جامعة جدة
University of Jeddah

مكتب إدارة البيانات
Data Management Office

سياسة مشاركة البيانات بجامعة جدة

تصنيف الوثيقة: مقيد
رقم الإصدار 1.0
التاريخ: 8 / 12 / 2025
المرجع: ضوابط ومواصفات إدارة البيانات الوطنية وحماية البيانات الشخصية

تفاصيل الوثيقة

اسم الوثيقة	سياسة مشاركة البيانات بجامعة جدة		
المؤسسة	جامعة جدة		
مالك الوثيقة	مكتب إدارة البيانات		
رقم الاصدار	1.3		
تاريخ أحدث إصدار	8/12/2025	تاريخ المراجعة القادم	8/12/2026
تصنيف الوثيقة	مقيد		

ضبط أحدث إصدار

رقم الاصدار	التاريخ	تحرير	الدور	مراجعة	الدور	اعتماد	الدور
1.3	8/12/2025	د. نورة الغامدي	المشرف على مكتب إدارة البيانات	د. خلود الغامدي	مسؤول حوكمة البيانات	د. نورة الغامدي	المشرف على مكتب إدارة البيانات

سجل الإصدارات

رقم الإصدار	التاريخ	تحرير	التعديلات
1.3	8/12/2025	د. نورة الغامدي	• اضافة المصطلحات • تعديل الأدوار والمسؤوليات • اضافة السياسات المرتبطة • اضافة المراجع
1.2	14/7/2024	د. ماجدة وزان	تحديث السياسة وفقا لتعديلات الهيئة الوطنية للبيانات والذكاء الاصطناعي
1	17/11/2024	د. ماجدة وزان	انشاء النسخة الأولى

المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات مشاركة البيانات التي يتم انتاجها ومعالجتها بـجامعة جدة وذلك لتحقيق أحد أهم الأهداف الرئيسية لإدارة البيانات. تشارك جامعة جدة البيانات الرئيسية التي تنتجها مع الجهات الحكومية لتحقيق التكامل بين هذه الجهات، و يتم مشاركة البيانات لأغراض مشروعة مبنية على أساس نظامي أو احتياج عملي مبرر يهدف الى تحقيق مصلحة عامة دون الحاق أي ضرر بالمصالح الوطنية، أو أنشطة الجهات أو خصوصية الأفراد أو سلامة البيئة، ويستثنى من ذلك البيانات والجهات المستثناة بأوامر سامية.

تمت موائمة هذه السياسة مع ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية الصادرة من المكتب الوطني لإدارة البيانات والمتطلبات التنظيمية والتشريعية ذات العلاقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على مكتب إدارة البياناتمراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، ويجوز أيضا تحديثها فور حدوث اي تعديلات أو تغييرات تتعلق بالمتطلبات التشريعية والتنظيمية ذات العلاقة، ويتم تغيير رقم إصدار الوثيقة عند القيام بأي تعديل سواء كان جوهرياً أو ثانويا. وينبغي اعتماد هذه التحديثات أوالتعديلات من قبل اللجنة الاشرافيةلإدارة البيانات بجامعة جدة.

نطاق السياسة

01
تنطبق أحكام هذه السياسة على بيانات جامعة جدة، وتنظم عملية مشاركتها مع مقدم الطلب أياً كان شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ورسائل البريد الإلكتروني والبيانات المخزنة على الوسائط الإلكترونية أو أشرطة الصوت أو الفيديو أو الخرائط أو الصور الفوتوغرافية أو المخطوطات أو الوثائق المكتوبة بخط اليد، أو أي شكل آخر من أشكال البيانات المسجلة.

02
تستثنى من نطاق تطبيق أحكام هذه السياسة عمليات مشاركة البيانات في حال كان مقدم الطلب جهة حكومية وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية، أو تنفيذاً لاتفاقية دولية تكون المملكة طرفاً فيها.

03
يستثنى من نطاق تطبيق أحكام هذه السياسة في حال كان مقدم الطلب جهة حكومية وكان طلب مشاركة البيانات الغرض ممارسة مهام رقابية أو متابعة أداء الجهات الحكومية وفقاً لأنظمتها أو تنظيماتها،

على أن يتم الالتزام بما يأتي:

أ- توثيق طلب مشاركة البيانات في سجل خاص بذلك من قبل مكتب إدارة البيانات في جامعة جدة

ب- أن يكون مقدم الطلب مسؤولا عن طلب البيانات بالحد الأدنى اللازم لتحقيق الغرض من جمعها والمحافظة عليها بما لا يخل بالأحكام النظامية أو المتطلبات التنظيمية الأخرى ذوات العلاقة.

ج- أن تكون مشاركة البيانات بصورة آلية من خلال قناة التكامل الحكومية أو أي وسيلة آلية آمنة، وإن تعذر ذلك وكانت وسيلة المشاركة غير آلية فتتم مشاركة البيانات من خلال وسيلة آمنة وموثوقة، وفقاً لما يصدر من الجهات المختصة.

د- إتلاف البيانات التي تمت مشاركتها بعد انتهاء الغرض من الحصول عليها، مع مراعاة الأحكام النظامية والمتطلبات التنظيمية ذوات العلاقة.

المبادئ الرئيسية لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

على كل جهة مصـــدر مشـــاركة البيانات التي تصـــدرها وفقاً لأحكام هذه السياسة وذلك لتعزيز الاســـتفادة من هذه البيانات وتحقيق التكامل بين الجهات الحكومية.

المبدأ الثاني: مبدأ المرة الواحدة

قيام الجهات الحكومية بجمع البيانات - في سياق ممارسة اختصاصاتها المقررة نظاماً لمرة واحدة مع إمكانية مشـــــاركتها وإعادة اســـتخدامها بما لا يتعارض مع الأنظمة ذات العلاقة وذلك للحد من ازدواجيتها وتعارضـــها وتعدد مصـــادرها وضـــمان تكاملها وحداثتها وجودتها.

المبدأ الثالث: مشروعية الغرض

تتم مشـــاركة البيانات لأغراض مشـــروعة مبنية على أســـاس نظامي أو احتياج عملي مبرر دون إلحاق أي ضـــرر بالمصـــال الوطنية، أو أنشـــطة الجهات أو خصـــوصـــية الأفراد أو ســـلامة البيئة وحصـــر اســـتخدامها من قبل مقدم الطلب للأغراض المحددة في طلب مشـــاركة البيانات.

المبدأ الرابع: الاطلاع المصرح به

أن يكون لدى جميع أطراف عملية مشـاركة البيانات صـلاحية الاطلاع على هذه البيانات والحصـول عليها واسـتخدامها وذلك من خلال تحـديـد المخولين بـالاطلاع على هـذه البيـانـات بعد القيـام بـالإجراءات اللازمـة للتـأكـد من موثوقيتهم إن تطلـب الأمر ذلـك، حسب طبيعة ومستوى تصنيفها ودرجة حساسيتها وفقاً لسياسة تصنيف البيانات.

المبدأ الخامس: الشفافية

تتم إتـاحـة جميع المعلومـات الضرورية المتعلقـة بطلـب مشاركة البيـانـات لجميع أطراف عمليـة مشـــــاركـة البيـانـات، وذلـك من خلال إيضـــاح البيانات المطلوبة ومســـتويات تصـــنيفها - بحســـب ما تنص عليه ســـياســـة تصـــنيف البيانات والغرض من طلبها، وطرق حفظها، والضوابط المستخدمة لحمايتها وآلية إتلافها.

المبادئ الرئيسية لمشاركة البيانات

المبدأ السادس: المسؤولية المشتركة

أن يكون جميع أطراف عملية مشـاركة البيانات مسـؤولين مسـؤولية مشـتركة عن قرارات مشـاركة البيانات، وفقاً للأدوار والمسـؤوليات في اتفاقية مشاركة البيانات أو الضوابط المناسبة - بحسب الأحوال لضمان معالجتها وفقاً للأغراض المحددة.

المبدأ السابع: أمن البيانات

أن يقوم جميع أطراف عملية مشـــاركة البيانات بتطبيق الضـوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة وفقاً للمتطلبات التنظيمية ذوات العلاقة، ووفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني.

المبدأ الثامن: الاستخدام الأخلاقي

أن يقوم جميع أطراف عملية مشـــاركة البيانات إضـــافة إلى الالتزام بالمتطلبات التنظيمية ذوات العلاقة بتطبيق الممارســـات الأخلاقية لضمان استخدام البيانات في إطار من المسؤولية والعدالة والنزاهة والأمانة

القواعد العامة لمشاركة البيانات

- أن تكون الجامعة مسؤولة عن إعداد وتطبيق السياسات و الإجراءات المتعلقة بممارسة حق الوصول إلى المعلومات العامة أو الحصول عليها، ويكون المسؤول الأول بالجامعة مسؤول عن الموافقة عليها واعتمادها.

- أن تقوم الجامعة بإنشاء وحدة إدارية تكون مرتبطة بمكاتب إدارة البيانات في الجهات الحكومية التي تم تأسيسها بموجب الأمر السامي الكريم رقم 59766 وتاريخ 20/11/1439 هو يسند لها مسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالجامعة والمتعلقة بحق الوصول إلى المعلومات، على أن تتضمن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستوي لسياسة تصنيف البيانات في حال عدم وجودها وفقا لسياسة تصنيف البيانات - واستخدامها كمرجع رئيسي عند معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها.

