الآثار والمخاطر المترتبة على ذلك، حسب الإجراءات التنظيمية المتبعة في مكتب إدارة البيانات.

٦. التواصل

في حال وجود أي استفسارات يرجى التواصل مع مكتب إدارة البيانات في جامعة الأميرة نورة بنت عبد الرحمن - بريد إلكتروني: DMO@pnu.edu.sa.

٧. السياسات ذات العلاقة

- ٧.١. سياسة حماية البيانات الشخصية.
- ٧.٢. سياسة مشاركة البيانات.
- ٧.٣. سياسة حرية المعلومات.
- ٧.٤. سياسة البيانات المفتوحة.
- ٧.٥. سياسة تخزين البيانات.

انتهى



