المملكة العربية السعودية
وزارة التعليم
جامعة الملك خالد
الإدارة العـــامة للأمـن الـسيبـرانـي

Kingdom of Saudi Arabia
Ministry of Education
King Khalid University
General Administration of Cybersecurity

سياسة استخدام موظفي الدعم الفني والطلاب للمعامل والأجهزة بصورة مقبولة

الإصدار: أكتوبر ٢٠٢٢
النسخة: ١,٠
عامة

KKUCYBERSECURITY
الإدارة العامة للأمن السيبراني
GENERAL ADMINISTRATION OF CYBERSECURITY

الوثيقة المرجعية

عنوان الوثيقة	سياسة استخدام موظفي الدعم الفني والطلاب للمعامل والأجهزة بصورة مقبولة			
التصنيف	✔ عامة	خاصة	سرية	سرية للغاية
الحالة	فعّال			
النوع	وثيقة			

الإعداد

رقم النسخة	التاريخ	إعداد
1.0	١-اكتوبر-٢٠٢٢م	عذى القرني

المراجعة

رقم النسخة	التاريخ	المُراجع
1.0	٥-نوفمبر-٢٠٢٢ م	بدرية القحطاني مريم الشهري

الاعتماد

رقم النسخة	التاريخ	المُعتمد
1.0	٢-يناير-٢٠٢٣م	رئيس لجنة التعاملات الإلكترونية معالي رئيس جامعة الملك خالد

المحتويات

١. المقدمة

تُمثّل هذه الوثيقة سياسة استخدام موظفي الدعم الفني و الطلاب للمعامل والأجهزة بصورة مقبولة بجامعة الملك خالد والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من تِسعة أقسام رئيسية لِتشمل هذه المُقدِمَة يليها الغَرض، والنطاق، والمصطلحات والتعريفات، والأدوار والمسؤوليات، وبنود السياسة، والمرجعيات، والالتزام، وأخيراً معايير الاستثناءات.

على جَمِيع المستخدمين القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بسياسة استخدام موظفي الدعم الفني و الطلاب للمعامل والأجهزة بصورة مقبولة وفى حالة عدم الاستيعاب أو عدم الفهم الكامل من قِبَل أي مستخدم لتلك الوثيقة أو لأي جزءٌ منها، فإنه يَجِب عليه التواصل في الحال مع الإدارة العامة للأمن السيبراني حتى يتسنى له فهم النِقاط غير الواضحة بالنسبة له.

تُعَدُ الإدارة العامة للأمن السيبراني بالجامعة هي المالكة لِتلك الوثيقة.

إن مدة صلاحية هذه الوثيقة هي ٣ أعوام من تاريخ إصدارها، ويجب على الإدارة العامة للأمن السيبراني مراجعة وتحديث هذه الوثيقة مرة واحدة على الأقل كل عام، أو يجوز أيضاً تحديثها فور حُدوث أى تعديلات أو تغييرات تتعلّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تغيير رقم إصدار الوثيقة حال القِيام بأى تعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ اللجنة الإشرافية للأمن السيبراني بالجامعة.

٢. الغرض

تهدف هذه السياسة الى ضمان توفير طريقة للحصول على استثناء للامتثال لسياسات أو معايير الأمن السيبراني وفقا لسـياسـات وإجراءات الجامعة والمُتطلبات التشريعية والتنظيمية ذات العلاقة..

٣. النطاق

تنطبق هذه الوثيقة على كافة الأصول المعلوماتية والتقنية والخدمات المقدمة في المعامل، وكذلك كافة مستخدميها من الموظفين والطلاب سواء كانوا يعملون بصفة دائمة أو مؤقتة، أو يعملون بدوام كامل أو دوام جزئي، أو متعاقدين كموظفي شركات الإسناد الخارجي. وكذلك مستخدمي وموظفي جميع الأطراف الخارجية كالمقاولين والموردين والشركات الاستشارية والجهات الحكومية وشركات الخدمات المُدارة وغيرها.

