



شروط الاستخدام



جدول المحتويات

الهدف.....	3
نطاق المسؤولية وقابلية التطبيق.....	3
شروط الاستخدام.....	4
الإستفسارات والشكاوى وبيانات التواصل.....	6

الهدف:

تهدف شروط الاستخدام هذه الى توضيح سياسة الاستخدام الصحيح للموقع الإلكتروني، البريد الإلكتروني والخدمات الإلكترونية. يأتي ذلك ايضا ضمن السعي الى تقليل المخاطر السيبرانية المتعلقة باستخدام أنظمة الجامعة الإسلامية وأصولها، وحمايتها من التهديدات الخارجية والداخلية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

نطاق العمل وقابلية الاستخدام:

تغطي هذه الشروط سياسة الاستخدام الصحيح للموقع الإلكتروني، البريد الإلكتروني والخدمات الإلكترونية وتنطبق على جميع منسوبي الجامعة الإسلامية.

1. البنود العامة

- 1.1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بالجامعة الإسلامية بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها
- 1.2 يحضر انتهاك حقوق أي شخص أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى أو قوانين أو لوائح مماثلة؛ بما في ذلك؛ على سبيل المثال لا الحصر، تثبيت برامج غير مصرحة أو غير قانونية
- 1.3 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة مرور الخاصة بمدير المستخدم أو مسؤوليه
- 1.4 يمنع نشر معلومات تخص الجامعة الإسلامية عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون إذن مسبق.
- 1.5 يمنع استخدام أنظمة الجامعة و أصولها بغرض تحقيق منفعة شخصية أو أعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجامعة
- 1.6 يمنع القيام بأي أنشطة تهدف الى تجاوز أنظمة الحماية الخاصة بالجامعة بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على إذن مسبق، وبما يتوافق مع الإجراءات المعتمدة داخل الجامعة
- 1.8 يجب إبلاغ إدارة الأمن السيبراني في حال فقدان المعلومات أو تسريبها أو سرقتها

2. حماية أجهزة الحاسب الآلي

- 2.1 يمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة وسلامتها دون الحصول على إذن مسبق من إدارة الأمن السيبراني بما في ذلك الأنشطة التي تمكن المستخدم من الحصول على إمتيازات وصلاحيات أعلى

3. استخدام الإنترنت والبرمجيات

- 3.1 يجب إبلاغ إدارة الأمن السيبراني في حال وجود أي مواقع مشبوهة ينبغي حجبها؛ أو العكس
- 3.2 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل
- 3.3 يمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية
- 3.4 يجب استخدام متصفح أمن ومصرح به للوصول الى الشبكة الداخلية أو شبكة الإنترنت
- 3.5 يمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول الى شبكة الإنترنت
- 3.6 يجب تبليغ إدارة الامن السيبراني عند الإشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.
- 3.7 عند استخدامك لهذا الموقع يمنع إجراء فحص أمني لغرض إكتشاف الثغرات الأمنية، ويشمل ذلك إختبار الإختراقات، أو مراقبة شبكات الجامعة الإسلامية و أنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني
- 3.8 يمنع استخدام مواقع مشاركة الملفات دون الحصول على إذن مسبق من إدارة الأمن السيبراني

4. استخدام البريد الإلكتروني ونظام الإتصالات

- 4.1 يمنع استخدام البريد الإلكتروني في أغراض غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييرها
- 4.2 يمنع تداول رسائل تحتوي على محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية و الخارجية.
- 4.3 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الإتصالات
- 4.4 يجب عدم تسجيل البريد الإلكتروني الخاص بالجامعة الإسلامية في أي موقع ليس له علاقة بالعمل
- 4.5 يجب تبليغ إدارة الأمن السيبراني عند الإشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار على أنظمة الجامعة
- 4.6 تحتفظ الجامعة الإسلامية بالحق في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقا للإجراءات والتنظيمات ذات العلاقة
- 4.7 يمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى إن كانت تبدو من مصادر موثوقة

5. استخدام كلمات المرور

- 5.1 يجب إختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الجامعة الإسلامية وأصولها، كما يجب إختيار كلمات مرور مختلفة عن كلمات المرور الحسابات الشخصية، مثل حسابات البريد الشخصي وحسابات التواصل الإجتماعي
- 5.2 يمنع مشاركة كلمات المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والإتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف أآر بما في ذلك زملاء العمل وموظفوا عمادة تقنية المعلومات
- 5.3 يجب تغيير كلمة المرور: عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام

الإستفسارات والشكاوى وبيانات التواصل:

في حال وجود أي استفسار أو شكوى أو طلب فيما يخص حقوقك المتعلقة بمعالجة بياناتك الشخصية أو حول ما ورد في سياسة الإستخدام المقبول بشكل عام, يمكنك التواصل مع إدارة الأمن السيبراني في الجامعة الإسلامية عبر قنوات التواصل التالية:
القسم المختص: الجامعة الإسلامية - إدارة الأمن السيبراني
العنوان: الجامعة الإسلامية - المدينة المنورة, ص. ب. (170)
رقم الهاتف: 920022042
البريد الإلكتروني: contact@iu.edu.sa تحويلة : 8333