جامعة حفر الباطن
University of Hafr Al Batin

مكتب إدارة البيانات
DATA MANAGEMENT OFFICE




سياسة مؤسسية

# سياسة إدارة المحتوى والوثائق

إطار إدارة المحتوى والوثائق في الجامعة طوال دورة حياتها

| الإصدار | تاريخ الإصدار | المراجعة القادمة | التصنيف |
|---|---|---|---|
| 1.0 | 2025-07-22 | 2027-07-20 | عام |

المملكة العربية السعودية، حفر الباطن · ص.ب 1803 · الرمز البريدي 31991
هاتف 013 7203426 · فاكس 013 7247212 · www.uhb.edu.sa

رؤية 2030 VISION
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

# ضبط الوثيقة

## تفاصيل الوثيقة

| | |
|---|---|
| **اسم الوثيقة** | سياسة إدارة المحتوى والوثائق |
| **المؤسسة** | جامعة حفر الباطن |
| **مالك الوثيقة** | وحدة حوكمة البيانات |
| **رقم الإصدار** | 1.0 |
| **الحالة** | إصدار |
| **تاريخ الإصدار** | 2025-07-22 |
| **تاريخ المراجعة القادمة** | 2027-07-20 |
| **تصنيف الوثيقة** | عام |

## جدول اعتماد الوثيقة

| الإصدار | التاريخ | التعديلات | تحرير | مراجعة | موافقة |
|---|---|---|---|---|---|
| 1.0 | 2025-07-20 | لا يوجد | **أمجاد حمدان العنزي** | **أ. صالح عامر العنزي**<br>مسؤول إتاحة البيانات | **أ.د. محمد متعب العتيبي**<br>المشرف على مكتب إدارة البيانات |

## الموافقات

| الاسم / الجهة | الوظيفة / رقم المحضر | التاريخ |
|---|---|---|
| **أ.د. محمد متعب العتيبي** | المشرف على مكتب إدارة البيانات | 2025-07-22 |
| **اللجنة التنفيذية الدائمة لإدارة وحوكمة البيانات بالجامعة** | رقم المحضر: 2245-1-2002-2 | 1447-02-27 |
| **رقم قرار الاعتماد من لجنة المعاملات الإلكترونية** | رقم المحضر: 2251-1-1232-1 | 1447-03-26 |

## سجل الإصدارات

| رقم الإصدار | تاريخ المراجعة | المساهم | التعديل |
|---|---|---|---|
| 1 | 2025-07-22 | مكتب إدارة البيانات | الإصدار الأول |

# المحتوى


جدول التعريفات ..... 4

أولًا المقدمة ..... 5

ثانيًا المبادئ الرئيسية لإدارة المحتوى والوثائق ..... 6

ثالثًا بيان السياسة ..... 6

رابعًا الأدوار والمسؤوليات ..... 10

السياسات المرتبطة ..... 10

بيانات التواصل ..... 11

المراجع ..... 11

# جدول التعريفات

| المصطلح | التعريف |
|---|---|
| **المحتوى** | جميع المعلومات والمواد الرقمية أو غير الرقمية التي تنتجها أو تستقبلها الجامعة أثناء أداء مهامها، بما يشمل المستندات والسجلات والوسائط بمختلف أنواعها. |
| **الوثائق** | السجلات الرسمية التي تحتوي على معلومات مُعتمدة وموثقة تُستخدم كمرجع في الإجراءات والقرارات الإدارية والأكاديمية داخل الجامعة. |
| **دورة حياة المحتوى** | المراحل التي يمر بها المحتوى أو الوثيقة منذ إنشائها أو استلامها وحتى أرشفتها أو إتلافها، وتشمل: الإنشاء، التخزين، الاستخدام، المشاركة، الأرشفة/الإتلاف. |
| **الأرشفة** | عملية حفظ المحتوى والوثائق لفترة زمنية محددة وفق ضوابط الجامعة بهدف الرجوع إليها عند الحاجة وضمان استمراريتها. |
| **الإتلاف** | التخلص الآمن من المحتوى أو الوثائق التي انتهت الحاجة إليها أو انتهت مدة حفظها المعتمدة، وفق الضوابط الأمنية والتنظيمية للجامعة. |
| **المستودع المركزي للمحتوى** | الجهة أو النظام المعتمد لحفظ وإدارة المحتوى والوثائق في الجامعة، بما يضمن التحكم والصلاحيات وسهولة الوصول. |
| **مستويات السرية** | تصنيفات الحساسية المعتمدة على محتوى الوثائق (عام، مقيد، سري، سري للغاية) لضمان الحماية الملائمة بحسب درجة المخاطر. |
| **المالك** | الجهة أو الفرد داخل الجامعة المسؤول عن المحتوى أو الوثيقة من حيث الدقة والاستخدام والتحديث والامتثال للضوابط. |
| **المستخدم المصرح** | أي فرد داخل الجامعة مُخول بالوصول إلى المحتوى أو الوثائق واستخدامها لأغراض العمل فقط. |
| **الضوابط** | التعليمات والمعايير الواجب الالتزام بها خلال إدارة المحتوى والوثائق لضمان جودتها وسريتها وتوافرها. |