٤. المصطلحات والتعريفات

- **الأمن السيبراني**: حسب ما نص عليه تنظيم الهيئة الوطنية للأمن السيبراني، الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١٤٣٩/٢/١١هـ) فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
- **NCA**: الهيئة الوطنية للأمن السيبراني.
- **ISO**: المنظمة الدولية للمعايير (منظمة الأيزو).

- **ECC**: الضوابط الأساسية للأمن السيبراني.
- **الأصل:** أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصـول؛ بعض هذه الأصـول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات، والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
- **السرية**: الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.
- **سلامة المعلومات**: الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات والموثوقية.
- **التوافُر**: ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
- **حادَثة**: انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
- **صلاحية المستخدم**: خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى بعض الموارد وكذلك أمن الأصول المعلوماتية والتقنية للجهة بصفة عامة وضوابط الوصول بصفة خاصة.
- **ضابط**: مقياس لتقييد ومعالجة المخاطر.
- **المخاطر**: المخاطر التي تمِسّ عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفـراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المُصَرَّح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نُظم المعلومات.

٥. الأدوار والمسؤوليات

المسؤول	الإعداد والتحديث والمراجعة	الاعتماد	النشر	الالتزام
اللجنة الإشرافية للأمن السيبراني		■		
الإدارة العامة للأمن السيبراني	■		■	
الإدارة العامة لتقنية المعلومات الإدارة العامة للأمن السيبراني جميع موظفي وطلاب الجامعة				■

6. بنود السياسة

- **سياسة الدعم الفني للمعامل وأجهزة الحاسب:**

1. رفع نموذج طلب للبرامج من قبل الكلية لإدارة الدعم الفني ويتم دراسته من قبل المسؤول عن العمل على المعامل ومدى احتياجه وبعد ذلك يتم الرفع لإدارة الامن السيبراني لفحص البرامج والموافقة عليها.
2. عدم توصيل المعامل الاphysical بالإنترنت وشبكة الجامعة الا بعد الرفع لإدارة الامن السيبراني بحاله المعمل والفحص من قبل فريق الدعم الفني
3. تقييد البرامج المثبتة بالمعمل حسب احتياج الجهة وحسب الاستخدام الفعلي عليها.
4. التأكد الدوري من ان مكافح الفيروسات يعمل بشكل فعال على أجهزة المعامل
5. تقييد استخدام وسائط التخزين الخارجية في أجهزة المعامل.

- **الوصول ألى مرافق وأجهزة معامل الحاسب الآلي**

1. معامل الحاسب الآلي في جامعة الملك خالد مخصصة لتدريب الطلاب ولكن يجوز أن يستخدمها أخرون كمشاركين في الأنشطة التي ترعاها الجامعة. ويجوز لهذه المعامل أن تضع إجراءات لإصدار تصاريح مؤقتة للمشاركين في هذه الأنشطة .
2. قد يُطلب من الأفراد الذين يستخدمون مرافق الحاسب الآلي أن يكشفوا عن هوياتهم بإظهار البطاقة الجامعية أو عن طريق تسجيل الدخول الى أنظمة الحاسب الآلي. ويجوز أن يطلب المسؤولون عن معامل الحاسب الآلي في الجامعة من الأفراد غير المصرح لهم باستخدام هذه المرافق أن يغادروها.
3. . خصصت حسابات الحاسب الآلي للتحكم في الوصول إلى بعض مصادر الحوسبة .
4. المستخدمون مسؤولون عن جميع استخدامات حساباتهم الخاصة بحواسيبهم الآلية. ويجب عليهم عدم كشف اسم المستخدم ولا كلمات المرور لمستخدمين آخرين. ويجب على المستخدمين تسجيل خروج من الجهاز في نهاية كل جلسة.
5. يعد استخدام حساب حاسب آلي مخصص لشخص آخر خرقًا لسياسة الجامعة .