- أن تقوم الجامعة بتحديد وتوفير الوسائل الممكنة نماذج طلب المعلومات العامة - سواء كانت نماذج ورقية أو إلكترونية والتي من خلالها يمكن للفرد طلب الاطلاع على المعلومات العامة أو الحصول عليها.

- أن تقوم الجامعة بالتحقق من هوية الأفراد قبل منحهم حق الاطلاع على المعلومات العامة أو الحصول عليها وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات العلاقة.

- أن تقوم الجامعة بوضع المعايير اللازمة لتحديد الرسوم المترتبة على معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها بناء على طبيعة البيانات وحجمها والجهد المبذول والوقت المستغرق عليها وفقا لوثيقة سياسة تحقيق الدخل من البيانات. أن تقوم الجامعة بتوثيق جميع سجلات طلبات الوصول إلى المعلومات أو الحصول عليها والقرارات المتخذة حيال هذه الطلبات، على أن يتم مراجعة هذه السجلات لمعالجة حالات سوء الاستخدام أو عدم الاستجابة.

القواعد العامة لمشاركة البيانات

مع مراعاة الخطوات اللازمة لإجراء عملية مشاركة البيانات الموضحة في البند (سادسا)، تتمثل القواعد العامة التي يجب على جامعة جدة اتباعها عند مشاركة البيانات فيما يأتي:

1. في حال كان مقدم الطلب جهة حكومية، وكانت البيانات مطلوبة بصورة آلية تتم عملية مشاركةالبيانات باستخدام قناة التكامل الحكومية.

2. في حال كانت مشاركة البيانات بين الجهات الحكومية بصورة آلية وتعذر استخدام قناة التكامل الحكومية أو كانت هناك أسباب مبررة لدى أطراف عملية مشاركة البيانات، فتقترح الأطراف وسيلة مشاركة آمنة ومناسبة ويتم أخذ موافقة المكتب عليها.

3. في حال تعذر استخدام أي من الوسائل المشار إليها في الفقرة (1) والفقرة (2) وكانت البيانات مطلوبة من خلال وسيلة غير آلية، يجب على أطراف عملية مشاركة البيانات القيام بمشاركة البيانات من خلال وسيلة آمنة وموثوقة، وفقاً لما يصدر من الجهات المختصة.

4. يكون سوق البيانات الوسيلة المعتمدة لطلبات مشاركة البيانات بين الجهات الحكومية وللجهات الحكومية - في حال عدم إمكانية الحصول على البيانات من خلال سوق البيانات تقديم الطلب إلى مكتب جامعة جدة المطلوبة منها مشاركة البيانات لنشر البيانات المطلوبة على قناة التكامل الحكومية وفقاً للآلية التي يحددها المكتب.

5. في حال كان مقدم الطلب جهة غير حكومية يتم تقديم طلب مشاركة البيانات إلى مكتب جامعة جدة المطلوبة منها مشاركة البيانات وفقاً للآلية التي يحددها المكتب.

6. يتم إرفاق البيانات الوصفية عند مشاركة البيانات، على أن يتم إيضاح مستويات تصنيف البيانات المطلوبة.

7. في حال كان مقدم الطلب جهة حكومية يتم تطبيق ضوابط مشاركة البيانات وفقاً لنموذج يتم إعداده من المكتب.

القواعد العامة لمشاركة البيانات

مع مراعاة الخطوات اللازمة لإجراء عملية مشاركة البيانات الموضحة في البند (سادسا)، تتمثل القواعد العامة التي يجب على جامعة جدة اتباعها عند مشاركة البيانات فيما يأتي:

8. في حال كانت البيانات المطلوبة بيانات لأغراض تشغيلية ولم تكن جامعة جدة المطلوبة منها مشاركة البيانات هي جامعة جدة المصدر أو جهة مفوضة ولم يتضمن الطلب موافقة جامعة جدة المصدر، تقوم جامعة جدة المطلوبة منها مشاركة البيانات بإشعار مقدم الطلب خلال (5) أيام عمل من تاريخ استلام الطلب بالحصول على موافقة جامعة جدة المصدر، وعلى جامعة جدة المصدر الرد على الطلب بالموافقة أو الرفض كلياً أو جزئياً على أن يكون الرفض مسبباً وذلك خلال مدة لا تزيد عن (10) أيام عمل من تاريخ طلب الموافقة.

9. في حال عدم رد جامعة جدة المصدر خلال المدة المحددة في الفقرة (8) من هذا البند فيعد ذلك رفضاً للطلب، ويمكن المقدم الطلب - بحسب الأحوال المشار لها في الفقرة (8) من هذا البند - الرفع للمكتب للنظر فيه وفق ما نصت عليه الفقرة (3) من البند (ثامنا) من هذه السياسة.

10. يمكن للجهة المطلوبة منها مشاركة البيانات القيام بمشاركةالبيانات دون الحصول على موافقة جامعة جدة المصدر في حال وجود تفويض بذلك، وفقاً لماورد في البند (رابعاً.)

11. على أطراف عملية المشاركة الالتزام بالأحكام المنظمة للمنافسة عند القيام بعملية مشاركة البيانات، وعدم الاتفاق على ما من شأنه الإخلال بالأحكام النظامية ذات الصلة.

12. مع مراعاة ما نصت عليه الفقرة (6) من البند (سادسا)، يتم توقيع اتفاقية مشاركة البيانات من قبل المسؤول الأول أو من يفوضه لدى جامعة جدة المطلوبة منها مشاركة البيانات في حال كانت البيانات المطلوبة مصنفة على مستوى سري أو سري للغاية، ويتم توقيعها من قبل مدير مكتب إدارة البيانات لدى جامعة جدة المطلوبة منها مشاركة البيانات عند مشاركة البيانات المصنفة على مستوى مقيد.

13. في حال كانت البيانات المطلوبة مشاركتهاالأغراض تحليلية، فيتم طلب البيانات من بنك البيانات الوطني بعد الحصول على موافقة جامعة جدة المصدر، وفي حال تعذر ذلك فيتم الحصول عليها من جامعة جدة المصدر مع مراعاة الأحكام الواردة في الفقرة (1) و (2) و (3) من هذا البند.

طلب التفويض بمشاركة البيانات

1. يمكن للجهة المطلوبة منها مشاركة البيانات القيام بعملية مشاركة البيانات بناء على تفويض من جامعة جدة المصدر، على أن يتضمن التفويض الآتي:

أ- مدة التفويض وآلية التمديد.

ب - نوع البيانات ومستوى تصنيفها.

ج - وسيلة المشاركة مع مراعاة الأحكام المنصوص عليها في البند (ثالثاً).

د - المسؤوليات والأدوار لضمان أمن وحماية البيانات عند مشاركتها مع مقدم الطلب.

هـ - آلية تسوية الخلافات الناشئة عن التفويض وأي بنود أخرى ترى جامعة جدة المفوضة للبيانات (مصدرة التفويض) إضافتها في التفويض.

2. يجوز للجهة المفوضة للبيانات (مصدرة التفويض متابعة التزام جامعة جدة المفوضة بالمتطلبات الواردة في التفويض وطلب سجلات طلبات المشاركة والبيانات التي تمت مشاركتها.

3. على جامعة جدة المفوضة اتخاذ الخطوات اللازمة لضمان حداثة البيانات قبل القيام بعملية مشاركة البيانات.

آلية تحديد ضوابط مشاركة البيانات

يجب على جميع أطراف عملية مشاركة البيانات تحديد الضوابط اللازمة لإدارة البيانات - التي سيتم مشاركتها وحمايتها بشكل مناسب، على النحو الآتي:

الأساس النظامي:

المبادئ ذات العلاقة (المبدأ الأول: تعزيز ثقافة المشاركة، المبدأ الثاني: مبدأ المرة الواحدة، المبدأ الثالث: مشروعية الغرض، المبدأ السادس: المسؤولية المشتركة، المبدأ الثامن: الاستخدام الأخلاقي).

أ- أن يتم إيضاح الأساس النظامي أو الاحتياج العملي المبرر لمشاركة البيانات، ومنها على سبيل المثال تنظيم جامعة جدة أو الأوامر والقرارات ذوات الصلة التي تسمح للجهة بالحصول على البيانات.

ب - أن تتم المحافظة على سرية البيانات وفقاً لمستوى تصنيفها وخصوصية أصحاب البيانات الشخصية وحماية حقوق الملكية الفكرية.

التفويض:

المبادئ ذات العلاقة (المبدأ الرابع: الاطلاع المصرح به، المبدأ السابع: أمن البيانات.)

أ- تحديد المخولين بطلب البيانات وتلقيها لدى أطراف عملية المشاركة وفقا لضوابط الاستخدام والوصول إلى البيانات الموضحة في سياسة تصنيف البيانات، على أن يتم تعيين أو تفويض الشخص المناسب - حسب المؤهلات والتدريب المطلوب لضمان التعامل مع البيانات بشكل مسؤول.

ب - يتم منب الصلاحيات بناءً على مبدأ الحاجة إلى المعرفة ومبدأ الحد الأدنى من الامتيازات بحسب ما هو منصوص عليه في سياسة تصنيف البيانات عند التعامل مع البيانات التي تمت مشاركتها.

