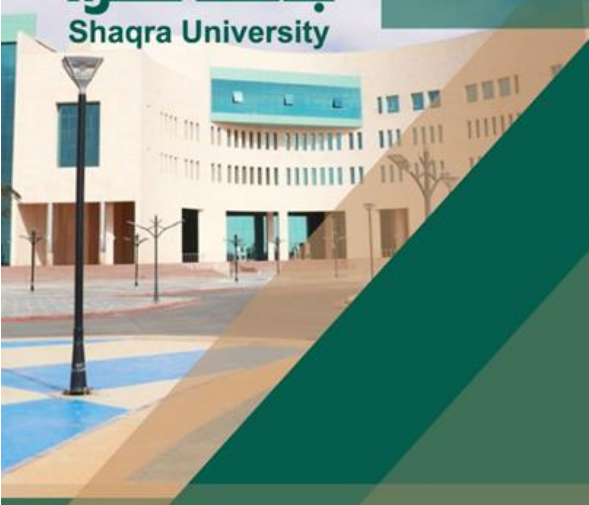
جامعة شقراء
Shaqra University

إدارة الأمن السيبراني
Cyber Security Department



الاستخدام المقبول للأصول

رمز الوثيقة	Shaqra-CS-P-005
النسخة	V 1.1
تاريخ النسخة	07/05/2024
إشارة المشاركة	برتقالي – مشاركة محدودة

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للإستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط . ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

المستلم يحق له مشاركة المعلومات المصنفة بالإشارة الخضراء في نفس منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولايسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

الغرض

الغرض من هذه السياسة هو تحديد متطلبات الاستخدام المقبول في جامعة شقراء لتقليل المخاطر السيبرانية عليها وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تمت موائمة هذه السياسة مع الضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بجامعة شقراء، وتنطبق على جميع العاملين (الموظفين والمتعاقدين) لدى جامعة شقراء.

بنود السياسة

1- البنود العامة

1-1 يجب اتباع متطلبات الأمن السيبراني في السياسات والمعايير والإجراءات المعتمدة لدى جامعة شقراء.

2-1 يجب حماية البيانات، والأصول (الأجهزة أو المعلومات أو البرامج) والتعامل معها حسب حساسيتها وتصنيفها، وفقًا لسياسة حماية البيانات المعتمدة لدى جامعة شقراء وضمان سرية البيانات وسلامتها وتوافرها.

3-1 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

4-1 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، وحفظها في مكان معزول وآمن.

5-1 يمنع الإفصاح عن أي معلومات تخص جامعة شقراء، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخليًا أو خارجيًا.

6-1 يُمنع نشر معلومات تخص جامعة شقراء عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح من صاحب الصلاحية.

7-1 يُمنع استخدام أنظمة جامعة شقراء وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة شقراء.

8-1 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بجامعة شقراء دون الحصول على تصريح مسبق من إدارة الأمن السيبراني، وبما يتوافق مع سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية المعتمدة لدى جامعة شقراء.

9-1 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بجامعة شقراء، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة شقراء.

10-1 تحتفظ إدارة الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والأجهزة الشخصية المتعلقة بالعمل، ومراجعتها دوريًا لمراقبة الالتزام بسياسات ومعايير الأمن السيبراني المعتمدة لدى جامعة شقراء.

1-11 يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات الخاصة بجامعة شقراء أو سرقتها أو تسريبها.

1-12 يجب متابعة قواعد الاستخدام المقبول للمعلومات والأصول المرتبطة بأنظمة معالجة المعلومات.

1-13 يجب على جميع الموظفين والعاملين في جامعة شقراء إرجاع جميع الملفات والمستندات والمعلومات والأصول التي في حوزتهم عند إنهاء عملهم أو عقدهم أو اتفاقهم.

1-14 يمنع نقل الأصول خارج مواقعها بدون إذن مسبق من الإدارات المعنية.

1-15 يجب حماية الأصول التي تكون خارج المواقع مع مراعاة المخاطر المختلفة للعمل خارج مباني جامعة شقراء.

1-16 يجب حضور الجلسات واللقاءات والمحتويات الخاصة بحملات التوعية الأمنية التي تقدمها جامعة شقراء والالتزام بها.

1-17 يجب على جميع العاملين إقرار الموافقة على الاستخدام المقبول للأصول المعتمدة لدى جامعة شقراء.