- **سياسة الاستخدام المقبول لمرافق وتجهيزات معامل الحاسب الآلي**

١. يجب استخدام المصادر للغرض المقصود منها
٢. .يجب على الطلاب الالتزام بقواعد السرية التي تحكم استخدام كلمات المرور والحسابات، ويجب عدم اطلاع الآخرين على تفاصيل هذه الكلمات والحسابات .
٣. .لا يجوز أن يستخدم الطلاب غير الأجهزة المصرح لهم باستخدامها .
٤. تشجع الجامعة وتروج لاستخدام بريد الجامعة الإلكتروني لأغراض إدارية وتعليمية ومهنية. وبالتالي، يجب على الطلاب استخدام البريد الإلكتروني الجامعي في اتصالاتهم الرسمية .
٥. يتعين على الطالب استخدام مرافق معامل الحاسب الآلي وأجهزتها بطريقة لا يكون لها تأثير ضار على استقرار ووظائف الأنظمة أو الشبكات .
٦. يمنع توصيل اجهزة (FireWire) وحدات التخزين (USB)حتى يتم مراجعة موظفي الدعم الفني في الإدارة العامة لتقنية المعلومات للحصول على معلومات محددة بشأن هذه الاستخدامات.
٧. .يخضع كل استخدام لأجهزة الحاسب الآلي المحمولة في مرافق الحاسب الآلي بالجامعة لسياسات الجامعة والإدارة القانونية بها.
٨. .تحتفظ الجامعة بحقها في إجراء أي تعديلات على هذه السياسة في أي وقت .
٩. الإدارة العامة لتقنية المعلومات ليست مسؤولة عن محتوى الإنترنت الذي تم تصفحه بواسطة الطالب النهائي، أو المشكلات التي قد تحدث للطالب من تصفح مواقع الويب غير الموثوق بها .
١٠. تمنع الجامعة تحميل أي برامج وتثبيتها على أجهزه الحاسب الآلي الخاصة بها وينبغي أن تطلب هذه البرامج من خلال رفع بلاغ على مركز الاتصال الموحد ٨٠٠٠ او (نظام بلاغات تقنية المعلومات) لمكتب

الدعم الفني التابع الإدارة العامة لتقنية المعلومات ويكون ذلك بعد موافقة الإدارة العامة للأمن السيبراني .

١١. يجب إعادة المرافق والأجهزة إلى ما كانت عليه من نظافة وترتيب بعد كل استخدام .

١٢. يتحمل موظفي المعمل مسؤولية أي فقدان للأجهزة أو سرقتها أو إلحاق الضرر بها جراء الإهمال فيها، وعندما يعتقد الطالب او الموظف أن جهازاً قد سرق، فعليه أن يرفع تقريراً إلى إدارة الكلية واشعار الإدارة العامة للامن السيبراني

١٣. لا يمكن الوصول إلى المعامل والأجهزة الخاصة بها إلا خلال ساعات العمل

١٤. يجب على الطلاب، الذين يكتشفون أو يعثرون على مشاكل أمنية أو نشاط مشبوه، الاتصال مباشرة بالمشرف على مرافق المعمل، وأجهزته ليقوم بدوره برفع بلاغ مباشرة للإدارة العامة للأمن السيبراني على التحويله الموحدة ٦٦٦٥ .

سياسة استخدام الطلاب لمرافق وتجهيزات معمل الحاسب الآلي بطريقة غير مقبولة

١. عدم الانخراط في أي نشاط يهدف إلى تعريض امن النظام للخطر أو المساس بخصوصية المستخدمين الآخرين أو عرقلة عملهم. ويشمل ذلك على سبيل المثال حصر الأجهزة والبرامج الإلكترونية.

٢. .عدم استخدام الحاسب الآلي الموجود في المعمل لمهاجمة أنظمة حاسب آلي أو شبكات أخرى ، والتدخل في التشغيل السليم لها أو المساس بأمنها

٣. عدم استخدام أنظمة المعمل لإرسال بريد إلكتروني مزور أو إرسال بريد جماعي أو إرسال بريد إلكتروني تجاري غير مرغوب فيه أو لتشويه هوية المستخدم بطريقة احتيالية في أي اتصال .