نوع البيانات:

المبادئ ذات العلاقة: (المبدأ الأول: تعزيز ثقافةالمشاركة المبدأ الثاني: مبدأ المرةالواحدة، المبدأ الثالث: مشروعية الفرض المبدأ الخامس: الشفافية).

أ - أن يتم تحديد الحد الأدنى من البيانات المطلوبة لتحقيق الأغراض المحددة.

ب - أن يتم تحديد البيانات المطلوبة وصيغتها والمتطلبات المتعلقة بتعديلها أو تغييرها مثل صيغة البيانات دقة البيانات مستوى التفاصيل، هيكلة البيانات، نوع البيانات.

ج- أن يتم تحديد آلية يتفق عليها أطراف عملية المشاركة لتحديث البيانات التي تمت مشاركتها مسبقاً في حال الحاجة إلى ذلك.

آلية تحديد ضوابط مشاركة البيانات

يجب على جميع أطراف عملية مشاركة البيانات تحديد الضوابط اللازمة لإدارة البيانات - التي سيتم مشاركتها وحمايتها بشكل مناسب، على النحو الآتي:

المعالجة المسبقة للبيانات

المبادئ ذات العلاقة (المبدأ الثاني: مبدأ المرة الواحدة، المبدأ السابع: أمن البيانات).

أ- أن يتم تحديد ما إذا كان هناك حاجة إلى معالجة البيانات قبل مشاركتها، وفي حال الحاجة إلى ذلك يتم الاتفاق على أساليب المعالجة المطلوبة - على سبيل المثال: التجب وإخفاء الهوية والتجميع على ألا تتم معالجة البيانات بشكل يغير المحتوى.

ب- أن يتم تقييم جودة البيانات المطلوبة وصحتها وسلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها.

وسائل مشاركة البيانات

المبادئ ذات العلاقة (المبدأ السابع: أمن البيانات).

أ- أن يتم التحقق من أمن وموثوقية قنوات مشاركة البيانات في حال عدم إمكانية استخدام الوسائل المنصوص عليها في الفقرة (1) من البند (ثالثاً) للتقليل من المخاطر المحتملة، وفقاً للمتطلبات التنظيمية الصادرة عن الجهات ذوات الاختصاص.

ب- أن يتم الاتفاق على مدد الاحتفاظ وآلية إتلاف البيانات محل طلب مشاركة البيانات عند تحقيق الغرض من الحصول عليها مع مراعاة المتطلبات التنظيمية ذوات العلاقة.

استخدام البيانات والمحافظة عليها

المبادئ ذات العلاقة (المبدأ الثالث: مشروعية الغرض، المبدأ الخامس: الشفافية، المبدأ السابع: أمن البيانات المبدأ الثامن: الاستخدام الأخلاقي).

أ- أن يتم تحديد متطلبات حماية البيانات التي ستتم مشاركتها، وتطبيق الضوابط المحددة لحمايتها بعد مشاركتها وفقاً لمستوى تصنيفها.

ب- أن يتم فرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وجدت)، مثل قيود خاصة بالمعالجة، أو قيود مكانية أو زمانية، أو حقوق حصرية أو تجارية.

ج- أن يتم تحديد حقوق جامعة جدة المطلوبة منها مشاركة البيانات في عملية مشاركة البيانات بإجراء عمليات التدقيق والمراجعة، بالإضافة حقوقه اتجاه أي طرف ثالث مستفيد من البيانات.

د- أن يتم الاتفاق على إجراءات تسوية النزاعات.

هـ - أن يتم تحديد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الآلية المنظمة لذلك.

آلية تحديد ضوابط مشاركة البيانات

يجب على جميع أطراف عملية مشاركة البيانات تحديد الضوابط اللازمة لإدارة البيانات - التي سيتم مشاركتها وحمايتها بشكل مناسب، على النحو الآتي:

مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة

المبادئ ذات العلاقة المبدأ الثالث: مشروعية الغرض المبدأ السابع: أمن البيانات.

أ- أن يتم تحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.

ب- أن يتم تحديد عدد مرات مشاركة البيانات، والمتطلبات اللازمة للمراجعة، وإجراء التعديلات، والإجراءات التي سيتم اتخاذها عند انتهاء الاتفاقية(مثل إخفاء هوية أصحاب البيانات أو إلغاء الوصول إلى البيانات أو إتلافها.

ج- أن يتم تحديد الأطراف الذين يحق لهم إنهاء مشاركة البيانات قبل التاريخ المتفق عليه، والمستند النظامي، وفترة الإشعار المسموح بها.

آلية تحديد ضوابط مشاركة البيانات

يجب على جميع أطراف عملية مشاركة البيانات تحديد الضوابط اللازمة لإدارة البيانات - التي سيتم مشاركتها وحمايتها بشكل مناسب، على النحو الآتي:

أحكام المسؤولية

المبادئ ذات العلاقة المبدأ السادس المسؤولية المشتركة

أ- أن يتم الاتفاق على تحديد المسؤوليات في حال عدم الالتزام ببنود الاتفاقية، وغيرها من الالتزامات بين أطراف عملية مشاركة البيانات.

ب- أن يتم تحديد القواعد المتعلقة بأحكام المسؤولية والتعويض عند مشاركة بيانات خاطئة أو غير دقيقة، أو عند وجود مشاكل فنية أثناء عملية نقل البيانات، أو فقدان البيانات بشكل غير مقصود أو غير نظامي مما قد يتسبب في أضرار أخرى.

سادساً: الخطوات اللازمة لإجراء عملية مشاركة البيانات تتم معالجة طلبات مشاركة البيانات بحسب التسلسل الآتي:

1. مع مراعاة ما نصت عليه الفقرة رقم (4) و (5) من البند (ثالثاً) ، يقوم مقدم الطلب بإرسال طلب مشاركة البيانات إلى مكتب جامعة جدة المطلوبة منها مشاركة البيانات، على أن يتم إرسال الطلب عن طريق مكتب جامعة جدة في حال كان مقدم الطلب جهة حكومية.

2. قيام جامعة جدة المطلوبة منها مشاركة البيانات بالتحقق من مستوى تصنيف البيانات المطلوبة، وفي حال عدم تحديد مستوى التصنيف، يجب على مكتب جامعة جدة المطلوبة منها مشاركة البيانات تصنيف البيانات المطلوبة وفقاً لسياسة تصنيف البيانات.

3. قيام مكتب جامعة جدة المطلوبة منها مشاركة البيانات بتقييم الطلب وفقاً لما يلي:

أ- وجود غرض مشروع من مشاركة البيانات مبني على أساس نظامي أو احتياج عملي مبرر.

ب- اقتصار البيانات المطلوبة وفق الحد الأدنى اللازم لتحقيق الغرض من طلب المشاركة.

ج- موافقة جامعة جدة المصدر في حال كان طلب مشاركة البيانات مقدماً إلى جهة غير جامعة جدة المصدر أو جامعة جدة المفوضة.

4. لمكتب جامعة جدة المطلوبة منها مشاركة البيانات حال عدم استيفاء الطلب للمتطلبات المنصوص عليها في الفقرة (3) من هذا البند أن يرفض الطلب مع إيضاح مسببات الرفض وإتاحة الفرصة لمقدم الطلب لاستكمال المتطلبات وفقاً للفقرة (2) من الإطار الزمني لعملية مشاركة البيانات الواردة في البند (سابعاً).

5. عند استيفاء جميع متطلبات المشاركة يتم تحديد الضوابط المناسبة وفقا للبند (خامسا) وذلك لضمان الالتزام بمبادئ مشاركة البيانات وتحقيق الأهداف المحددة لكل منها.

6. يتم توقيع اتفاقية مشاركة البيانات في حال كان مقدم الطلب جهة غير حكومية، ويتم استيفاء الضوابط المشار إليها في الفقرة (2) من البند (ثامنا) في حال كان مقدم الطلب جهة حكومية.

7. عند استيفاء ما ورد في الفقرة (6) من هذا البند، تتم مشاركة البيانات المطلوبة مع مقدم الطلب وفقاً للمدد الزمنية المحددة في البند (سابعاً.)

8. لا تنطبق الأحكام الواردة في الفقرة (3) و (6) من هذا البند في حال كانت البيانات التي سيتم مشاركتها بيانات مصنفة على مستوى عام.

الإطار الزمني لعملية مشاركة البيانات

1. يقوم مكتب جامعة جدة المطلوبة منها مشـاركة البيانات بتقييم الطلب خلال فترة زمنية لا تتجاوز (10) أيام عمل من تاريخ اسـتلام الطلب واشعار مقدم الطلب بالقرار على أن يكون القرار مكتوبا و مستبا.

2. في حال رفض طلب المشاركة، فيحق لمقدم الطلب استكمال المتطلبات وإعادة تقديم الطلب، وعلى مكتب جامعة جدة المطلوبة منها مشاركة البيانات إعادة تقييم الطلب وإصدار قرارها خلال فترة زمنية لا تتجاوز (5) أيام عمل من تاريخ استلامه.

