جامعة الملك سعود
King Saud University

مكتب إدارة البيانات
data management office

سياسة تصنيف البيانات

إعداد : مكتب إدارة البيانات

٢٠٢٢م

الإصدار الثاني


بسم الله الرحمن الرحيم


1957

معلومات الوثيقة

التصنيف	المعلومات
الوثيقة	سياسة تصنيف البيانات
الإصدار	1.1
المعرف	KSU-DMO-PL-001
الحالة	مُعتمدة
جهة الإعداد	مكتب إدارة البيانات بجامعة الملك سعود
المراجع (المراجعون)	رئيس مكتب إدارة البيانات بجامعة الملك سعود
المعتمد لها	معالي رئيس جامعة الملك سعود التوقيع
تاريخ الاعتماد	٢٣ / ١٠ / ٢٠٢٢م
تاريخ النفاذ	٢٣ / ١٠ / ٢٠٢٢م إلى ٣١ / ١٢ / ٢٠٢٤م
التصنيف	عام
مالك الوثيقة	مكتب إدارة البيانات بجامعة الملك سعود

نسـخ الوثـيـقـة

الإصدار	التاريخ	المساهم	ملاحظات
1.0	مارس، ٢٠٢٢	مكتب إدارة البيانات	تطوير الإصدار الأول من السياسة
1.1	أكتوبر، ٢٠٢٢	مكتب إدارة البيانات	مراجعة الإصدار الأول من السياسة بناءً على الملاحظات الواردة من جهات الجامعة

فهرس المحتويات

١. التعريفات

سعيًا لتطبيق هذه السياسة، تم تحديد معاني الكلمات والمصطلحات الرئيسة الواردة فيها، وتعني أينما وردت المعاني الموضحة أمامها، ما لم يقتضِ سياق النص خلاف ذلك، وهي:

الجامعة:

جامعة الملك سعود.

الامتثال:

تطبيق بنود هذه السياسة وضمان المراقبة الدورية لذلك.

الوصول إلى البيانات:

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

سريّة البيانات:

الحفاظ على القيود المصرّح بها للوصول إلى البيانات أو الإفصاح عنها.

البيانات الحساسة:

البيانات التي يؤدي فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنية أو أنشطة الجهات الحكومية أو خصوصية الأفراد وحماية حقوقهم.

مستخدم البيانات:

أي شخص يُمنح صلاحية الوصول إلى البيانات؛ لغرض الاطلاع عليها أو استخدامها أو تحديثها وفق المهام المصرح بها.

الضوابط الأمنية:

الأجهزة والإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ووسائل معالجتها والوصول إليها.

٢. الهدف

تهدف هذه السياسة إلى وضع متطلبات تصنيف البيانات بجامعة الملك سعود وفق أفضل الممارسات المحلية والدولية، كما تهدف – أيضًا – إلى الالتزام بالمتطلبات التشريعية الخاصة بها في وثيقتي «ضوابط إدارة البيانات وحوكمتها وحماية البيانات الشخصية (الإصدار: يناير ٢٠٢١م)"، و" سياسات حوكمة البيانات الوطنية (الإصدار الثاني: مايو ٢٠٢١ م)" الصادرتين عن مكتب إدارة البيانات الوطنية.

٣. نطاق التطبيق

تسري هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك سعود – سواء أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها – وأيًا كان مصدرها أو طبيعتها، وتتعدد أشكال ومضامين هذه البيانات والمعلومات، التي منها على سبيل المثال لا الحصر: السجلات الورقية، ووثائق الاجتماعات، ورسائل البريد الإلكتروني، والبيانات والمعلومات المخزنة على الكمبيوتر، أو أشرطة الصوت، والفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال المعلومات المسجلة بشكل إلكتروني وغير إلكتروني والقابلة للنشر.

٤. الامتثال لهذه السياسة

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسة، وعلى جهات الجامعة ضمان تطبيق هذه السياسة داخل إداراتها، علمًا بأن الالتزام ببنود هذه السياسة يخضع لمراجعة دورية من مكتب إدارة البيانات بالجامعة، وأي عدم التزام أو انتهاك لها سيؤدي إلى المساءلة القانونية واتخاذ الإجراءات اللازمة حسب ما توصي عليه لجنة إدارة البيانات وحوكمتها بالجامعة.

٥. المبادئ الرئيسة لتصنيف البيانات

يتم تصنيف البيانات بجامعة الملك سعود وفق المبادئ الأساسية التالية:

المبدأ الأول: التصنيف في الوقت المناسب

تتم عملية تصنيف البيانات عند إنشائها أو استلامها على ألّا يتم تجاهل تصنيف البيانات لمدة تزيد عن ثلاثة أشهر أو قبل مشاركتها، عند استلام بيانات غير مصنفة من طرف آخر فيجب تصنيفها بالتنسيق مع الطرف المرسل أو اعتبارها «مُقيّدة» إذا تعذر التنسيق والتصنيف.

المبدأ الثاني: الضرورة والتناسب

يتم تصنيف البيانات حسب قيمتها وحساسيتها (أثَر تسريبها) مع الأخذ بعين الاعتبار الموازنة بين قيمتها وسريّتها.

المبدأ الثالث: الأصل في البيانات الإتاحة

الأصل في البيانات الإتاحة (أي: تصنف بأنها «عامة») ما لم تقتض طبيعتها وحساسيتها رفع مستوى تصنيفها من «عام» إلى تصنيف أعلى.

