

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

اسم الوثيقة	سياسة أمن المعلومات وحماية البيانات
نوع الوثيقة	سياسة
رمز الوثيقة	AUB-POLICY
تاريخ الإصدار	2026 / 04 / 18
الإصدار	V1.0
الفترة الزمنية للخطة	خمس سنوات
الجهة المالكة	رئاسة الجامعة
الجهة المنفذة	تشكيلات الجامعة
المراجعة	قسم ضمان الجودة / اللجنة المختصة
الاعتماد	موثقة ومعتمدة
الموقع الرسمي	http://abu.edu.iq/ar

مصادقة رئيس الجامعة:



سياسة أمن المعلومات وحماية البيانات

المقدمة

تلتزم جامعة أهل البيت عليهم السلام بحماية أصولها المعلوماتية وضمان سرية وسلامة وتوافر البيانات، بوصفها ركيزة أساسية لدعم العملية التعليمية والبحثية والإدارية. ومع التوسع في التحول الرقمي واستخدام الأنظمة الإلكترونية، تزداد أهمية تبني إطار مؤسسي متكامل لأمن المعلومات يحد من المخاطر السيبرانية ويحافظ على خصوصية البيانات.

وانطلاقاً من ذلك، تم إعداد هذه السياسة لتحديد الضوابط والمعايير والإجراءات اللازمة لحماية المعلومات والبيانات في جميع وحدات الجامعة، بما يضمن الامتثال للأنظمة المعتمدة وتعزيز الثقة في البيئة الرقمية المؤسسية



أولاً: الغرض من السياسة

تهدف هذه السياسة إلى حماية المعلومات والبيانات من الوصول غير المصرح به أو التلاعب أو فقدان، وضمان استمرارية الأعمال، وتعزيز أمن الأنظمة الرقمية في الجامعة.

ثانياً: نطاق التطبيق

تُطبق هذه السياسة على جميع منتسبي الجامعة (التدريسيين، الإداريين، العاملين، والطلبة) وعلى جميع الأنظمة الإلكترونية، وقواعد البيانات، والأجهزة، والشبكات المستخدمة داخل الجامعة أو المرتبطة بها.

ثالثاً: مبادئ السياسة

1. السرية: حماية المعلومات من الوصول غير المصرح به .



2. السلامة: ضمان دقة البيانات وعدم التلاعب بها .
3. التوافر: ضمان توفر المعلومات عند الحاجة .
4. المساءلة: تحديد المسؤوليات بوضوح .
5. الامتثال: الالتزام بالقوانين والتعليمات ذات العلاقة .
6. التحسين المستمر: تطوير أنظمة الحماية بشكل دوري .

رابعاً: تصنيف المعلومات

1. معلومات عامة: متاحة للنشر .
2. معلومات داخلية: للاستخدام المؤسسي فقط .
3. معلومات سرية: تتطلب حماية خاصة .



4. معلومات شديدة الحساسية: ذات مستوى عالٍ من الحماية (مثل البيانات الشخصية والمالية).

خامساً: ضوابط أمن المعلومات

1- إدارة الوصول

• منح الصلاحيات وفق الحاجة الوظيفية

• استخدام أنظمة المصادقة (كلمات مرور قوية، تحقق متعدد العوامل).

• مراجعة الصلاحيات بشكل دوري.

2- حماية الأنظمة والشبكات

• استخدام برامج الحماية من الفيروسات والاختراق.



• تحديث الأنظمة بشكل مستمر.

• تأمين الشبكات الداخلية والخارجية.

3- حماية البيانات

• تشفير البيانات الحساسة.

• النسخ الاحتياطي الدوري.

• منع نقل البيانات دون تصريح.

4- أمن الأجهزة

• حماية الأجهزة بكلمات مرور.

• منع استخدام الأجهزة غير المصرح بها.

• تأمين الأجهزة المحمولة.



5-الاستخدام المقبول

- استخدام الأنظمة لأغراض العمل فقط.
- منع تحميل البرامج غير المعتمدة.
- الالتزام بسياسات الاستخدام الإلكتروني.

سادساً: إدارة المخاطر الأمنية

1. تحديد المخاطر المحتملة .
2. تقييم مستوى الخطورة .
3. وضع خطط للتقليل من المخاطر .
4. مراجعة دورية للمخاطر .



سابعاً: الاستجابة للحوادث الأمنية

1. الإبلاغ الفوري عن أي حادث أمني .
2. تشكيل فريق للاستجابة للحوادث .
3. احتواء الحادث وتقليل الأضرار .
4. التحقيق وتحليل الأسباب .
5. اتخاذ إجراءات تصحيحية ومنع التكرار .

ثامناً: التوعية والتدريب

1. تنظيم برامج تدريبية لأمن المعلومات .
2. نشر ثقافة الأمن السيبراني .
3. توعية المستخدمين بالمخاطر الإلكترونية .



تاسعاً: المتابعة والتدقيق

1. إجراء تدقيق دوري على الأنظمة .
2. تقييم مستوى الامتثال للسياسة .
3. إعداد تقارير أمنية دورية .
4. تحديث السياسة وفق المستجدات .
5. نعتبر هذه السياسة سارية المفعول على ان لا تتعارض مع القوانين والتعليمات النافذة

عاشراً: المسؤوليات

- مجلس الجامعة :اعتماد السياسة والإشراف العام .
- رئاسة الجامعة :دعم تنفيذ السياسة .



. قسم الحاسبة الالكترونية :تنفيذ إجراءات الأمن السيبراني .

. قسم ضمان الجودة :متابعة الالتزام والتقييم .

. جميع المستخدمين :الالتزام بتطبيق السياسة .

الخاتمة

تمثل هذه السياسة إطاراً متكاملًا لحماية المعلومات والبيانات في جامعة أهل البيت عليهم السلام، بما يعزز أمن البيئة الرقمية ويضمن استمرارية الأعمال، ويرفع مستوى الثقة في الأنظمة المؤسسية، ويدعم تحقيق الأهداف الاستراتيجية للجامعة في ظل التحول الرقمي المتسارع.