3. بعد الموافقة على عملية مشـــاركة البيانات، يقوم مكتب جامعة جدة باســـتكمال ما نصـــت عليه الفقرة (6) من البند (ســـادســـا) وذلك خلال (5) أيام عمل من تاريخ الموافقة، على أن تتم مشـــاركة البيانات المطلوبة مع مقدم الطلب خلال (10) أيام عمل من تاريخ الانتهاء من الإجراءات المنصوص عليها في الفقرة (6) من البند (سادساً).

4. في حال كانت معالجة الطلب المقدم تتطلب جهداً غير عادي من جامعة جدة المطلوبة منها مشاركة البيانات أو كانت طبيعة الطلب تقتضـي مدداً أطول من المنصـوص عليه في هذه السـياسـة، فيكون للجهة المطلوبة منها مشـاركة البيانات تحديد مدد إضـافية وإشـعار مقدم الطلب بهذه المدة مع بيان السبب.

5. في حال عدم رد جامعة جدة المطلوبة منها مشـــاركة البيانات خلال المدة المحددة المنصـــوص عليها في الفقرة رقم (1) من هذا البند، فيحق لمقدم الطلب تقديم إشـــعار خطي أو إلكتروني إلى مكتب جامعة جدة المطلوبة منها مشـــاركة البيانات، وعلى مكتب جامعة جدة المطلوبة منها مشـــاركة البيانات متابعة حالة الطلب ثم إشـــعار مقدم الطلب بمســـببات التأخر بالرد وذلك خلال فترة زمنية لا تتجاوز (5) أيام عمل، وفي حال عدم رد جامعة جدة المطلوبة منها مشـــاركة البيانات خلال هذه المدة فيكون لمقدم الطلب تقديم الإشـــعار إلى المكـتـب للنظر فيه وفق ما نصت عليه الفقرة (3) من البند (ثامنا) من هذه السياسة.

أدوار ومسؤوليات الأطراف المعنية في مشاركة البيانات

1. يلتزم أطراف عملية مشاركة البيانات بأمن وحماية البيانات واستخدامها وفقا للأغراض المحددة، بحسب ما نص عليه المبدأ (السابع من هذه السياسة، ويحق لمكتب جامعة جدة التي قامت بمشاركة البيانات مراجعة مدى الالتزام بشكل دوري وفقاً للآليات التي يصدرها المكتب.

2. يقوم المكتب بإعداد نماذج قياسية لكل من:
أ- طلب مشاركة البيانات
ب- اتفاقية مشاركة البيانات.
ج- الضوابط المشار إليها في الفقرة (7) من البند (ثالثاً).
د- نموذج التفويض.

3. في حال وجود خلاف بين أطراف عملية مشاركة البيانات يتعلق بتنفيذ أحكام السياسة، يتم اللجوء للمكتب لطلب بيان الرأي النظامي وفقاً للآلية التي يحددها المكتب.

4. وفي حال لم تتم معالجة الخلاف وفقاً للفقرة)3(من هذا البند، يقوم المكتب باستكمال الإجراءات النظامية.

5. تلتزم أطراف عملية المشاركة بالمتطلبات النظامية والمتطلبات الأخرى ذوات الصلة المتعلقة بالإشعار عن حوادث تسرب البيانات.

6. في حال تضمن الطلب مشاركة بيانات شخصية فيتم مراعاة أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية وأحوال الإفصاح الواردة في النظام.

7. على جامعة جدة الاحتفاظ بسجلات خاصة بطلبات مشاركة البيانات والوثائق المرتبطة بها ولمدة خمس سنوات من انتهاء طلب المشاركة.

8. يجب على مكتب جامعة جدة إعداد ونشر سياسة لمشاركة البيانات الخاصة بها وفقاً لهذه السياسة.

9. على جامعة جدة نشر بيانات التواصل المعتمدة لمكتب جامعة جدة (على سبيل المثال: البريد الإلكتروني الخاص بمكتب إدارة البيانات في جامعة جدة وذلك لتمكين تقديم طلبات المشاركة من خلالها.

10. على جامعة جدة اتخاذ الوسائل الفنية والإدارية والتنظيمية اللازمة لضمان سرعة الاستجابة لطلبات مشاركة البيانات للالتزام بالإطار الزمني الموضح في البند (سابعا)، على سبيل المثال إعداد أدلة إجرائية داخلية للاستجابة لطلبات مشاركة البيانات واتفاقيات مستوى الخدمة، ومصفوفة الصلاحيات داخل جامعة جدة.

11. يقوم المكتب بمتابعة الالتزام بأحكام هذه السياسة، وللمكتب الاستعانة بأي جهة خارجية المتابعة الالتزام وفق الآلية التي يحددها المكتب.

جامعة جدة
University of Jeddah

الأدوار والمسؤوليات

مالك السياسة: مدير مكتب إدارة البيانات.
مراجعة السياسة وتحديثها: مكتب إدارة البيانات.
تنفيذ السياسة وتطبيقها: كافة قطاعات الجامعة.
قياس الالتزام بالسياسة: مكتب إدارة البيانات.

التحديث والمراجعة

يجب على مكتب إدارة البيانات مراجعة السياسة سنويا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة جدة أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

- يجب على مدير مكتب إدارة البيانات التأكد من التزام جامعة جدة بهذه السياسة دوريا.
- يجب على جميع العاملين في جامعة جدة الالتزام بهذه السياسة.

جامعة جدة
University of Jeddah

مكتب إدارة البيانات
Data Management Office

سياسة التخزين والاستبقاء للبيانات بجامعة جدة

تصنيف الوثيقة: مقيد
رقم الإصدار 1.2
التاريخ: 8/12/2025
المرجع: ضوابط ومواصفات إدارة البيانات الوطنية وحماية البيانات الشخصية

تفاصيل الوثيقة

اسم الوثيقة	سياسة التخزين والاستبقاء بجامعة جدة		
المؤسسة	جامعة جدة		
مالك الوثيقة	مكتب إدارة البيانات		
رقم الاصدار	1.2		
تاريخ أحدث إصدار	8/12/2025	تاريخ المراجعة القادم	8/12/2026
تصنيف الوثيقة	مقيد		

ضبط أحدث إصدار

رقم الاصدار	التاريخ	تحرير	الدور	مراجعة	الدور	اعتماد	الدور
1.2	8/12/2025	د. نورة الغامدي	المشرف على مكتب إدارة البيانات	د. خلود الغامدي	مسؤول حوكمة البيانات	د. نورة الغامدي	المشرف على مكتب إدارة البيانات

سجل الإصدارات

رقم الإصدار	التاريخ	تحرير	التعديلات
1.2	8/12/2025	د. نورة الغامدي	• اضافة المصطلحات • اضافة المبادئ التوجيهية لسياسة التخزين والاستبقاء • اضافة قواعد التخزين لحماية البيانات في حالات الكوارث • اضافة فترات استبقاء البيانات ومستودعات التخزين • اضافة قواعد الاتلاف بناءا على نوع وتصنيف البيانات • اضافة الاجراءات المطلوبة في حال الفقدان الدائم للبيانات غير المقصود • اضافة الأدوار والمسؤوليات • اضافة السياسات المرتبطة • اضافة المراجع
1.0	17/11/2024	د. ماجدة الوزان	إنشاء النسخة الأولى من سياسة التخزين والاستبقاء للبيانات

المحتويات

المصطلحات

المصطلح	التعريف
الجامعة	جامعة جدة
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظّمة مثل الأرقام أو الحروف أو الصور الثابتة أو التسجيلات المرئية أو التسجيلات الصوتية أو الرموز التعبيرية
إدارة البيانات	عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين الجهات من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيمة والثمينة.
البيانات الحساسة /الحرجة	بيانات محورية تؤثر بشكل مباشر على التقارير الإدارية، أو المؤشرات، أو الالتزام التنظيمي، أو اتخاذ القرار.
البيانات الشخصية	كل بيان مهما كان مصدره أو شكله من شأنه ان يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفه مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال- لا الحصر الاسم، وارقام الهويات الشخصية، وارقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد، وغير ذلك من البيانات ذات الطابع الشخصي.
البيانات المهيكلة	بيانات مُنظمة في شكل جدول تخزن في (قواعد بيانات)، تتبع هيكلا ثابتًا ومحددًا بشكل مسبق.
البيانات غير المهيكلة	بيانات لا تتبع تنسيقاً أو هيكلا محدداً مسبقاً، مما يجعلها أصعب في البحث والتحليل التلقائي
قواعد البيانات	هي مجموعات منظمة من البيانات المخزنة إلكترونياً، تتيح الوصول السهل، والإدارة الفعالة، والتحديث، والاسترجاع.
النسخ الاحتياطي	النسخ الاحتياطي لقواعد البيانات هو عملية إنشاء نسخة طبق الأصل أو جزئية من البيانات والهيكل الخاص بقاعدة البيانات، وتخزينها في موقع منفصل وآمن.
تقني البيانات	هم المحترفون المسؤولون عن التنفيذ العملي والإداري اليومي لأنظمة البيانات وقواعد البيانات.

الهدف

الهدف من هذه السياسة هو تحديد متطلبات إدارة البيانات لتخزين واستبقاء البيانات خلال دورة حياة كافة البيانات المحفوظة الخاصة بـجامعة جدة لحمايتها امتثالا لضوابط ومواصفات إدارة البيانات وحوكمتها وحماية البيانات الشخصية.