المبدأ الرابع: المستوى الأعلى من الحماية

عند احتواء البيانات على مجموعة من البيانات الفرعية ذات تصنيفات مختلفة، يتم اعتماد التصنيف الأعلى لضمان توفير الحماية اللازمة للبيانات الفرعية الحساسة.

المبدأ الخامس: فصل المهام

يجب الفصل بين مهام ومسؤوليات منسوبي الجامعة فيما يتعلق بحصر وبتصنيف البيانات وحمايتها واستخدامها بما يضمن عدم تداخل الاختصاص وتشتت المسؤولية.

المبدأ السادس: الحاجة إلى المعرفة

يتم الوصول للبيانات بناءً على مفهوم «الحاجة للمعرفة» بحيث تمنح الصلاحيات لمنسوبي الجامعة في الوصول للبيانات بقدر حاجة مهامهم الوظيفية لذلك.

المبدأ السابع: الحد الأدنى من الصلاحيات

يتم منح منسوبي الجامعة الحد الأدنى من الصلاحيات واللازمة لأداء المهام والمسؤوليات المناطة بهم.

المبدأ الثامن: تكامل تصنيف البيانات

لضمان توفير مستوى حماية متكامل للبيانات في جهات الجامعة كلها، يجب التأكد من تكامل تصنيف البيانات بالتعاون مع إدارة الأمن السيبراني بحيث لا تملك نفس البيانات تصنيفات مختلفة وفق هذه السياسة وسياسات الأمن السيبراني.

المبدأ التاسع: المراجعة الدورية

من الممكن أن تتغير حساسية وقيمة البيانات مع مرور الوقت؛ لذلك على جهات الجامعة ضمان مراجعة تصنيف البيانات سنويًا.

٦. ضوابط تصنيف البيانات

٦،١. البنود العامة

١. على جهات الجامعة تصنيف البيانات حال إنشائها أو تلقيها بناءً على سياسة وإجراء تصنيف البيانات.

٢. تعدُّ البيانات غير المصنفة «مُقيّدة» وتطبق الضوابط الأمنية المناسبة وفق لذلك حتى يتم وضع التصنيف المناسب لها.

٣. على جميع الجهات الجامعية وضع خطة لتصنيف البيانات التي تملكها بما فيها تلك البيانات التي أنشئت قبل اعتماد هذه السياسة، ويجب اعتماد الخطة من قبل المسؤول الأول بالجهة ومشاركة الخطة مع مكتب إدارة البيانات بالجامعة بعد اعتمادها.

٦،٢. بنود الحماية

وفيما يلي أهم الضوابط التي يمكن الاستفادة منها في عملية تصنيف البيانات، وربطها بما يصدر من إرشادات من الهيئة الوطنية للأمن السيبراني المتعلقة بهذا الخصوص:

١. **علامات الحماية:** يجب وضع علامة التصنيف – التي تحدد مستوى التصنيف – على الوثائق الورقية والإلكترونية.

٢. **الاستخدام:** وضع آلية مناسبة لاستخدام البيانات وفق مستويات تصنيفها.

٣. **الوصول:** على جهات الجامعة التحكم بالوصول المادي والمنطقي إلى البيانات المصنفة ومنح الوصول بناءً على مبدأي «الحد الأدنى من الصلاحيات» و «حق المعرفة» ويجب إنهاء حق الوصول بمجرد انتهاء العلاقة الوظيفية.

٤. **التخزين:** عدم ترك البيانات المصنفة على أنها «سريّة للغاية» أو «سريّة» أو «مقيّدة» أو الوسائط التقنية التي تعالجها أو تخزنها دون مراقبة أو تشفيرها وفقًا لمعيار التشفير الصادر من الهيئة الوطنية للأمن السيبراني.

٥. **مشاركة البيانات:** على منسوبي الجامعة والمتعاقدين معها التحقق من تصنيف البيانات قبل مشاركتها داخلياً أو خارجياً.

٦. **مشاركة البيانات والاحتفاظ بها والتخلص منها وأرشفتها:** على جهات الجامعة تحديد أنسب الطرق الآمنة لحفظ وأرشفة ومشاركة وتبادل وإتلاف البيانات المصنفة على أنها «سريّة للغاية» أو «سريّة» أو «مقيّدة».

٧. **إلغاء التصنيف (رفع السريّة):** على مستخدمي البيانات إبلاغ الجهة الجامعية المالكة للبيانات في حال اكتشافهم أن تصنيف البيانات غير مناسب، ويتطلب إلغاء التصنيف أو خفضه فهمًا دقيقًا لطبيعة البيانات وحساسيتها.

٧. مستويات تصنيف البيانات

تُصنف البيانات بحسب قيمتها وحساسيتها إلى أربعة مستويات: سرّي للغاية، سرّي، مقيّد، عام، وكما هو موضح في إجراء تصنيف البيانات (KSU-DMO-PR-001).

٨. الوثائق المرتبطة بسياسة تصنيف البيانات

ترتبط بهذه السياسة حاليًا الوثائق التالية:

١. إجراء تصنيف البيانات (KSU-DMO-PR-001).

٢. سجل حصر البيانات (KSU-DMO-R-002).

٣. سجل تصنيف البيانات (KSU-DMO-R-003).

قد يصدر مكتب إدارة البيانات بالجامعة – لاحقًا – إجراءات أو سجلات أو نماذج أخرى مرتبطة بهذه السياسة، ويتولى كذلك إعداد وتحديث واعتماد الإجراءات والسجلات المرتبطة بهذه السياسة.


King Saud University
جامعة الملك سعود