٤. عدم فصل الكابلات عن أجهزة الحاسب لتوصيلها بالأجهزة الشخصية .

٥. عدم تفكيك الأجهزة لاستكشاف المشكلات (التي ظهرت أثناء العمل) وإصلاحها دون إبلاغ القائمين على أمر المعمل .

٦. يمنع إخراج الأجهزة من المعامل أو أخذ عناصر من مستلزمات المعمل

٧. يمنع تغيير تكوينات النظام أو البرنامج .

٨. يمنع قطع اتصال الأجهزة، تثبيت الأجهزة، أو تغيير تكوينات الأجهزة

٩. يمنع ترك الأجهزة خارج المركز تحت أي ظرف من الظروف حتى لو كانت صالة الحواسيب مغلقة. وعلى أي شخص تسبب في ضياع جهاز من الأجهزة جراء تركه خارج المركز أن يأتي بجهاز بديل تعويضاً لهذا الجهاز الضائع علما بأن امتيازات الوصول الخاصة به ستلغى

١٠. يمنع استخدام أنظمة المعمل للشروع في أي اتصال يهدف إلى غرس الرعب الآخرين أو إكراههم أو مضايقتهم أو تهديدهم.

١١. .يمنع استخدام أنظمة المعمل لتوزيع أو تطوير الفيروسات أو الفيروسات المتنقلة أو البرامج المشابهة .

١٢. يمنع تبادل المواد المحمية بحقوق الطبع والنشر بشكل غير قانوني مع الآخرين.

١٣. يمنع فصل أنظمة المعمل لتوصيل أجهزة الحاسب المحمول

١٤. .يمنع توصيل أجهزة الحاسب المحمولة بمقابس الشبكة غير المستخدمة.

١٥. يمنع استخدام شبكة الجامعة بأي طريقة غير قانونية، على سبيل المثال لأغراض تجارية أو تسجيل الدخول بطريقة غير مصرح بها أو تصفح مواقع الويب أو المحتوى غير القانوني .

١٦. يمنع محاولة مخالفة معايير أمن شبكة الجامعة أو الإخلال بها أو الإخلال بأي جهاز آخر متصل بالشبكة أو الوصول إليه عبر الإنترنت .

١٧. يمنع استخدام شبكة الجامعة لإنشاء ونشر وتخزين وعرض مواد فاحشة أو مواد إباحية أو مواد مسيئة أو غير لائقة أو إساءة سمعة أو أدبيات الكراهية .

١٨. يمنع إنشاء نسخ غير قانونية أو انتهاك المواد المحمية بموجب حقوق الطبع والنشر لاستخدامها أو حفظها على أجهزة الجامعة أو إرسالها عبر شبكة الجامعة فهذا التصرف ممنوع. ومن الأشياء

الممنوعة الأخرى الاستخدام غير القانوني لشبكة الجامعة مثل إرسال أو تنزيل أو نشر أي مادة تنتهك قوانين المملكة العربية السعودية وتخالف القيم الإسلامية.

١٩. يمنع استخدام السلوك غير الجاد أو التخريبي أو المدمر أو عدم المبالاة في معامل الحاسب الآلي أو المناطق الطرفية لأنه غير مسموح به.