تمت موائمة هذه السياسة مع ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية الصادرة من المكتب الوطني لإدارة البيانات والمتطلبات التنظيمية والتشريعية ذات العلاقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على مكتب إدارة البيانات مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، ويجوز أيضا تحديثها فور حدوث أي تعديلات أو تغييرات تتعلق بالمتطلبات التشريعية والتنظيمية ذات العلاقة، ويتم تغيير رقم إصدار الوثيقة عند القيام بأي تعديل سواء كان جوهرياً أو ثانويا. وينبغي اعتماد هذه التحديثات أو التعديلات من قبل اللجنة الاشرافية لإدارة البيانات بجامعة جدة

نطاق السياسة

تنطبق هذه السياسة على جميع كليات الجامعة، والإدارات، والمراكز البحثية، والوحدات الإدارية، وجميع أعضاء هيئة التدريس، والموظفين الإداريين، والطلاب، والمتعاقدين، والجهات الخارجية التي تتعامل مع بيانات الجامعة، كما تشمل جميع أنواع البيانات التي تمتلكها أو تديرها الجامعة أو تنتجها

المبادئ التوجيهية لسياسة التخزين والاستبقاء

المبدأ الأول: تصنيف البيانات

يجب أن تصنف جميع البيانات بحسب سياسة تصنيف البيانات حيث يحدد تصنيف البيانات مستويات الوصول، متطلبات التخزين، فترة الاستبقاء، وطريقة الاتلاف

المبدأ الثاني: تحديد فترات الاستبقاء

لابد من الالتزام بالأنظمة واللوائح الوطنية وأنظمة ولوائح جامعة جدة لتحديد فترة الاستبقاء، في حال عدم وجود لائحة معتمدة، تحدد فترة الاستبقاء بناءا على الحاجات التشغيلية.

المبدأ الثالث: التخزين الامن

يجب تخزين البيانات بدرجة امان تتناسب مع تصنيفها، سواء كانت الية التخزين الكترونية، مادية أو سحابية.

المبدأ الرابع: المراجعة المستمرة

يجب تحديد عمليات مراجعة دورية لدقة وملاءمة الية التخزين مع اهمية البيانات وحساسيتها

المبدأ الخامس: الاتلاف الامن

عند انتهاء فترة الاستبقاء، يجب إتلاف البيانات بشكل آمن ونهائي ودون إمكانية الاسترداد.

قواعد عامة لسياسة التخزين والاستبقاء

قواعد عامة

- يجب أن تلتزم جامعة جدة بالمتطلبات التشريعية والتنظيمية المتعلقة بحماية البيانات في المملكة العربية السعودية.
- يجب أن تحدد جامعة جدة وتحدث متطلبات إدارة دورة حياة كافة البيانات المحفوظة بشكل دوري.
- يجب على جامعة جدة ضمان إدارة دورة حياة كافة البيانات المحفوظة بكفاءة .
- يجب أن تراقب جامعة جدة وتبلغ عن أداء قواعد البيانات، وأن تضع وتلتزم بعمليات واضحة لتمكين موظفي الجامعة من الوصول إلى قواعد البيانات كلا بحسب صلاحيته، كما يجب أن تلتزم بإدارة مساحة التخزين لدى الجامعة.
- على جامعة جدة أن تضع وتتبع خطة للتعافي من الكوارث وعمليات للنسخ الاحتياطي للبيانات واستعادتها.
- على جامعة جدة أن تحدد مؤشرات الأداء الرئيسية لجمع إحصاءات ومعلومات عن استخدامات وعمليات تخزين البيانات لديها.

القواعد الاسترشادية لسياسة التخزين والاستبقاء

مراقبة قواعد البيانات

- على جامعة جدة أن تراقب وتبلغ عن أداء قواعد البيانات على أساس دوري، بحيث تشمل عملية المراقبة السعة ومقدار مساحة التخزين غير المستخدمة.
- كفاءة الاستعلامات شاملة فترة تنفيذ الاستعلامات وأخطاؤها.
- تتبع التغييرات، أي تعقب التغييرات المدخلة إلى قاعدة البيانات لإمكانية تصحيح الأخطاء عند الحاجة في جامعة جدة.

ضبط الوصول إلى قاعدة البيانات

- على جامعة جدة أن تحدد أدورا للتقنين المختصين وفقًا لضوابط مجال تصنيف البيانات
- على جامعة جدة أن تضع وتلتزم بعملية واضحة لمنح موظفيها صلاحية الوصول إلى قواعد البيانات، وعلى العملية أن تطبق نظاًما للوصول إلى قاعدة البيانات قائما على الاختصاصات.

تحديث نظام إدارة قواعد البيانات

- على جامعة جدة أن تعمل على تحديث أدوات إدارة قواعد البيانات إلى آخر نسخة صادرة من المطور، أو عليها أن تضع خطة للتحديث

القواعد الاسترشادية لسياسة التخزين والاستبقاء

إدارة ضبط اعدادات مخزن البيانات

على الجامعة أن تضع وتلتزم بعملية واضحة لإدارة ضبط اعدادات مخزن البيانات لديها. وعلى العملية أن تشمل الخطوات التالية:

- تحديد اعدادات الضبط: تحديد وتوثيق الصفات المحددة لضبط وتهيئة نظام قواعد البيانات خصائص التحكم في تغيير اعدادات الضبط ـ للتمكين من اجراء التغييرات الخاصة لقواعد البيانات
- خصائص تتبع ضبط الإعدادات: متابعة التغييرات المنفذة في الإعدادات
- تدقيق اعدادات الضبط: ضمان اتساق اعدادات الضبط لقاعدة البيانات مع الإعدادات الصحيحة الموثقة

اتفاقيات مستوى الخدمة

- على جامعة جدة أن تضع وتنفذ اتفاقيات مستوى الخدمة الخاصة بأداء قواعد البيانات حيث تحدد متطلبات الجهة لأداء قواعد البيانات، وتوفر البيانات، واستعادتها. وعلى اتفاقيات مستوى الخدمة الخاصة بأداء قواعد البيانات لدى الجهة أن تشمل ما يلي :
  - الإطار الزمني لإتاحة قاعدة البيانات للمستخدمين.
  - أقصى زمن مسموح به لإنجاز العمليات الالكترونية لتطبيق معين
  - إجراءات التصعيد الواجب اتخاذها عند مخالفة اتفاقية مستوى الخدمة

النسخ الاحتياطي للبيانات واسترجاعها

- على جامعة جدة أن تضع وتتبع عملية واضحة للنسخ الاحتياطي للبيانات واسترجاعها، وتشمل ما يلي ولكن لا تقتصر عليه:
  - تحديد تواتر النسخ الاحتياطي لكل نظام معلومات، نطاق النسخ الاحتياطي لكل نظام معلومات، ويشمل نطاق البيانات ونطاق سجل معاملات قاعدة البيانات، موقع الملفات الاحتياطية، ويشمل وسيطة التخزين، والموقع المادي لمخزن البيانات.
  - التحقق الدوري من اكتمال النسخ الاحتياطي باستخدام نسخ النظام غير المستخدمة في بيئات الإنتاج

القواعد الاسترشادية لسياسة التخزين والاستبقاء

على جامعة جدة أن تضع خطة للتعافي من الكوارث وتشمل ما يلي (لا للحصر:)

التعافي من الكوارث

- قائمة مرتبة حسب الأولوية لتحدد ترتيب استرجاع أنظمة المعلومات.
- تخصيص الأدوار المسؤولة عن التعامل مع حالات الاستجابة للحوادث.
- تحديد الإجراءات الواجب اتخاذها لتقليل الأضرار وتخفيف عواقب الحوادث على العمليات الحيوية للجامعة.
- تحديد أهداف خطة التعافي وأقصى فترة مستهدفة يمكن فقد البيانات خلالها دون إحداث ضرر للأعمال لكل نظام معلومات مذكور في الخطة.

ضبط الوصول إلى بيانات الإنتاج

على جامعة جدة أن تضع وتلتزم بعملية واضحة لتطبيق تغييرات قاعدة البيانات في بيئة الإنتاج. وعلى العملية أن تشمل الخطوات التالية، ولكن لا تقتصر عليها:

- تحديد الإجراءات الواجب اتخاذها لتنفيذ التغيرات في قواعد البيانات.
- تحديد الإجراءات الواجب اتخاذها لإلغاء التغييرات في حالة وجود المشاكل.

