جامعة البحرين

سياسة تصنيف البيانات والمعلومات والوثائق

الملكية / مسؤولية السياسة: مدير عام الخدمات الإدارية

تاريخ السريان: ١٩ أكتوبر ٢٠٢٥م

المحتوى

1 تعاريف عامة..... ٣

2 هدف السياسة..... ٤

3 نطاق السياسة..... ٤

4 محتوى السياسة ٤

5 المسؤوليات والأدوار ٧

6 الإجراءات المتبعة في السياسة ٨

7 جهة الاتصال والمعلومات.....

معلومات السياسة

المسمى:	سياسة تصنيف البيانات والمعلومات والوثائق	
وصف السياسة:	تُعد هذه السياسة إطاراً تنظيمياً شاملاً لحماية البيانات والمعلومات والوثائق في جامعة البحرين من خلال تصنيفها إلى أربعة مستويات (سري للغاية، سري، محظور/محدود، عام) وربط كل مستوى بضوابط حماية مناسبة، على نحو يضمن حماية فعالة لجميع البيانات والمعلومات والوثائق الأكاديمية والإدارية والمالية والبحثية في الجامعة.	
نطاق السياسة:	☐ أكاديمي ☐ إداري ☐ بحثي ☐ طلابي ☒ عام	
حالة السياسة :	☒ سياسة جديدة	☐ التعديل على سياسة قائمة
جهة الاعتماد:	مجلس جامعة البحرين	
الملكية / مسؤولية السياسة:	مدير عام الخدمات الإدارية	
تاريخ الاعتماد:	١٩ أكتوبر ٢٠٢٥م	
تاريخ السريان:	١٩ أكتوبر ٢٠٢٥م	
تاريخ المو افقة على آخر مراجعة:	١٩ أكتوبر ٢٠٢٥م	
تاريخ المراجعة القادمة:	أكتوبر ٢٠٣٠م	
رقم قرار مجلس الجامعة:	٢٠٢٥/١/٥٥٧	
رقم الوثيقة:	UOB-GDAS-PO-007	
الوثائق ذات الصلة:	قانون رقم (٣٠) لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية، قانون رقم (١٦) لسنة ٢٠١٤ بشأن حماية معلومات ووثائق الدولة، قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات وسياسات أمن المعلومات المرعية بالجامعة	

الجهات المعنية بالسياسة

☐ رئيس الجامعة.

☐ نواب رئيس الجامعة.

☐ المستشار القانوني.

☐ العمداء.

☐ المدراء.

☐ أعضاء هيئة التدريس.

☐ الموظفون الإداريون.

☐ الطلبة.

☒ جميع منتسبي الجامعة.

١ تعاريف عامة

في تطبيق أحكام هذه السياسة، يكون للكلمات والعبارات التالية المعانيَ المبينةَ قرينَ كُلٍّ منها، ما لم يقتض سياقُ النص خلاف ذلك:

الجامعة:	جامعة البحرين.
البيانات والمعلومات والوثائق:	جميع البيانات والمعلومات والوثائق النصية أو الورقية أو الإلكترونية التي تنتجها أو تتداولها الجامعة عبر أنظمتها وتطبيقاتها وتقنياتها.
التصنيف:	عملية تقييم البيانات والمعلومات والوثائق وفقًا لدرجة حساسيتها وأهميتها، ومن ثم تعيين مستوى الحماية الملائم لها بما يكفل سرّيتها وسلامتها وتوافرها.
مستوى التصنيف:	الدرجة المحددة لحساسية وأهمية البيانات والمعلومات والوثائق داخل الجامعة.
الوسم:	عملية وضع إشارة مادية أو الكترونية واضحة على الوثائق أو المعلومات المصدّرة أو المخزنة، بما يُبيّن مستوى تصنيفها ويُسهل التعرف على متطلبات التعامل معها.
مالك البيانات والمعلومات والوثائق:	الجهة الإدارية أو الأكاديمية (كلية، عمادة، إدارة، مركز أو غيرها من الوحدات التنظيمية) التي تنشئ البيانات والمعلومات والوثائق وتتحمل المسؤولية الأساسية عن دقتها وجودتها وتصنيفها وتنفيذ ضوابط حمايتها.
مستخدم البيانات والمعلومات والوثائق:	أي فرد من منتسبي الجامعة أو المتعاملين معها يُمنح صلاحية الوصول إلى البيانات والمعلومات والوثائق واستخدامها في حدود ما تقتضيه مهام عمله أو اختصاصه.