أولًا

# المقدمة

تُعد إدارة دورة حياة المحتوى والوثائق من الركائز الأساسية لتعزيز حوكمة المعلومات وضمان حماية المعرفة المؤسسية واستمراريتها. وحرصًا من الجامعة على رفع مستوى النضج التنظيمي في إدارة المحتوى، جاءت هذه السياسة لتحديد المبادئ والإجراءات التي تكفل التعامل مع المحتوى والوثائق خلال مختلف مراحلها بدءًا من الإنشاء أو الاستلام ثم التخزين والاستخدام والمشاركة، وصولًا إلى الأرشفة أو الإتلاف، وفق منهجية واضحة وضوابط معتمدة تضمن السرية والجودة والتوافر وسهولة الوصول.

## 1.1 الغرض من الوثيقة

تهدف هذه السياسة إلى وضع إطار موحد لإدارة المحتوى والوثائق في الجامعة، بما يضمن الحوكمة الفعالة والامتثال للمتطلبات التنظيمية، وسهولة الوصول، والحفاظ على البيانات والمعلومات وتنظيم تداولها.

## 1.2 نطاق عمل السياسة وتطبيقها

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها الجامعة مهما كان مصدرها، أو شكلها أو طبيعتها ويشمل ذلك الوثائق والسجلات الورقية، الاجتماعات، الاتصالات عبر وسائل التواصل والتطبيقات، رسائل البريد الالكتروني، البيانات المخزنة على وسائط إلكترونية، أشرطة الصوت أو الفيديو، الخرائط، الصور، المخطوطات، أو أي شكل آخر من أشكال البيانات المسجلة. تتلاءم هذه السياسة مع ضوابط ومواصفات إدارة البيانات وحوكمتها وحماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية – الإصدار 1.5 في يناير 2021م، والمتطلبات التنظيمية والتشريعية ذات العلاقة، وبما يتعارض مع الأنظمة المرعية وما يصدر بشأنها من تعديلات. وتنطبق هذه السياسة على جميع العاملين في الجامعة ....، والأطراف الخارجية وفق العلاقات التعاقدية.

## 1.3 جدول مراجعة السياسة

يجب مراجعة هذه السياسة بشكل منتظم بحيث تكون هذه المراجعة مرة واحدة سنويًا على أقل تقدير وفقًا لما يوجه به المشرف العام على السياسة ويطلب من مكتب إدارة البيانات داخل الجامعة.

## 1.4 مراقبة الامتثال

يقاس الامتثال لسياسة دورة حياة إدارة المحتوى والوثائق وفقًا لمعايير ومؤشرات الأداء الموضوعة من مكتب إدارة البيانات في الجامعة وبالتوافق مع متطلبات مكتب إدارة البيانات الوطنية، ويتم مراجعة معايير الامتثال بشكل دوري من قبل مدير مكتب إدارة البيانات.

ثانيًا

# المبادئ الرئيسية لإدارة المحتوى والوثائق

تعتمد الجامعة على المبادئ التالية في إدارة المحتوى والوثائق:

### 1 المبدأ الأول: التوافر وسهولة الوصول

ضمان سهولة استرجاع الوثائق والمستندات والوصول لها عند الحاجة ووفقًا للصلاحيات الممنوحة.