ظروف التخزين لحماية البيانات في حالات الكوارث

- تطبيق سياسات النسخ الاحتياطي المنتظم بشكل دوري (يومي/أسبوعي) للبيانات الحرجة.
- تخزين نسخ البيانات في موقع جغرافي منفصل عن الموقع الرئيسي للجامعة، مع مراعاة أن يكون داخل المملكة و أن تكون مراكز بيانات مصممة لمقاومة الحرائق والفيضانات والاضطرابات البيئية
- تشفير البيانات أثناء نقلها وتخزينها، مع تطبيق ضوابط الوصول الصارمة.
- اختبار دوري لخطة استرداد البيانات للتأكد من فعاليتها

القواعد الاسترشادية لسياسة التخزين والاستبقاء

فترات استبقاء البيانات

- يتم تحديد فترات استبقاء البيانات وتخزينها بناءً على ثلاثة معايير رئيسية (تصنيف البيانات، قيمتها التشغيلية والقانونية، المتطلبات النظامية المعمول بها) (يرجى الاطلاع على الجدول أدناه)
- تطبق الية استباق وتخزين البيانات عن طريق تعيين مسؤول استبقاء للبيانات في كل جهة داخل الجامعة، تبدأ فترة الاستبقاء من تاريخ انشاء السجل او اخر تعديل عليه (أيهما أحدث)
- يتم تحديد جدول مرجعي استرشادي للاستبقاء لكل مجموعة بيانات رئيسية في الجامعة

البيانات الرئيسية	مستوى التصنيف	القيمة التشغيلية/ القانونية	المتطلبات القانونية السعودية المرجعية	فترة الاستبقاء الأساسية
يقوم مسؤول استبقاء البيانات بتحديد مجموعة البيانات الرئيسية في جهته.	يقوم مسؤول استبقاء البيانات بالتعاون مع مختص البيانات بتصنيف البيانات إلى: • سري للغاية • سري • مقيد • عام	يقوم مسؤول استبقاء البيانات بالتعاون مع مختص البيانات بتصنيف البيانات بحسب قيمتها التشغيلية والقانونية إلى: • عالية • متوسطة • متدنية	يقوم مسؤول استبقاء البيانات بالتعاون مع مختص البيانات والمستشار القانوني بالاطلاع على اللوائح ذات الصلة، على سبيل المثال لا الحصر: نظام الجامعات، لائحة الوثائق والمحفوظات، ضوابط هيئة البيانات والذكاء الاصطناعي (SDAIA)	بناءا على ماسبق، يتم تحديد فترة الاستبقاء الأساسية: • أقل من ٣ سنوات • ٣-٧ سنوات • ٧-١٥ سنة • دائمة

مستودعات التخزين حسب فترة الاستبقاء

فترة الاستبقاء	مكان التخزين الأساسي	مكان التخزين الاحتياطي
أقل من 3 سنوات	الأنظمة الحية الفعالة	نسخ احتياطي على الموقع الرئيسي
3-7 سنوات	نظام الأرشيف الإلكتروني (وثق)	مركز بيانات ثانوي داخل المملكة
7-15 سنة	مركز أرشيف وطني معتمد	تخزين خارج الجامعة معتمد
أكثر من 15 سنة / دائم	أرشيف الجامعة الدائم	نسخة في الأرشيف الوطني السعودي

القواعد الاسترشادية لسياسة التخزين والاستبقاء

قواعد الاتلاف بناءا على نوع و تصنيف البيانات

فيما يلي قائمة مبسطة استرشادية لقواعد الاتلاف الامن للبيانات بحسب تصيفها ونوعها:

البيانات الرقمية

تصنيف البيانات	طريقة الإتلاف	الإجراء	التوثيق المطلوب
بيانات سريّة للغاية	إتلاف مادي	تدمير الوسيط مادياً (تمزيق، سحق، محو مغناطيسي)	شهادة إتلاف موقعة + تسجيل بالرقم التسلسلي للوسيط
بيانات سريّة	محو آمن	استخدام برامج محو آمن أو تشفير ثم حذف مفتاح التشفير	سجل المحو + إشعار للإدارة المختصة
بيانات داخليّة مقيدة	إعادة كتابة على البيانات	كتابة بيانات عشوائية فوق الملفات أو إعادة تهيئة منخفضة المستوى	سجل بالعملية مع تاريخ التنفيذ
بيانات عامة	حذف عادي	حذف من النظام + إفراغ سلة المحذوفات	لا يحتاج توثيق تفصيلي

البيانات الورقية

تصنيف البيانات	طريقة الإتلاف	الإجراء	التوثيق المطلوب
بيانات سريّة للغاية	التمزيق الدقيق والتدمير	تمزيق إلى قطع متناهية الدقة أو التحويل إلى عجينة	شهادة إتلاف + حضور شاهدين
بيانات سريّة	التمزيق الآمن	تمزيق آمن	سجل التدمير مع الكمية والتاريخ
بيانات داخليّة مقيدة	إعادة التدوير الآمن	تمزيق عادي ثم إرسال لشركة إعادة تدوير معتمدة	إيصال الاستلام من شركة الإتلاف
بيانات عامة	إعادة التدوير العادي	وضع في حاويات إعادة التدوير العامة	لا يحتاج توثيق

الاجراءات المطلوبة في حالة الفقدان الدائم للبيانات الغير مقصود

فيما يلي قائمة الاجراءات للاتلاف الامن للبيانات بحسب تصيفها ونوعها:

الاجراءا ت الفورية حين اكتشاف الخلل	
1. الإبلاغ الفوري	إخطار رئيس القسم/الوحدة ومدير ادارة التحول الرقمي وتقنية المعلومات فوراً
2. عزل النظام المتضرر	فصل الجهاز/الخادم/الوسيط عن الشبكة لمنع انتشار الضرر في حال كانت البيانات رقمية
3. التقييم الأولي	تحديد نوع البيانات المفقودة، تصنيفها، (الأجهزة المتأثرة في حال كانت البيانات رقمية)
الإجراءات خلال ٢٤ ساعة	
4. تشكيل فريق الاستجابة	ضم ممثلين من كافة الجهات شاملة ممثلين من التقنية ، الإدارة القانونية، الوحدة المعنية.
5. جمع الأدلة	أخذ لقطات للنظام، سجلات الدخول، تحليل السبب الجذري لحدوث المشكلة
6. تقييم الأثر	تحديد: مستوى الخطر، عدد الأشخاص المتأثرين، الالتزامات القانونية
الإجراءات خلال ٧٢ ساعة	
7. الإخطار الداخلي	إبلاغ الإدارة العليا واللجنة العليا لإدارة وحوكمة البيانات
8. الإخطار الخارجي	إذا فقدت بيانات شخصية، لابد من إبلاغ هيئة البيانات والذكاء الاصطناعي (SDAIA)خلال 72 ساعة
9. تنشيط خطة الاسترداد	استعادة البيانات من آخر نسخة احتياطية صالحة
10. استرداد البيانات	استعادة البيانات المفقودة من النسخ الاحتياطية
11. تعويض الفاقد	إعادة إدخال البيانات التي لا توجد لها نسخ احتياطية (إن أمكن)
12. الاحتواء والتحسين	تطبيق إجراءات تصحيحية لمنع تكرار الحادث
الإجراءات خلال أسبوع	
13. تقرير الحادث	توثيق كامل للحادث: الأسباب، الإجراءات، الدروس المستفادة
14. المراجعة القانونية	تقييم الالتزام بالنظم السعودية ووجود مخاطر قانونية

الأطراف المعنية بالسياسة

الأطراف المعنية بالسياسة	الأدوار الرئيسية
الإدارة العليا في الجامعة	• اعتماد السياسة رسمياً • تخصيص الموازنات اللازمة • المراجعة النهائية للمخاطر • المسؤول النهائي عن الامتثال • دعم الثقافة المؤسسية للسياسة
اللجنة الإشرافية لإدارة وحوكمة البيانات	• الإشراف على تنفيذ السياسة • حل التعارضات بين الوحدات • تحديث السياسة سنوياً
مركز الوثائق والمحفوظات	• استلام وحفظ البيانات الدائمة • تطبيق معايير الأرشيف الوطني • تسهيل استرجاع الأرشيف
إدارة التحول الرقمي وتقنية المعلومات	• توفير بنية التخزين المناسبة • تنفيذ النسخ الاحتياطي والاسترداد • تأمين البيانات تقنياً • تشغيل مراكز البيانات الفعلية • ضمان التوفرية والمرونة • الصيانة الدورية لأنظمة التخزين
مكتب إدارة البيانات	• ضمان الامتثال لنظام حماية البيانات الشخصية • التدقيق الداخلي على سياسات الاستبقاء • التواصل مع الهيئات الرقابية (SDAIA، الأرشيف الوطني
إدارة الأمن السيبراني	• مراقبة أمن تخزين البيانات • التحقيق في حوادث الاختراق/الفقدان • تطبيق سياسات التشفير
مستخدمي البيانات (الموظفون والطلبة)	• اتباع سياسة التخزين في عملهم اليومي • تصنيف البيانات التي ينتجونها • الإبلاغ عن أي مخالفات أو فقدان

الأدوار والمسؤوليات

المهام الرئيسية	اللجنة العليا لإدارة وحوكمة البيانات	اللجنة الإشرافية لإدارة وحوكمة البيانات	إدارة التحول الرقمي وتقنية المعلومات	مكتب إدارة البيانات
تطوير وتحديث سياسة التخزين والاستبقاء	A	C	I	R
تصنيف البيانات	A	R	R	R
إدارة جدول الاستبقاء وتحديثه	A	R	R	R
التخزين الامن للبيانات	A	I	R	C
الاتلاف الامن	A	I	R	C
الامتثال والتدقيق	A	R	R	R

- تشمل اللجنة العليا لإدارة وحوكمة البيانات رئيس الجامعة ووكلائه
- تشمل اللجنة الإشرافية لإدارة وحوكمة البيانات ملاك البيانات الرئيسية في الجامعة

- R - Responsible (المسؤول عن التنفيذ):
"الشخص الذي يعمل" – الذي ينفذ المهمة فعليًا.
- A - Accountable (المسؤول عن المحاسبة/الموافقة النهائية):
"المحاسب الوحيد" – له الكلمة النهائية ويحاسب على النتيجة .
- C - Consulted (يُستشار):
"يُطلب رأيه" – يتم استشارته قبل التنفيذ.
- I - Informed (يُعلم):
"يُعلم فقط" – يتم إطلاعه على النتائج أو القرارات.