1-18 يجب على جميع العاملين الموافقة والإقرار على قواعد السلوك وسياسة الاستخدام المقبول عند أي مراجعة أو تحديث عليها.

1-19 يجب أن يكون الوصول إلى أصول جامعة شقراء وفقًا للمسؤوليات والأدوار المطلوبة لأداء المهام فقط.

1-20 يجب تنبيه مشرفي الأصول التقنية حول تصحيحات الأمن السيبراني التي يجب تطبيقها وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى جامعة شقراء.

1-21 يجب على ملاك الأصول مراجعة صلاحيات وصول المستخدمين على فترات محددة ومنتظمة.

1-22 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على جامعة شقراء أو أصولها مثل: وجود مواقع مشبوهة، الاشتباه بوجود مخاطر سيبرانية أو الاشتباه بمحتوى بريد الكتروني قد يتسبب بضرر لـجامعة شقراء.

2- حماية أجهزة الحاسب الآلي

1-2 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

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

3-2 يُمنع استخدام أو تثبيت أجهزة أو أدوات أو تطبيقات غير معتمدة من جامعة شقراء على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة التعلّم الإلكتروني والتحول الرقمي.

3- الاستخدام المقبول للإنترنت والبرمجيات

1-3 يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية وعدم التفاعل معها إلا بالتواصل مع إدارة الأمن السيبراني.

2-3 يُمنع 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 لأي غرض من أغراض العمل، أو استخدام وسائط تخزين خارجية بدون أخذ الموافقة من جامعة شقراء.

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

4-3 يُمنع استخدام التقنيات التي تسمح بتجاوز الخادم الوكيل (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

5-3 يُمنع تحميل البرمجيات والأدوات أو تثبيتها على أصول جامعة شقراء دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

6-3 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تحميل الوسائط والملفات واستخدام برمجيات مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

7-3 يُمنع إجراء أي فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة شقراء وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

4- الاستخدام المقبول للبريد الإلكتروني

1-4 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس الإلكتروني في غير أغراض العمل، ويكون الاستخدام فقط بما يتوافق مع سياسات الأمن السيبراني ومعاييره المعتمدة لدى جامعة شقراء.

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

3-4 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بجامعة شقراء في أي موقع ليس له علاقة بالعمل.

4-4 تحتفظ جامعة شقراء بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقًا للإجراءات والتنظيمات ذات العلاقة المعتمدة لدى جامعة شقراء.

5-4 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5- استخدام كلمات المرور

1-6 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة شقراء وأصولها وفقًا لسياسة إدارة هويات الدخول والصلاحيات في جامعة شقراء. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

2-6 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 التعلّم الإلكتروني والتحول الرقمي وإبلاغ إدارة الأمن السيبراني فورًا في حال وقوع ذلك.

3-6 يجب تغيير كلمة المرور بشكل دوري وفقًا لمتطلبات سياسة كلمة المرور أو عند الحصول على كلمة مرور جديدة من قبل مسؤول النظام.

4-6 يمنع استخدام كلمات مرور مستخدمة من قبل أو متعارف عليها، بالإضافة إلى عدم مشاركة كلمة المرور الخاصة بالمستخدم لأي شخص إطلاقًا.

6- استخدام المكتب

1-7 يجب الالتزام بسياسة المكتب الآمن والنظيف المعتمدة لدى جامعة شقراء، والتأكد من خلو سطح المكتب وشاشة العرض من المعلومات المصنفة والحساسة وفقًا للتصنيفات المعتمدة لدى جامعة شقراء.

2-7 يُمنع ترك أي معلومات مصنفة أو حساسة بالنسبة لجامعة شقراء في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

3-7 يمنع ترك أبواب المكتب والخزانات التي تحتوي على معلومات مصنفة وحساسة مفتوحة.

الأدوار والمسؤوليات

1- **مالك السياسة:** مدير إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** إدارة الموارد البشرية.

4- **قياس الالتزام بالسياسة:** إدارة الأمن السيبراني.

التحديث والمراجعة

يجب على إدارة الأمن السيبراني مراجعة السياسة سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في جامعة شقراء أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالسياسة

1- يجب على مدير إدارة الأمن السيبراني التأكد من التزام جامعة شقراء بهذه السياسة دوريًا.

2- يجب على جميع العاملين في جامعة شقراء الالتزام بهذه السياسة.

3- قد يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في جامعة شقراء.