٢ هدف السياسة

تهدف هذه السياسة إلى حماية البيانات والمعلومات والوثائق وضمان سريتها وحمايتها من الوصول غير المصرح، والامتثال للقوانين والسياسات المرعية بالدولة.

٣ نطاق السياسة

تنطبق هذه السياسة على جميع البيانات والمعلومات والوثائق المخزنة أو المعالجة أو المتداولة بالجامعة، سواء كانت ورقية أو إلكترونية، ويشمل ذلك البيانات المتبادلة مع الأطراف الثالثة من مزودين أو متعاقدين أو شركاء خارجيين، كما تُعتبر الملاحق المرافقة لهذه السياسة جزءًا لا يتجزأ منها وتتمتع بذات القوة الإلزامية.

٤ محتوى السياسة

٤,١ مستويات التصنيف

تُصنَّف البيانات والمعلومات والوثائق في الجامعة ضمن واحد من المستويات الأربعة الآتية، استنادًا إلى تقييم أثر الكشف غير المصرح به عنها، وذلك وفقًا لما هو موضح في الملحق رقم (١) المرافق لهذه السياسة:

٤,١,١ المستوى الأول: سري للغاية

تُصنَّف ضمن هذا المستوى البيانات والمعلومات والوثائق التي يؤدي الكشف غير المصرح به عنها إلى إلحاق ضرر بالغ الخطورة بالأمن الوطني أو المصالح العليا للدولة أو الجامعة. ويُقصر الاطلاع عليها على الأشخاص المصرح لهم بالاسم من قبل رئيس الجامعة.

٤,١,٢ المستوى الثاني: سري

تصنف ضمن هذا المستوى البيانات والمعلومات والوثائق التي يؤدي الكشف غير المصرح به عنها إلى إلحاق ضرر بمصالح الجامعة أو الدولة، أو إلى انتهاك خطير لخصوصية الأفراد. ويُحدد الوصول إلى

هذا المستوى للموظفين المصرح لهم الذين تقتضي طبيعة عملهم ذلك، وفق صلاحيات تُمنح بناءً على الدور الوظيفي.

٤,١,٣ المستوى الثالث: محظور/محدود

تصنف ضمن هذا المستوى البيانات والمعلومات والوثائق المخصصة للاستخدام الداخلي فقط داخل الجامعة، ويُعد المستوى الافتراضي لمعظم البيانات والمعلومات والوثائق غير المصنفة للنشر العام. ويُسمح بالاطلاع عليها لجميع منتسبي الجامعة ما لم يفرض مالك البيانات والمعلومات والوثائق قيودًا إضافية.

٤,١,٤ المستوى الرابع: عام

تصنف ضمن هذا المستوى البيانات والمعلومات والوثائق التي تمت الموافقة على نشرها للعامة، وتُتاح للجميع دون قيود.

٤,٢ معايير التصنيف

تُصنَّف البيانات والمعلومات والوثائق وفقًا لمعايير تهدف إلى ضمان سريتها وسلامتها وتوافرها، وذلك استنادًا إلى ما يلي:

١- تقييم التأثير: يتم التصنيف بناءً على أثر الكشف غير المصرح به على الاضرار من عدمه بالمصلحة العامة للجامعة أو بحسن سير العمل فيها أو بمصلحة أو خصوصية منتسبيها أو المتعاملين معها على نحو يستلزم ادراج المعلومة من عدمه تحت مستوى من مستويات السرية.

٢- العوامل المؤثرة في التصنيف: يُحدد مستوى التصنيف أيضًا وفقًا لطبيعة البيانات والمعلومات والوثائق ومحتواها، ومصدرها، والجهة المستفيدة منها، والمتطلبات القانونية والتنظيمية ذات الصلة.

٤,٣ متطلبات الحماية حسب التصنيف

تُعتمد في الجامعة المتطلبات الأمنية الآتية لحماية البيانات والمعلومات والوثائق:

١- متطلبات عامة: تلتزم الجهات المعنية في الجامعة بتطبيق الضوابط الأساسية لحماية البيانات والمعلومات والوثائق، بما يشمل الوقاية من الفيروسات، تفعيل أنظمة الجدران النارية، تنفيذ التحديثات الأمنية الدورية، وأخذ نسخ احتياطية منتظمة لضمان استمرارية الأعمال.
٢- متطلبات خاصة بالبيانات والمعلومات والوثائق عالية الحساسية (سري للغاية وسري): بالإضافة إلى المتطلبات العامة المنصوص عليها أعلاه، تلتزم الجهات المعنية بتشفير البيانات والمعلومات والوثائق أثناء التخزين وأثناء النقل، وفرض ضوابط وصول منطقية صارمة على مستوى الأنظمة والتطبيقات، وتخزين النسخ الورقية في خزائن محكمة الإغلاق داخل أماكن مؤمنة، وكذلك تسجيل ومراقبة جميع محاولات الوصول ومراجعتها بصفة دورية، فضلًا عن استخدام أنظمة وتقنيات متخصصة لمنع تسرب البيانات والمعلومات والوثائق بكافة صورها
٣- الوسم: يتعين وضع علامات ووسوم واضحة على البيانات والمعلومات والوثائق المصنفة وفقًا لمستوى تصنيفها، وذلك باستخدام الوسائل المادية أو الالكترونية المعتمدة في الجامعة. وتفصَّل معايير وأشكال الوسم في الملحق (٢) المرافق لهذه السياسة.

٤,٤ إدارة دورة الحياة

تلتزم الجامعة بإدارة دورة حياة البيانات والمعلومات والوثائق منذ إنشائها وحتى إتلافها، وفق الضوابط الآتية:

١- التصنيف عند الإنشاء: يتولى مالك البيانات والمعلومات والوثائق المختص تصنيف ما يتم إنشاؤه أو استلامه لأول مرة، بهدف تحديد مستوى الحساسية وتطبيق الضوابط الأمنية الملائمة وفقًا للسياسات المعتمدة
٢- المراجعة الدورية: تُراجع التصنيفات من قبل مالك الوثيقة عند حدوث تغييرات جوهرية في طبيعة البيانات والمعلومات والوثائق أو استخداماتها، للتحقق من استمرار ملاءمة مستوى التصنيف.
٣- الإتلاف الآمن: تُتلف البيانات والمعلومات والوثائق المصنفة إتلافًا آمنًا، سواء كانت ورقية باستخدام وسائل الإعدام المعتمدة، أو إلكترونية باستخدام تقنيات المسح النهائي، وبما يضمن استحالة استردادها أو إعادة استخدامها.

٥ المسؤوليات والأدوار

الجهة	المسؤولية
رئيس الجامعة:	اعتماد هذه السياسة من مجلس الجامعة والاشراف على تنفيذها وتوفير الموارد اللازمة لحماية البيانات والمعلومات والوثائق.
إدارة تقنية المعلومات والتعليم الرقمي:	تطبيق الضوابط التقنية اللازمة لحماية البيانات والمعلومات والوثائق، وادارة صلاحيات الوصول، ومراقبة الشبكات والأنظمة، وتقديم الدعم الفني.
مالك البيانات والمعلومات والوثائق:	تصنيف البيانات والمعلومات والوثائق الواقعة تحت مسؤوليته، وتحديد متطلبات الوصول، ومنح الصلاحيات، واجراء المراجعات الدورية للتصنيف والصلاحيات.
مستخدم البيانات والمعلومات والوثائق:	الالتزام بأحكام هذه السياسة، والتعامل مع البيانات والمعلومات والوثائق وفق مستوى تصنيفها، وحماية كلمات المرور الخاصة به، والابلاغ فورًا عن أي حادثة تمس أمن البيانات والمعلومات والوثائق.
مكتب التدقيق الداخلي:	الرقابة على الالتزام بأحكام هذه السياسة، من خلال إجراء مراجعات دورية على آليات تصنيف البيانات والمعلومات والوثائق وحمايتها، ورفع تقارير دورية بنتائج المراجعة والتوصيات إلى رئيس الجامعة.
جهات التدريب بالجامعة:	تنظيم برامج تدريبية وتوعوية دورية تستهدف جميع منتسبيها من أكاديميين وإداريين وطلبة، وذلك لرفع مستوى الوعي بأهمية تصنيف البيانات والمعلومات والوثائق وضوابط حمايتها، وتوضيح الإجراءات الواجب اتباعها للتعامل معها وفقًا لمستوى التصنيف المعتمد، وبما يضمن الامتثال التام لأحكام هذه السياسة.

٦ الإجراءات المتبعة في السياسة

١- **إجراءات التصنيف:** يلتزم مالك البيانات والمعلومات والوثائق بتقييم البيانات والمعلومات والوثائق الجديدة أو المستلمة، وتحديد مستوى التصنيف المناسب لها، ووضع الوسوم المحددة، وتوثيق القرار في سجل رسمي، وإبلاغ المستخدمين المعنيين بمتطلبات التعامل معها.