التحديث والمراجعة

يجب على مكتب إدارة البيانات مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة جدة أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

- يجب على مدير مكتب إدارة البيانات التأكد من التزام جامعة جدة بهذه السياسة دوريا.
- يجب على جميع العاملين في جامعة جدة الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة جدة.

السياسات المرتبطة

- سياسة تصنيف البيانات
- سياسة حوكمة البيانات

المراجع

ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية، مكتب إدارة البيانات الوطنية، سدايا.

جامعة جدة
University of Jeddah

مكتب إدارة البيانات
Data Management Office

سياسة تصنيف البيانات بجامعة جدة

تصنيف الوثيقة: مقيد
رقم الإصدار 1.0
التاريخ: 30 / 11 / 2025
المرجع: ضوابط ومواصفات إدارة البيانات الوطنية وحماية البيانات الشخصية

تفاصيل الوثيقة

اسم الوثيقة	سياسة تصنيف البيانات بجامعة جدة		
المؤسسة	جامعة جدة		
مالك الوثيقة	مكتب إدارة البيانات		
رقم الاصدار	2.1		
تاريخ أحدث إصدار	8/12/2025	تاريخ المراجعة القادم	8/12/2025
تصنيف الوثيقة	مقيد		

ضبط أحدث إصدار

الاسم	الدور	تحرير	مراجعة	اعتماد
V 2.1	8/12/2025	د. نورة الغامدي	د. طرفة الراشد	د. نورة الغامدي

سجل الإصدارات

رقم الإصدار	التاريخ	تحرير	التعديلات	اعتماد
2.1	8/12/2025	د. نورة الغامدي	• اضافة المصطلحات • اضافة ضوابط التصنيف • اضافة الخطوات اللازمة للتصنيف • اضافة الأدوار والمسؤوليات • اضافة السياسات المرتبطة • اضافة المراجع	د. نورة الغامدي
2	5/5/2024	د. ماجدة الوزان	تعديل مستويات التصنيف حسب المتطلبات الحديثة	د. محمد كلكتاوي
1.2	2/14/2024	د. ماجدة الوزان	تعديل المالك	د. محمد كلكتاوي
1.1	8/9/2021	د. ماجدة وزان	إضافة شعار الجامعة وشعار إدارة الأمن السيبراني	د. منير الشيخ
1.0	8/18/2020	ا. ماجدة وزان	انشاء النسخة الأولى	د. عادل الشمراني

المحتويات

المصطلحات

المصطلح	التعريف
الجامعة	جامعة جدة
مالكي البيانات	هي جهة أو قطاع داخلي يملك جزء من البيانات في الجامعة (بيانات الأعمال الخاصة بالقطاع)، مثال: عمادة القبول والتسجيل مالك بيانات الطلبة
ممثلي بيانات الأعمال	هو الشخص الذي يمثل جهة مالكة لجزء من بيانات الجامعة ومهمته التحقق من امتثال جهته لسياسات مكتب إدارة البيانات الوطنية المتعلقة بأنظمة تصنيف البيانات وخصوصية البيانات وحرية المعلومات وسياسات ومعايير إدارة البيانات، مثال: عميد القبول والتسجيل
مختص البيانات	هو الشخص المسؤول عن دعم وضمان تطبيق الجهة مالكة البيانات التي يمثلها لأنظمة تصنيف البيانات وخصوصية البيانات وحرية المعلومات وسياسات إدارة البيانات (مثل مشاركة البيانات وتحقيق الإيرادات من البيانات) ومعايير إدارة البيانات والامتثال لها.

الهدف

الهدف من هـذه السياسة هو تحـديـد متطلبـات والية تصنيف البيـانـات بحسب مستوى حساسيتها في جامعة جدة سواء كانت بيانات مهيكلة أو غير مهيكلة، وذلـك امتثالا للضوابط والمواصفات الوطنية لإدارة البيانات وحوكمتها وحماية البيانات الشخصية.

تمت موائمة هذه السياسة مع ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية الصادرة من المكتب الوطني لإدارة البيانات والمتطلبات التنظيمية والتشريعية ذات العلاقة.

إن مدة صلاحية هذه الوثيقة هي 3 أعوام من تاريخ إصدارها، ويجب على مكتب إدارة البيانات مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، ويجوز أيضا تحديثها فور حدوث أي تعديلات أو تغييرات تتعلق بالمتطلبات التشريعية والتنظيمية ذات العلاقة، ويتم تغيير رقم إصدار الوثيقة عند القيام بأي تعديل سواء كان جوهرياً أو ثانويا. وينبغي اعتماد هذه التحديثات أو التعديلات من قبل اللجنة الاشرافية لإدارة البيانات بجامعة جدة.

نطاق السياسة

تنطبق هذه السياسة على جميع البيانات في جامعة جدة التي تحتفظ بها جامعة جدة وتخزنها وتعالجها وتنقلها من خلال الأصول المعلوماتية والتقنية وتنشرها، وتطبق السياسة على جميع المستخدمين والعاملين (الموظفين والمتعاقدين) في جامعة جدة.

المبادئ الرئيسية لتصنيف البيانات

تم تحديد سبع مبادئ أساسية لتصنيف البيانات وهي كالتالي:

المبدأ الأول: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة في المجال التنموي مالم تقتضي طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية والسرية مثل البيانات ذات التأثير الحساس في المجال السياسي والأمني.

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 انشائها 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 اتلافها - بطريقة تحول دون تداخل الاختصاص.

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.

قواعد عامة

01
يجب على مكتب إدارة البيانات توعية منسوبي جامعة جدة بأهمية حماية البيانات التي يتم إنشاؤها، وتخزينها من قبل الجامعة، وتحديد الإجراءات اللازمة لحماية سرية وسلامة وتوافر بيانات الجامعة.

02
ويجب على جميع المنسوبين والمستخدمين الذين يعملون بصورة مباشرة أو غير مباشرة لدى الجامعة، أو الجهات التابعة لها أو أية جهة تقوم بتنفيذ عمل نيابة عن الجامعة الامتثال لهذه السياسة، حيث أن ذلك يتضمن استخدام الأصول المعلوماتية التابعة لها.

03
تكون قطاعات الجامعة مسؤولة عن تطبيق الضوابط الإدارية والتشغيلية والمادية، والتقنية المناسبة للوصول او استخدام او نقل، او التخلص من بيانات الجامعة وفقا لهذه السياسة.

04
جميع المعلومات الخاصة بالجامعة هي مسؤولية كل من يتعامل معها وعلى النحو التالي:

4-1: مختص البيانات : يجب أن يكون لكل جهة داخلية مسؤول مختص لبيانات الجهة، وهو من توكل إليه المهمة لتحقيق المهام الرئيسية التالية:

- إنشاء تصنيف مبدئي للبيانات، يتضمن إعطاء مستويات تصنيف لجميع البيانات داخل جهته.
- التأكد من أن البيانات يتم مراجعتها بانتظام حسب أهميتها ومدى التغيرات المؤثرة على أهميتها عند وقوع المخاطر : كالتهديدات الجديدة أو نقاط الضعف المكتشفة في الأنظمة أو أية تغيرات فيا لبيئة المحيطة بها.
- مراجعة وتعديل التصنيف بين فترة وأخرى حسب التغيرات في أولويات العمل أو القوانين والتعليمات والأنظمة.
- يتحمل ممثلي بيانات الأعمال المسؤولية النهائية في أمن وحماية الموارد المعلوماتية في جهته المالكة للبيانات.
- التأكد من أن جميع المستخدمين على علم بكيفية تداول وحماية المعلومات بطريقة تتناسب مع تصنيفها تطوير إجراءات أمن وحماية المعلومات في الإدارة.

مستويات تصنيف البيانات

2-4: يتم تصنيف البيانات في أي نظام إداري أو أكاديمي والتي تم إنتاجها داخل او خارج الجامعة إلى أربعة مستويات وبناءً على مدى الحساسية و الخصوصية و القيمة العائدة للجامعة:

سرية للغاية

تصنف 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 وقد يكون للكشف عن مثل هذه البيانات أثر سلبي عالي على الجامعة أو على المصالح الوطنية، بما في ذلك الإخلال بالاتفاقيات والمعاهدات او 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، أو صحة الأفراد وسلامتهم على نطاق واسع وخصوصية كبار المسؤولين، أو الموارد البيئية أو الطبيعية. وينبغي تطبيق أقصى مستويات التحكم في هذه البيانات.

سرية

تصنف البيانات على أنها بيانات سرية إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى ضرر جسيم على الجامعة أو على المصالح الوطنية مثل إلحاق ضرر جزئي على سمعة المملكة والعلاقات الدبلوماسية أو الكفاءة التشغيلية للعمليات الأمنية أو العسكرية أو الاقتصاد الوطني أو البنية التحتية الوطنية والأعمال الحكومية، أو يُحدث خسارة مالية على المستوى التنظيمي تؤدي إلى إفلاس أو عجز الجهات عن أداء مهامها او خسارة جسيمة للقدرة التنافسية أو كليهما معا، او يتسبب في حدوث أذى جسيم على حياة مجموعة من الأفراد أو تؤدي إلى ضرر على المدى الطويل للموارد البيئية او الطبيعية، او التحقيق في القضايا الكبرى المحددة نظاما كقضايا تمويل الارهاب.