٢٠. يمنع محاولة الوصول الغير مصرح بها إلى حاسب آلي آخر (داخل الحرم الجامعي أو خارجه) لأنه يعد تصرفاً محظوراً ويؤدي إلى الإلغاء الفوري للاتصال بالشبكة المشتبه بها حتى يتم حل المشكلة

7. الالتزام

- يجب أن تتوافق سياسة استخدام موظفي الدعم الفني والطلاب للمعامل والأجهزة بصورة مقبولة مع الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (ECC:1-2018) ومع جميع متطلبات معيار الأيزو العالمي لأمن المعلومات (ISO/IEC 27001:2013).
- ينبغي الالتزام بسياسة إدارة الاستثناء من قِبَل جميع المستخدمين والموظفين والأطراف المعنية ذات العلاقة، ويجب على جميع مدراء الإدارات والأقسام التأكُّد من الالتزام المُستمر بتطبيقها.
- يَنبغي مُراجعة الالتزام بتطبيق السياسة دَورياً بواسطة الإدارة العامة للأمن السيبراني، كما يَجِب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك للسياسة. ويجب أنَّ تتكافئ حِدَّة الإجراءات التأديبية مع حجم الانتهاك أو جَسامة الحادِث المُرتكَب، ويَتحَدَّدْ ذلك عَقب الانتهاء من التحقيقات اللازمة والتي يدورها قد تُسفِر عن التالي، على سبيل المثال :
  - فَقْدْ امتيازات الوصول إلى الأصول المعلوماتية والتقنية.
  - عقوبات قَدْ تكُون مَالية، وقد تصِل إلى إنهاء خِدمة المُوظَف، أو النزول بمستواه الوظيفي إلى درجة أقل، وذلك حَسبما تراه الإدارة العليا مناسباً وفق الأنظمة والتعليمات و القوانين الرسمية.

8. معايير الاستثناءات

- تهْدُف هذه الوثيقة إلى تلبية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه، يَجِب تقديم طلَبْ رَسمِي، عند الحاجة إلى الحُصول على استثناء. ويُقدَّم الطلب إلى الإدارة العامة للأمن السيبراني، مع ذِكْر حيثيات طلب الاستثناء بوضوح، وعَرْض الفوائد المَرْجُوَّة من هذا الاستثناء، ليتم البَتّ فيه ومَنْح الموافقة النِهائية من قِبَلْ اللجنة الإشرافية للأمن السيبراني.
- تصِل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى، إلَّا أنَّه يُجوز إعادة تقييم طلَب الاستثناء وتجدِيد المُوافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضَى الأمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثلاث أعوام السالِف ذِكْرهُم.

سياسة استثناء معامل الحاسب الالي:

- استثناء عدد من معامل الحاسب الالي من بعض القيود الموجودة في السياسة، على أن تكون وفق الشروط التالية:

اولاً: الشبكة

- تكون معزولة تماماً
- منع الاتصال اللاسلكي بداخلها تماماً
- تسمح للاتصال بالأنترنت مباشرة (وأي انتهاك على جهة خارجية يتحمل عضو هيئة التدريس المسؤولية الكاملة) حيث لابد من توعية الطلاب والطالبات بسياسات اختبار الاختراق وتخلي الإدارة العامة للأمن السيبراني وموظفيها مسؤوليتهم من أي انتهاك يحدث لاحقاً.

ثانياً : طلبات تثبيت البرامج :

- حالياً يتم تثبيت البرامج ادناه على بيئة افتراضية (VM) فقط وليس مباشرة على الجهاز
  كـ Kali Linux و Virtual Box و Ubuntu و Seed Lab
- وفي حال الحاجة الى برامج أخرى يجب تقديم طلب بأسماء البرامج ولابد من موافقة ودراسة الإدارة العامة للأمن السيبراني في بداية كل فصل دراسي .
- تخصيص أسماء مستخدمين للأجهزة كـ (Lab1,Lab2, ...etc) ولايسمح باستخدام الحسابات الرسمية لمنسوبي الجامعة من طلاب وأعضاء هيئة تدريس.
- عمل تقييد لتنزيل البرامج على الاجهزة عدا البرامج الموجودة في (Software Center)
- لابد من وجود مكافح فيروسات محدث بشكل دوري
- تقييد استخدام وسائط التخزين

ثالثاً: مواصفات الأجهزة :

- أجهزة الحاسب لابد من ان تكون ويندوز١٠ او ١١
- CPU core I 7
- Ram16 GB at least
- HD500 GB at least