٢- **إجراءات منح الصلاحيات:** تُقدَّم طلبات الوصول إلى البيانات والمعلومات والوثائق وفقًا للإجراءات المعتمدة لدى الجهة المختصة، ويُراجعها مالك البيانات والمعلومات والوثائق للموافقة أو الرفض بناءً على الحاجة الفعلية. وتتولى إدارة تقنية المعلومات والتعليم الرقمي تنفيذ الصلاحيات المقررة على الأنظمة الالكترونية المعتمدة بالجامعة، مع توثيق جميع العمليات في سجلات رسمية، بالإضافة إلى توقيع اتفاقية عدم الإفصاح للطرف الثالث.

٣- **إجراءات المراجعة الدورية:** يُراجع مالك البيانات والمعلومات والوثائق الصلاحيات الممنوحة للوصل إليها بشكل دوري، وتُلغى فور زوال الحاجة إليها، كما يُراجع تصنيف البيانات والمعلومات والوثائق عند حدوث تغييرات جوهرية في طبيعتها أو استخداماتها وفقاً للمتغيرات القانونية، وتُوثق النتائج وتتخذ الإجراءات التصحيحية اللازمة.

٤- **إجراءات الإبلاغ عن الخروقات:** يجب على مستخدم البيانات والمعلومات والوثائق أو مالكها الإبلاغ الفوري عن أي خرق أو اشتباه بخرق يتعلق بها إلى إدارة تقنية المعلومات والتعليم الرقمي عبر القنوات الرسمية المعتمدة خلال ٢٤ ساعة من اكتشافه. ويلتزم مالك البيانات والمعلومات والوثائق في نطاق مسؤوليته بالإشراف على توثيق جميع حالات الخرق أو الانتهاك، بما في ذلك تحديد أسبابها والآثار المترتبة عليها والإجراءات المتخذة لمعالجتها، وذلك بالتنسيق مع إدارة تقنية المعلومات. وإذا ترتب على الحادثة التزامات قانونية تستوجب إخطار الجهات القانونية المختصة بموجب القوانين السارية، تتولى الإدارة العليا اتخاذ ما يلزم بشأنها في المواعيد المقررة.

٥- **إجراءات الاستجابة للحوادث:** تتولى إدارة تقنية المعلومات والتعليم الرقمي، فور تلقي البلاغ، مسؤولية الاستجابة الأولية للحوادث الأمنية المتعلقة بالبيانات والمعلومات والوثائق، بما يشمل اتخاذ التدابير العاجلة لاحتواء الحادثة والحد من آثارها المباشرة. وعند الحاجة، يُشكَّل فريق متخصص من الإدارة المذكورة للتحقق التفصيلي من الحادثة، وتحديد أسبابها وآثارها، واقتراح الإجراءات التصحيحية اللازمة. ثم يُرفع تقرير مفصل بنتائج التحقيق والتوصيات إلى مدير عام الخدمات الإدارية لاتخاذ القرارات المناسبة ومعالجة ما قد يترتب من التزامات أو تدابير لاحقة.

٦- **إجراءات الإتلاف الآمن للبيانات والمعلومات والوثائق:** عند انتهاء الغرض من الاحتفاظ بالبيانات أو عند انقضاء المدة القانونية أو التنظيمية للاحتفاظ بها، يجب التخلص منها باستخدام وسائل إتلاف آمنة ومعتمدة، بما يضمن عدم إمكانية استرجاعها أو إعادة استخدامها. ويشمل ذلك:

- بالنسبة للبيانات الورقية: الإتلاف باستخدام آلات التمزيق الأمني أو عبر مزود خدمة معتمد للإتلاف.
- بالنسبة للبيانات الرقمية/الإلكترونية: الحذف الآمن باستخدام برمجيات إزالة متقدمة (Data Wiping) أو تدمير الوسائط التخزينية فعليًا إذا لزم الأمر.

٧ أحكام ختامية

تُعدّ مخالفة أحكام هذه السياسة سببًا للمساءلة التأديبية أو الإدارية، بحسب الأحوال، وذلك وفقًا للوائح والأنظمة المطبقة في الجامعة، وذلك دون الإخلال بالمسؤولية القانونية المقررة بموجب القوانين ذات الصلة.