### 2 المبدأ الثاني: الامتثال

الالتزام بالقوانين واللوائح ذات العلاقة المعمول بها، وبما ورد في وثيقة ضوابط ومواصفات إدارة البيانات وحوكمتها وحماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية.

### 3 المبدأ الثالث: التحديث والدقة

أن تكون الوثائق محدثة ودقيقة مع تقليل التكرار غير الضروري.

### 4 المبدأ الرابع: الأمان والخصوصية

ضمان حماية الوثائق من الوصول غير المصرح به وذلك من خلال تحديد المخولين بالاطلاع عليها بعد القيام بالإجراءات اللازمة للتأكد من موثوقيتهم (إن تطلب الأمر ذلك، حسب طبيعة ومستوى تصنيفها ودرجة حساسيتها وفقًا لسياسة تصنيف البيانات)، وتطبيق الضوابط الأمنية المناسبة لحماية البيانات وفقًا للمتطلبات التنظيمية ذوات العلاقة، ووفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني، بالإضافة إلى الحفاظ عليها من الفقدان أو التلف.

ثالثًا

# بيان السياسة

## اصطلاحات تسمية الوثائق المستخدمة

للوصول إلى الوثائق واسترجاعها بسهولة، يتم اتباع ما يلي عند تسميتها:

- يجب أن تعكس أسماء الوثائق والمستندات والمجلدات محتواها بطريقة واضحة ومنتظمة.
- يتم وضع البيانات الوصفية المناسبة للوثائق والتي تستخدم في قوائم الوثائق مع تحديد الحقول التي تتكون منها (مثال ذلك: اسم الوثيقة، نسخة الوثيقة، وصف الوثيقة، فئة الحفظ، مكان الحفظ، بداية الحفظ، مدة الحفظ ...)

- يجب اتباع نسق معياري موحد عند تسمية الوثيقة، والذي يتكون من:
  - تاريخ إنشاء الملف أو تعديله
  - الاسم المختصر للإدارة أو القسم
  - رقم الملف
  - رقم النسخة
- يجب استخدام ترويسة الملف المعتمدة مع تحديد نوع النسخة (معتمدة – أولية – محدثة – ملغاة).

## تحديد مستويات التصنيف للوثائق

تعد عملية تحديد مستوى تصنيف الوثائق من الإجراءات المهمة التي من شأنها المحافظة عليها وتحديد مستوى الحماية المناسبة لها في التعامل معها، وتشير مستويات تصنيف البيانات إلى درجات مختلفة من الحساسية والأهمية وتشمل أربع مستويات رئيسية بناء على درجة الضرر أو الأثر الذي قد ينتج عن الوصول غير المصرح به إليها أو الإفصاح عنها.

مستويات تصنيف البيانات وفقًا لسياسة تصنيف البيانات المعتمدة بالجامعة كما يلي:

| مستوى التصنيف | درجة الأثر | الوصف |
|---|---|---|
| سري للغاية | عالي | تُصنف البيانات على أنها "بيانات سرية للغاية"، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى حدوث أضرار جسيمة أو خطيرة للغاية على المدى الطويل لا يمكن تداركها أو إصلاحها. |
| سري | متوسط | تُصنف البيانات على أنها "بيانات سرية"، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى حدوث أضرار جسيمة أو خطيرة يصعب السيطرة عليها أو تداركها على المدى القصير. |
| مقيد | منخفض | تُصنف البيانات على أنها "مقيّدة"، إذا كان الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها يؤدي إلى أضرار محدودة يمكن السيطرة عليها أو أضرار متقطعة على المدى القصير يمكن السيطرة عليها. |
| عام | لا يوجد | تُصنف البيانات على أنها "بيانات عامة" عندما لا يترتب على الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها أو عن محتواها أي ضرر على المدى الطويل أو القصير. |

وتصنف الوثائق من حيث مدة تخزينها والاحتفاظ بها إلى نوعين:

- وثائق دائمة الحفظ
- وثائق مؤقتة الحفظ

**وثائق دائمة الحفظ:** هي الوثائق التي يلزم الاحتفاظ الدائم بها ويتم الرجوع إليها لفترات طويلة، كما يؤثر إتلافها على إتاحتها وتوفر معلوماتها.

