الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

SEU/PRS/PL01/Ed.01/V.1

سياسة الاستخدام المقبول للأصول

2022/8

دليل سياسات وإجراءات الجامعة السعودية الإلكترونية

إدارة الأمن السيبراني

نسخة	تاريخ	المالك	ملاحظات	الحالة
1.0		إدارة الأمن السيبراني		ساري المفعول

	المسؤول	التاريخ	التوقيع
التطوير	منصور الشغاثرة	2022/8/21	
المراجعة	د. حمدان الزهراني	2022/8/22	
المصادقة			
الاعتماد	أ.د ليلك الصفدي		

1 مقدمة

1-1 الهدف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة الجامعة السعودية الإلكترونية وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

1-2 النطاق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بالجامعة السعودية الإلكترونية وتنطبق على جميع العاملين في الجامعة السعودية الإلكترونية.

2 عناصر السياسة:

2-1 البنود العامة

2-1-1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بالجامعة السعودية الإلكترونية بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

2-1-2 يحظر 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 مصرح بها أو غير قانونية.

2-1-3 يجب استخدام الطابعات للأغراض الرسمية فقط وعدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

2-1-4 يجب تأمين جميع وسائط التخزين بشكل آمن وملائم ، وحفظها في مكان معزول وآمن ، والتأكد من ضبط درجة الحرارة بدرجة معينة لا تؤثر على حفظها ، وحفظ وسائط التخزين الغير مستخدمة والتي تحتوي على معلومات وبيانات خاصة بالجامعة في أدراج أو خزائن مغلقة.

2-1-5 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

2-1-6 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

2-1-7 يمنع الإفصاح عن أي معلومات تخص الجامعة السعودية الإلكترونية، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

2-1-8 يمنع نشر معلومات تخص الجامعة السعودية الإلكترونية عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح وموافقة مسبقة.

2-1-9 يُمنع استخدام أنظمة الجامعة السعودية الإلكترونية وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجامعة السعودية الإلكترونية.

2-1-10 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بالجامعة السعودية الإلكترونية دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

2-1-11يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بالجامعة السعودية الإلكترونية، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى الجامعة السعودية الإلكترونية.

2-1-12 تحتفظ الجامعة السعودية الإلكترونية بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

2-1-13 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

2-1-14 يجب ارتداء البطاقة التعريفية في جميع مرافق الجامعة السعودية الإلكترونية.

2-1-15 يجب تبليغ إدارة الأمن السيبراني عند ملاحظة الأمور التالية:

- في حال فقدان المعلومات أو سرقتها أو تسريبها.
- في حال نشر معلومات خاصة بشكل غير رسمي أو في حال حدوث اختراق للملفات.
- الدخول غير المشروع إلى جميع أنظمة الجامعة سواءً كان للاطلاع أو لتعديل المحتويات.
- التنصت والالتقاط والاعتراض على المراسلات عن طريق شبكة وأجهزة الجامعة دون مسوغ نظامي.
- إعاقة الوصول لشبكة الجامعة أو إيقافها عن العمل بشكل غير نظامي.

- عند الاشتباه بوجود رسائل بريد إلكتروني مشبوهة بمحتوى قد يسبب الضرر لأنظمة الجامعة وأصولها المعلوماتية.

2-2 حماية أجهزة الحاسب الآلي بكافة أنواعها

2-2-1 يجب ضمان حماية الأجهزة ووسائط التخزين في جميع الأوقات وفي جميع الأماكن (المنزل، السيارة، المنزل، المكتب ،، إلخ)

2-2-2 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

2-2-3 يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من إدارة الأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

2-2-4 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

2-2-5 يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

2-2-6 يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات وتكنولوجيا التعليم.

2-2-7 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ الجامعة السعودية الإلكترونية أو أصولها.

2-2-8 يمنع إجراء أي تعديلات على الإعدادات الأمنية (مثل إعدادات كلمة المرور، قفل الشاشة، الجدار الناري، برنامج مكافحة الفيروسات ،، وغيرها من الإعدادات)

2-2-9 يجب الحصول على الإذن والموافقة من الإدارات المعنية بالجامعة عند نقل الأجهزة ووسائط التخزين التي تحتوي على معلومات تخص الجامعة قبل نقلها إلى أي موقع خارج الجامعة.

2-2-10 يجب الإبلاغ عن فقدان أو سرقة الأجهزة ووسائط التخزين فوراً.

2-3 الاستخدام المقبول للإنترنت والبرمجيات

2-3-1 يمنع استخدام شبكة و إنترنت الجامعة لمحاولة الدخول غير المصرح إلى أجهزة الحاسب أو المعلومات أو الخدمات.

2-3-2 يمنع استخدام أي مصدر آخر للإنترنت (مثل المودم الثابت أو مودم الجيل الثالث والرابع أو ماشابهها) غير ما يتم توفيره من قبل الجامعة في مواقع العمل.

2-3-3 يمنع القيام بأي أنشطة من الممكن أن تعرض شبكة الجامعة إلى أي مخاطر محتملة كالفيروسات والبرمجيات الخبيثة.

2-3-4 يجب إبلاغ إدارة الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

2-3-5 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

2-3-6 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

2-3-7 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

2-3-8 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو الخادم أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

2-3-9 يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول الجامعة السعودية الإلكترونية دون الحصول على تصريح مسبق من عمادة تقنية المعلومات وتكنولوجيا التعليم.

2-3-10 يمنع مشاهدة أو تنزيل محتوى غير ملائم (مواد مسيئة ، صور أو محتويات إباحية، أي تعليقات أخرى تؤدي إلى الإساءة إلى أي شخص)

2-3-11 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

2-3-12 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

2-3-13 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات الجامعة السعودية الإلكترونية وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

2-3-14 يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

2-3-15 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

2-4 الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

2-4-1 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

2-4-2 يمنع استخدام حسابات البريد الإلكتروني المجاني في المعاملات الرسمية أو للأغراض المتعلقة بالعمل (مثل قوقل ، ياهو ، هوتميل ، أو غيرها)

2-4-3 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

2-4-4 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

2-4-5 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالجامعة السعودية الإلكترونية في أي موقع ليس له علاقة بالعمل.

2-4-6 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة السعودية الإلكترونية أو أصولها.

2-4-7 تحتفظ الجامعة السعودية الإلكترونية بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

2-4-8 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

2-5 الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

2-5-1 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

2-5-2 يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

2-6 استخدام كلمات المرور

2-6-1 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الجامعة السعودية الإلكترونية وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

2-6-2 يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف

عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو عمادة تقنية المعلومات وتكنولوجيا التعليم.

3-6-2 يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

الأدوار والمسؤوليات

(أ) راعي ومالك وثيقة السياسة: إدارة الأمن السيبراني.

(ب)مراجعة السياسة وتحديثها: إدارة الأمن السيبراني.

(ج) تنفيذ السياسة وتطبيقها: عمادة الموارد البشرية وجميع العاملين.

الالتزام بالسياسة

1- يجب على مدير إدارة الأمن السيبراني ضمان التزام الجامعة السعودية الإلكترونية بهذه السياسة بشكل دوري.
2- يجب على جميع العاملين في الجامعة السعودية الإلكترونية الالتزام بهذه السياسة.
3- قد يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في الجامعة السعودية الإلكترونية.