٨ جهة الاتصال والمعلومات

للحصول على مزيد من المساعدة حول تطبيق هذه السياسة، بالإمكان التواصل مع مكتب المدير العام للخدمات الإدارية:

البريد الإلكتروني: dgas@uob.edu.bh، رقم الهاتف: ١٧٤٣٨٨٨٢

الملحق رقم (١)

أمثلة وضوابط الوصول

مستوى التصنيف	أمثلة	ضوابط الوصول
المستوى الأول: سري للغاية	• البيانات والمعلومات والوثائق التي تتعلق بالأمن الوطني وتكون الجامعة طرفًا فيها. • بيانات حساسة جدًا تخص شخصيات قيادية عليا. • كلمات المرور الرئيسية للبنية التحتية الحساسة. • خطط الطوارئ والأمن السيبراني.	وصول مقصور على أشخاص محددين بالاسم من قبل رئيس الجامعة، وتشفير البيانات والمعلومات والوثائق أثناء التخزين والنقل، وحفظ النسخ الورقية في خزائن مغلقة.
المستوى الثاني: سري	• البيانات والمعلومات والوثائق الشخصية الحساسة للطلاب والموظفين (صحية أو بيومترية). • السجلات الأكاديمية التفصيلية. • نتائج وتقييم الأبحاث قبل نشرها. • العقود والاتفاقيات الاستراتيجية. • البيانات والمعلومات المالية المفصلة قبل إعلانها. • الامتحانات.	وصول مقيد للمستخدمين المصرح لهم بحسب طبيعة عملهم، مع منح الصلاحيات وفق الدور الوظيفي، وتشفير البيانات والمعلومات والوثائق أثناء النقل والتخزين، واعتماد ضوابط مشاركة صارمة.
المستوى الثالث: محظور/محدود	• البيانات والمعلومات والوثائق المخصصة للمراسلات الداخلية. • محاضر الاجتماعات غير المعلنة. • المسودات الأولية للسياسات. • التقارير الإدارية الداخلية. • معلومات الاتصال الداخلية الخاصة بالموظفين.	وصول متاح لجميع منتسبي الجامعة ما لم يفرض مالك البيانات والمعلومات والوثائق قيودًا إضافية، مع تطبيق سياسات مشاركة محدودة وضوابط حماية أساسية (كلمات مرور وتخزين آمن).

مستوى التصنيف	أمثلة	ضوابط الوصول
المستوى الرابع: عام	• البيانات والمعلومات والوثائق المخصصة للنشر العام كالمعلومات المنشورة على الموقع الرسمي للجامعة. • الأخبار الصحفية. • التقويم الأكاديمي. • شروط القبول المعلنة. • السياسات واللوائح العامة المعتمدة. • البيانات المفتوحة والتي تشمل الإحصائيات.	وصول مفتوح للجميع دون قيود، مع الالتزام بالدقة الرسمية للمحتوى المنشور.

الملحق رقم (٢)

معايير وسم البيانات والمعلومات والوثائق

مستوى التصنيف	الوسم المادي (الوثائق الورقية)	الوسم الرقمي (المستندات الإلكترونية)	البريد الإلكتروني	اللون المخصص
المستوى الأول: سري للغاية	ختم/ملصق أحمر بارز يحمل عبارة "سري للغاية"	إدراج عبارة "سري للغاية" في الترويسة والتذييل	يبدأ العنوان بـ: "سري للغاية"	أحمر
المستوى الثاني: سري	ختم/ملصق أصفر يحمل عبارة "سري"	إدراج عبارة "سري" في الترويسة والتذييل	يبدأ العنوان بـ: "سري"	أصفر
المستوى الثالث: محظور/محدود	ختم/ملصق أزرق يحمل عبارة "محدود"	إدراج عبارة "محدود" في التذييل	يبدأ العنوان بـ: "محدود"	أزرق
المستوى الرابع: عام	لا يتطلب وسم خاص	لا يتطلب وسم خاص	لا يتطلب إضافة في العنوان	أخضر

ملاحظات تنفيذية:

١- تُلزم جميع الجهات بالجامعة بوضع الأختام أو الملصقات على الوثائق الورقية فور تصنيفها.

٢- تُضاف العبارات النصية للتصنيف آليًا في أنظمة إدارة المستندات الإلكترونية كلما أمكن.

٣- في وسائل تداول وتخزين البيانات والمعلومات والوثائق، يتحمل المُرسل مسؤولية إدراج التصنيف في العنوان وفقًا لمستوى حساسية الرسالة.