ومن ذلك على سبيل المثال لا الحصر:

- أ- الوثائق التي تثبت أملاك الدولة الخاصة.
- ب- الوثائق التي تحفظ حقوق الدولة الطبيعية والقانونية الدائمة تجاه الدول والأشخاص.
- ج- الوثائق التي تؤرخ وتدعم أنشطة الجامعة ... وترصد تطورها الوظيفي والإداري مثل:
  - أنظمتها ولوائحها الداخلية
  - قراراتها التنظيمية
  - سياساتها وخططها وبرامجها
  - ميزانياتها وحساباتها الختامية
  - إجراءاتها الإدارية
  - تنظيماتها الإدارية وأدلتها التنظيمية
  - التقارير المهمة
  - الاحصائيات
  - مخططاتها المعمارية وتصاميمها الهندسية ومواصفاتها
- د- مخططات ومواصفات المرافق العامة.
- ه- الاحكام القضائية.

**الوثائق مؤقتة الحفظ:** هي الوثائق التي تستخدم في فترات متقاربة ويجب الاحتفاظ بها في فترات زمنية من سنة إلى 20 سنة في الغالب، والتي يُحتمل الرجوع إليها لفترات محددة، كما يؤثر إتلافها مبكرًا على إتاحتها وتوفر معلوماتها، ومنها على سبيل المثال لا الحصر: بيانات الخطط والمشاريع التنفيذية، محاضر الاجتماعات، البيانات التشغيلية.

## الموافقة على إتاحة الوصول للوثائق

وفقًا لما ورد في لائحة الاطلاع على الوثائق والمحفوظات وتداولها الصادرة عن المركز الوطني للوثائق والمحفوظات بتاريخ 1421هـ، تنقسم الوثائق لأغراض الوصول والاطلاع عليها إلى فئتين:

- الفئة الأولى: وثائق يجوز الاطلاع عليها وتداولها، وهي الوثائق التي تتعلق بموضوعات عامة غير مقيدة أو سرية تم نشرها أو إبلاغها للجهات والأشخاص الاعتباريين أو الطبيعيين. ومن هذه الوثائق على سبيل المثال لا الحصر: الأنظمة واللوائح والسياسات والخطط والبرامج والميزانيات والإحصاءات والأبحاث والدراسات والتقارير الإحصائية.
- الفئة الثانية: وثائق يحظر نشرها أو الاطلاع عليها أو تداولها لغير الموظفين المختصين إلا بموافقة صاحب الصلاحية بحكم سريتها أو حساسيتها أو أنه ليس من المصلحة الاطلاع عليها أو نشرها.

يجوز الموافقة على اطلاع الباحثين والدارسين على الوثائق السرية وفقًا للضوابط التالية:

- أن تكون هذه الوثائق والمحفوظات محتوية على بيانات أو معلومات صالحة للبحوث والدراسات في الموضوعات المراد بحثها، مما يثري البحث العلمي ويساعد على التغلب على الآثار السلبية للقضايا المدروسة.
- إزالة أسماء الأشخاص الواردة في صور الوثائق والمحفوظات التي يزود بها الباحثين والدارسين قبل تمكينهم من الاطلاع عليها.
- أن تكون مدة حظر الوثيقة – ذات الحظر المؤقت – قد انتهت.
- أن يكون الباحث أو الدارس ممن يعرف له مكانه العلمي في مجال بحثه، أو يحضر خطابًا من الجهة المشرفة على بحثه أو الجهة التي يتبع لها.
- أن يشار في مصادر البحث إلى هذه الوثائق ومكان وجودها.
- أن يزود المركز الوطني للوثائق والمحفوظات بثلاث نسخ من هذا البحث ليتم إيداعها في مكتبته.

يتم الالتزام بعملية واضحة لمنح الموظفين صلاحية الوصول إلى الوثائق. وعلى العملية أن تطبق نظامًا للوصول إليها قائمًا على الاختصاصات والأدوار والمسؤوليات وحاجة العمل، ووفقًا لسياسة هويات إدارة الدخول والصلاحيات الصادرة من إدارة الأمن السيبراني والسياسات الأمنية المتعلقة بذلك والإجراءات المطبقة في عمادة التعليم الالكتروني والتحول الرقمي بالجامعة والجهات ذات الاختصاص.

## النسخ/ التخزين الاحتياطي واسترجاع الوثائق

وفقًا لسياسة التخزين والاستبقاء بالجامعة، يتم اتباع ما يلي:

- يجب إنشاء نسخ احتياطية لجميع الوثائق والملفات والمحفوظات، ويعتبر مسؤولي النظام ومركز البيانات في قسم مركز البيانات مسؤولين عن نسخ الوثائق وأخذ صور من النظام احتياطيًا، باستخدام الأنظمة المناسبة للنسخ الاحتياطي والبرامج الخاصة بمركز البيانات الحساسة بشكل يومي وكذلك اخذ نسخ احتياطي تزايدي لأي تغييرات طارئة على قاعدة البيانات بشكل يومي ونسخ احتياطي كامل للأنظمة بشكل أسبوعي، على أن تخزن (تحفظ البيانات في وحدة تخزين أخرى وتحفظ كنسخة احتياطية دون أن يكون لها أي اتصال بالإنترنت).
- يجب أن يستخدم الموقع الخاص بمركز التعافي من الكوارث DR لمزامنة النسخة الاحتياطية معه ويعتبر بمثابة نسخة احتياطية محفوظة خارج الموقع.
- يجب تشفير النسخ الاحتياطي من خلال أي نظام تشفير لدى إدارة تقنية المعلومات في الجامعة، قد ترى أنه الأنسب لعملية تشفير النسخ الاحتياطية للبيانات وبما يتوافق مع سياسة الامن السيبراني للتشفير.
- يجب إنشاء سجلات عملية النسخ الاحتياطي تلقائيًا على الأنظمة التي يتم فيها عمل النسخة الاحتياطية.
- يجب التأكد من القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.
- يجب إجراء فحص دوري كل ثلاثة أشهر للأنظمة الحساسة وكل ستة أشهر للأنظمة الأخرى للتحقق من مدى فعالية استعادة النسخ الاحتياطية.

### الاستبقاء والتخلص

- يتم إتلاف الوثائق بعد انتهاء فترة حفظها بطريقة آمنة تمنع الوصول لها أو استخدامها – وتشمل البيانات التشغيلية والمؤرشفة والنسخ الاحتياطية – وذلك وفقًا لما يصدر من إدارة الأمن السيبراني بالجامعة.
- يتم إتلاف الوثائق بعد الحصول على الموافقات اللازمة وعلى النحو الملائم لنوعها، ومدة الاحتفاظ بها، ومدى حساسيتها، واستخداماتها المستقبلية.
- يتم إتلاف ملفات البيانات الشخصية بعد انتهاء فترة الاحتفاظ بها، ويمكن الاحتفاظ بها دون إتلافها إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد وفق سياسة حماية البيانات الشخصية.
- يجب عدم إتلاف الوثائق دائمة الحفظ، أو البيانات التي يتعارض إتلافها مع متطلبات تنظيمية أو قانونية.
- تتم عمليات الإتلاف وفق جدول زمني يحدده مركز الوثائق والمحفوظات.
- تُسجل بشكل تفصيلي جميع الوثائق التي تم التخلص منها ويتم الاحتفاظ بهذا السجل حفظًا دائمًا.

رابعًا

## الأدوار والمسؤوليات

| | |
|---|---|
| 1 | راعي ومالك وثيقة السياسة: مكتب إدارة البيانات |
| 2 | مراجعة السياسة وتحديثها: مكتب إدارة البيانات |

**تنفيذ السياسة وتطبيقها:** مركز الوثائق والمحفوظات، والإدارة

## السياسات المرتبطة

- سياسة حماية البيانات الشخصية بجامعة حفر الباطن
- سياسة تصنيف البيانات بجامعة حفر الباطن
- سياسة الوصول إلى البيانات بجامعة حفر الباطن
- سياسة مشاركة البيانات بجامعة حفر الباطن
- سياسة حرية المعلومات بجامعة حفر الباطن
- سياسة خصوصية واستخدام البيانات بجامعة حفر الباطن
- سياسة الحذف والتخزين والاستبقاء بجامعة حفر الباطن
- سياسة الامتثال والتدقيق بجامعة حفر الباطن

# بيانات التواصل

مكتب إدارة البيانات dmo@uhb.edu.sa

# المراجع

1 سياسة التخزين والاستبقاء بجامعة حفر الباطن