



اسم الوثيقة	الدليل الإجرائي لإدارة وحماية بيانات الطلبة
نوع الوثيقة	دليل اجرائي
رمز الوثيقة	AUB-GUIDE-512
تاريخ الإصدار	2026 / 06 /22
الإصدار	V1.0
الفترة الزمنية للخطة	خمس سنوات
الجهة المالكة	قسم شؤون الطلبة
الجهة المنفذة	تشكيلات الجامعة
المراجعة	قسم ضمان الجودة
الاعتماد	موثقة ومعتمدة
الموقع الرسمي	http://abu.edu.iq/ar

مصادقة رئيس الجامعة:



الدليل الإجرائي لإدارة وحماية بيانات الطلبة

تولي جامعة أهل البيت عليهم السلام أهمية كبيرة لحماية بيانات الطلبة وضمان سريتها وسلامتها، باعتبارها من الأصول المعلوماتية الحساسة التي تتطلب إدارة دقيقة وأمنة. ويأتي هذا الدليل الإجرائي لتنظيم آليات جمع البيانات وتخزينها ومعالجتها والوصول إليها، بما يضمن حماية الخصوصية والامتثال للمعايير الأكاديمية والأمنية والتشريعات ذات الصلة.

أولاً: الهدف من الدليل

1. ضمان حماية بيانات الطلبة من الوصول غير المصرح به .
2. تنظيم آليات إدارة وتخزين البيانات الأكاديمية .
3. تحديد صلاحيات الوصول وفق الهيكل الإداري .
4. تعزيز أمن المعلومات داخل الجامعة .



5. ضمان دقة وسلامة البيانات واستمراريتها .

6. الامتثال لمعايير الجودة والحوكمة الرقمية .

ثانياً: نطاق التطبيق

يُطبق هذا الدليل على جميع بيانات الطلبة في الجامعة، ويشمل:

- البيانات الشخصية .
- البيانات الأكاديمية .
- السجلات المالية .
- بيانات التسجيل والقبول .
- بيانات الأنظمة الإلكترونية والمنصات التعليمية .



ثالثاً: مبادئ إدارة وحماية البيانات

1. السرية. (Confidentiality)
2. سلامة البيانات. (Integrity)
3. إتاحة البيانات المصرح بها. (Availability)
4. الحد الأدنى من الصلاحيات. (Least Privilege)
5. المساءلة وتتبع العمليات .
6. الامتثال للأنظمة والتعليمات النافذة .

رابعاً: تصنيف بيانات الطلبة

1- بيانات عامة

- الاسم، الرقم الجامعي، التخصص، المرحلة الدراسية .



2- بيانات حساسة

- العنوان، رقم الهاتف، البريد الإلكتروني .

3- بيانات سرية

- السجل الأكاديمي الكامل .
- البيانات المالية .
- نتائج الامتحانات والتقارير الداخلية .

خامساً: آليات جمع وتخزين البيانات

1. جمع البيانات من خلال استمارات رسمية معتمدة .
2. إدخال البيانات عبر أنظمة إلكترونية مركزية .
3. حفظ البيانات في قواعد بيانات مؤمنة .



4. إجراء نسخ احتياطية دورية. (Backup)

5. تحديث البيانات بشكل مستمر من قبل الجهات المخولة.

سادساً: آليات الوصول إلى البيانات والصلاحيات

1- مبدأ تحديد الصلاحيات

- يمنح الوصول للبيانات حسب الحاجة الوظيفية فقط .
- يمنع الوصول غير المصرح به لأي مستوى من البيانات .

2- مستويات الصلاحية

أ. رئاسة الجامعة

- صلاحية الاطلاع على التقارير الإجمالية .



ب. عمادات الكليات

- الاطلاع على بيانات الطلبة ضمن الكلية فقط .

ج. الأقسام العلمية

- الوصول إلى البيانات الأكاديمية للطلبة في القسم .

د. شعبة التسجيل

- إدخال وتحديث البيانات الأساسية .

3- صلاحيات الأنظمة الإلكترونية

- إنشاء حسابات مستخدمين بصلاحيات محددة .
- استخدام أسماء مستخدمين وكلمات مرور آمنة .
- تسجيل الدخول والخروج بشكل موثق .



سابعاً: حماية البيانات الإلكترونية

1. استخدام أنظمة حماية (Firewalls / Antivirus).

2. تشفير البيانات الحساسة .

3. تحديث الأنظمة بشكل دوري .

4. مراقبة الدخول غير المصرح به .

5. منع استخدام الأجهزة غير الموثوقة .

ثامناً: مشاركة البيانات

• لا يجوز مشاركة بيانات الطلبة إلا بموافقة رسمية .

• تتم مشاركة البيانات عبر قنوات مؤمنة فقط .

• يمنع إرسال البيانات عبر وسائل غير رسمية .



تاسعاً: التوثيق والتدقيق

1. تسجيل جميع عمليات الدخول والتعديل .
2. إعداد سجلات تدقيق دورية .
3. مراجعة الصلاحيات بشكل نصف سنوي .
4. التحقق من الالتزام بسياسات الحماية .

عاشراً: المخالفات والإجراءات التصحيحية

- أي خرق لسياسة حماية البيانات يعرض مرتكبه للمساءلة القانونية والإدارية .
- يتم التحقيق في أي حادثة أمنية فوراً .
- اتخاذ إجراءات تصحيحية لمنع تكرار الحادثة .

Ahl Al-Bayt University

**Central Supreme Committee for
Institutional Accreditation**

**Towards Fourth Generation
University: Quality, Technology,
Leadership, Innovation, and Excellence**



جامعة أهل البيت (ع)

**اللجنة المركزية العليا للاعتماد
المؤسسي**

**نحو جامعة الجيل الرابع: جودة،
تكنولوجيا، ريادة، ابتكار والتميز**

الخاتمة

يمثل هذا الدليل الإجرائي إطاراً مؤسسياً متكاملًا لإدارة وحماية بيانات الطلبة في جامعة أهل البيت عليهم السلام، ويهدف إلى ضمان سرية المعلومات ودقتها وسلامتها، وتنظيم صلاحيات الوصول إليها بما يعزز الثقة والحوكمة الرقمية ويدعم بيئة أكاديمية آمنة وفعّالة.