مستويات تصنيف البيانات

2-4: يتم تصنيف البيانات في أي نظام إداري أو أكاديمي والتي تم إنتاجها داخل او خارج الجامعة إلى أربعة مستويات وبناءً على مدى الحساسية و الخصوصية و القيمة العائدة للجامعة:

مقيدة

تصنف البيانات على أنها مقيدة، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى تأثير سلبي محدود على الجامعة أو على المصالح الوطنية.

عامة

تصنف 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 أعاه في حال عدم وجود تأثير على الجامعة أو على المصال الوطنية.

ضوابط تصنيف البيانات

بناءا على مستويات التصنيف، تقوم الجهات المالكة للبيانات 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 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 خال فترة زمنية محددة بموجب خطة عمل تعدها مكتب إدارة البيانات ويتم اعتمادها من رئيس الجامعة.
أدناه بعض الأمثلة على الضوابط التي يمكن استخدامها عند تصنيف البيانات، ويمكن الرجوع إلى ما يصدر من الهيئة الوطنية للأمن السيبراني من ضوابط وإرشادات تتعلق بحماية البيانات:

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 بالجامعة.

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

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 العلاقة.
- تتم مراجعة الجدول الزمني لفترة الاحتفاظ بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

ضوابط تصنيف البيانات

مشاركة البيانات

- تقوم جامعة جدةممثلة في مكتب إدارة البيانات 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 الجامعة 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.

التخلص من البيانات:

- يتم التخلص من جميع البيانات بشكل آمن وفقاً للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة ممثل بيانات الأعمال.
- يتم التخلص من البيانات التي تم تصنيفها على أنها "سرية 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.
- •تم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.

الأرشفة:

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقاً 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 1 يناير 2021).
  - بعد ظروف أو أحداث معينة تأثيراً مباشراً على البيانات (على سبيل المثال: إحداث تغيير في الأولويات الاستراتيجية أو تغيير موظفي الجهات الحكومية).

- يتطلب إلغاء التصنيف - رفع السرية - أو خفض مستويات التصنيف، بعيداً عن العوامل المساعدة على إلغاء التصنيف الواضحة تماماً، فهماً سليماً لمحتوى البيانات السرية والسياق الذي وردت فيه.

الخطوات اللازمة لتصنيف البيانات

الخطوة ا - تحديد جميع بيانات الجهة:

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

الخطوة 2 - تعيين مسؤول تصنيف البيانات:

على جامعة جدة تفويض شخص يتولى مسؤولية عملية التصنيف بمجرد تحديد جميع البيانات، غالباً ما يكون ممثل بيانات الأعمال هو الشخص الذي يفهم طبيعة البيانات وقيمتها داخل الجهة، وهو الشخص الذي يجب أن يتحمل المسؤولية حيال إجراء التصنيف الأولي، ونظراً إلى وجود 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 إليها
- 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) ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية: السرية للغاية (في المجال السياسي والأمني) ما لم تقتض طبيعتها أو حساسيتها مستويات أدنى من التصنيف.

الخطوة 3أ - تحديد فئة الأثر

يتمثل العنصر الأول من عملية تقييم الأثر في تحديد الفئة الرئيسة والفرعية للأثر المحتمل في أي من الفئات الرئيسية التالية:

- المصلحة الوطنية
- أنشطة الجهات
- صحة أو سلامة الأفراد
- الموارد البيئية

الخطوات اللازمة لتصنيف البيانات

الخطوة 3ب - تحديد مستوى الأثر

يشير 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 ... إلخ**

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 خال 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:

عالٍ : تصنف البيانات باعتبارها "سرية للغاية".

متوسط: تصنف البيانات على أنها "سرية".

منخفض: يلزم إجراء مزيدٍ من التقييمات (يرجى الاطلاع على الخطوة 4 و5).

لا يوجد أثر: تصنف البيانات على أنها بياناتٍ "عامة".

يجب الأخذ بعين الاعتبار الخطوتين 4 و5 عندما يكون مستوى الأثر المحدد منخفض.
يتم الانتقال إلى الخطوة 6 عندما تُصنف البيانات على أنها "سرية للغاية" أو "سرية" أو "عامة"

الخطوات اللازمة لتصنيف البيانات

الخطوة 4 - تحديد الأنظمة ذات العلاقة (فقط إذا كان مستوى الأثر منخفضاً).

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 الإلكترونية ... الخ وإذا كان الإفصاح عن البيانات مخالفاً للأنظمة، فيجب حينها تصنيف البيانات على أنها بيانات "مقيدة"، بخلاف ذلك يتعين على ممثل بيانات الأعمال مواصلة تنفيذ الخطوة 5.

الخطوة 5 - الموازنة بين مزايا الإفصاح عن البيانات والآثار السلبية (فقط إذا كانت الإجابة على الخطوة 4 "لا")

بعد التأكد من مستوى الأثر المنخفض وضمان أن الإفصاح لن يكون انتهاكاً لأي نظام نافذ، يجب أيضاً 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 الأفراد 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 "مقيدة".

الخطوة 6 - مراجعة مستوى التصنيف

يجب أن يفحص مراجع تصنيف البيانات – أحد منسوبي مكتب إدارة البيانات في جامعة جدة – 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 وفقاً لمستوى التصنيف عن طريق تطبيق عناصر التحكم ذات الصلة (راجع "ضوابط تصنيف البيانات").
يتم الانتهاء من عملية التصنيف عند تصنيف جميع البيانات التي تملكها الجهة والتحقق من مستويات التصنيف وتطبيق الضوابط ذات الصلة.
بعد تصنيف البيانات على نحو صحيح، يمكن للجهات مشاركتها مع جهات أخرى، أو إتاحتها ونشرها بصفتها بيانات مفتوحة عند تصنيفها بيانات "عامة"

الأدوار والمسؤوليات داخل جامعة جدة

على جامعة جدة تكليف أشخاص يتولون مسؤولية أداء الالتزامات المسندة لكل دور 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، وعادة 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 مصادر متعددة على 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 وفقاً 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:
يتحمل مسؤولية حماية البيانات عن طريق تطبيق الضوابط المعتمدة المحددة في قسم "ضوابط تصنيف البيانات" بالإضافة إلى ذلك، الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها، وتتألف مسؤوليات مختص بيانات الأعمال من:

- **التحكم في الوصول:** التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقا 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 ووفقاً للضوابط المحددة

مستخدم البيانات: الموظف الذي يتعامل مع البيانات أو يصل إليها أو يستخدمها أو يحدثها 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، ويكلف رئيس الجامعة من يراه من ذوي الاختصاص لأداء هذه الأدوار

الأدوار والمسؤوليات

المهام الرئيسية	اللجنة العليا لإدارة وحوكمة البيانات	اللجنة الإشرافية لإدارة وحوكمة البيانات	إدارة التحول الرقمي وتقنية المعلومات	مدير مكتب إدارة البيانات
صياغة سياسة تصنيف البيانات	A	C	I	R
صياغة خطة تشغيلية لتصنيف البيانات	A	C	I	R
معالجة المعيقات للخطط التشغيلية	C	A	R	R
تنفيذ جلسات التدريب والتوعية للمستخدمين	A	C	I	R
تحديد وتصنيف أصول البيانات الحالية (البيانات الموجودة)	A	C	I	R
معالجة الحوادث المتعلقة بسوء التصنيف أو الاختراق	A	R	R	R
مراقبة الامتثال لسياسة التصنيف	A	R	R	R
رفع التقارير للجنة العليا لإدارة وحوكمة البيانات	A	R	C	R

- تشمل اللجنة العليا لإدارة وحوكمة البيانات رئيس الجامعة ووكلائه
- تشمل اللجنة الإشرافية لإدارة وحوكمة البيانات ملاك البيانات الرئيسية في الجامعة

- R - Responsible (المسؤول عن التنفيذ):
"الشخص الذي يعمل" – الذي ينفذ المهمة فعليًا.
- A - Accountable (المسؤول عن المحاسبة/الموافقة النهائية):
"المحاسب الوحيد" – له الكلمة النهائية ويحاسب على النتيجة .
- C - Consulted (يُستشار):
"يُطلب رأيه" – يتم استشارته قبل التنفيذ.
- I - Informed (يُعلم):
"يُعلم فقط" – يتم إطلاعه على النتائج أو القرارات.

التحديث والمراجعة

يجب على مكتب إدارة البيانات مراجعة السياسة سنويا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة جدة أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

- يجب على مدير مكتب إدارة البيانات التأكد من التزام جامعة جدة بهذه السياسة دوريا.
- يجب على جميع العاملين في جامعة جدة الالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة جدة.

السياسات المرتبطة

- سياسة حوكمة البيانات
- سياسة البيانات المفتوحة
- سياسة حرية المعلومات
- سياسة مشاركة البيانات

المراجع

سياسة تصنيف البيانات، سدايا
ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية