الأمن السيبراني

سياسة الاستخدام المقبول

الإدارة العامة للأمن السيبراني

على جَمِيع منسوبي الجامعة القيام بالقراءة المُتأنِية والفهم الجيد والالتزام الكامل بسياسة الاستخدام المقبول. 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 النقَاط غير الواضحة بالنسبة له.

0172416665

cyber.kku.edu.sa

الأمن السيبراني

الاستخدام المقبول للأصول التقنية والمعلوماتية

- استخدام جميع المعلومات والأصول التقنية والمعلوماتية لأغراض العمل فقط.
- يحظر انتهاك حقوق أي شخص، أو جهة 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.
- عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
- حفظ وسائط التخزين الخارجية بشكل آمن وملائم.
- الامتناع عن نشر معلومات تخص الجامعة عبر وسائل الإعلام، وشبكات التواصل الاجتماعي.

الأمن السيبراني

المسؤولية عن الأصول التقنية والمعلوماتية

- يكون مالك الأصل مسؤولاً عن إدارة الأصول التقنية والمعلوماتية والتي تقع تحت مسؤوليته ويجب عليه متابعة حماية سريتها وسلامتها وتوافرها.
- مالك الأصل هو المسؤول عن تفويض شخص أو إدارة راعية ومسؤولة عن تشغيل الأصول التقنية والمعلوماتية، ويجب على الراعي أَنَّ يقوم بمنح الصلاحيات لكل المستخدمين والموظفين الذين يتوجب عليهم الوصول إلى الأصول التقنية والمعلوماتية وفقاً لأغراض واحتياجات العمل وبناءً على موافقة مالك الأصل.

الأمن السيبراني

إعادة الأصول التقنية والمعلوماتية عند الاستقالة أو إنهاء الخدمة

- عند انتهاء الخدمة أو الاستقالة، يجب على الموظف إعادة كافة الأصول التقنية والمعلوماتية إلى الجامعة.
- إلغاء أو تعطيل كافة حقوق الوصول لأي موظف انتهت خدمته أو استقال، وأي موظف ينتقل من إدارة إلى أخرى.
- تهيئة أي قرص صلب بالحاسوب الخاص بالموظف قبل تسليمه إلى أي موظف آخر أو قبل حفظه لاستخدامه لاحقاً.

الأمن السيبراني

سياسة المكتب النظيف والشاشة الخالية

- في حالة عدم تواجد الموظف المُصَرَّح له في مكتبه أو مكان عمله، إزالة جميع الوثائق الورقية ووسائط تخزين البيانات.
- حفظ المستندات والوسائط في أماكن آمنة.
- مسح أو إخفاء أي ملفات موجودة على سطح المكتب وذلك وفقاً لمتطلبات سياسة الشاشة الخالية.

الأمن السيبراني

مسؤولية المستخدم عن بيانات الهوية

- لا يحق لجميع منسوبي الجامعة السماح، بشكل مباشر أو غير مباشر، لشخص آخر (أو أشخاص) باستخدام حقوق الوصول الخاصة بهم، مثل اسم المستخدم وبطاقة الوصول، بالإضافة إلى حقوق الوصول والصلاحيات المخصصة للمستخدم.
- اختيار كلمات مرور مختلفة عن كلمات المرور للحسابات الشخصية، مثل حسابات البريد الإلكتروني ومواقع التواصل الاجتماعي.
- يعتبر الموظف مالكاً لحساب المستخدم الخاص به ويكون مسؤولاً عن استخدامه وعن أي معاملات أو أنشطة تتم باستخدام هذا الحساب.

الأمن السيبراني

سياسة استخدام الإنترنت

- استخدام خدمات الإنترنت الخاصة بالجامعة لأغراض العمل فقط وليس للاستخدام الشخصي.
- إبلاغ الإدارة العامة للأمن السيبراني في حالة وجود مواقع مشبوهة يجب حجبها.
- يمنع زيارة المواقع المشبوهة بما فيها مواقع تعليم الاختراق.
- يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية المنتهكة.
- يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراق.

الأمن السيبراني

سياسة استعمال البريد الإلكتروني

- التوقيع على جميع رسائل البريد الإلكتروني المرسلة من خدمات البريد الإلكتروني بالجامعة، على أن تتضمن الاسم الأول والأخير والمسمى الوظيفي والقسم الذي ينتمي إليه.
- الامتناع عن استخدام أي عناوين بريد إلكتروني شخصية لأغراض العمل.
- عدم فتح أي مرفقات أو روابط داخل رسائل البريد إلكتروني إلا إذا كانت مرسلة من أشخاص أو جهات مَوْثوق بها ومعروفة وغير مجهولة وبعد التحقق من سلامتها.
- استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات الرسمية.

الأمن السيبراني

مسؤولية النسخ الاحتياطي للبيانات والمعلومات

- يقع على عاتق جميع منسوبي الجامعة مسؤولية أَخْذ نُسخ احتياطية لبيانات ومعلومات عملهم.
- في حالة وجود بيانات أو معلومات سرية أو حساسة لابد من أخذ نسخ احتياطية من هذه البيانات والمعلومات وتخزينها في وسائط تخزين مستقلة ومؤمنة.

الأمن السيبراني

الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

- عدم استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.
- عدم إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

الأمن السيبراني

عمليات الفحص واختبار الاختراق

- عدم تنفيذ أي عمليات فحص للشبكة أو محاولة تجاوز الحلول الأمنية واستخدام برامج VPN, PROXY بدون إذن مباشر وصريح من إدارة الأمن السيبراني.
- عدم تنفيذ أي عمليات تقييم للثغرات أو اختبار اختراق أو تحليل حركة مرور الشبكة أو تنزيل برمجيات خبيثة داخل بيئة الجامعة سواءً لاستهداف أي جهاز أو خدمة تتبع للجامعة أو لغيرها. بدون إذن مباشر وصريح من إدارة الأمن السيبراني.

للاطلاع على نظام مكافحة جرائم المعلوماتية:

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة الثالثة

- **يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:**
- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا .
- الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها .
- التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة الرابعة

- **يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:**
- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند ، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .
- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة الخامسة

- **يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:**
- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة السابعة

- **يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية :**
- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .
- الدخول غير المشروع إلى موقع إلكتروني ، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة الثامنة

- **لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:**
- ارتكاب الجاني الجريمة من خلال عصابة منظمة .
- شغل الجاني وظيفة عامة ، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه.
- التغرير بالقُصَّر ومن في حكمهم، واستغلالهم .
- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة التاسعة

- يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

نظام مكافحة جرائم المعلوماتية - المادة العاشرة

- يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة .

الأمن السيبراني

نظام مكافحة جرائم المعلوماتية - المادة الحادية عشرة

- للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

نظام مكافحة جرائم المعلوماتية - المادة الثالثة عشرة

- مع عدم الإخلال بحقوق حسني النية ، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

الأمن السيبراني

الإبلاغ عن حوادث الأمن السيبراني

- يجب على جميع منسوبي الجامعة إبلاغ الإدارة العامة للأمن السيبراني في حالة حدوث أو اكتشاف حوادث أو نقاط ضعف أو أحداث تتعلق بالأمن السيبراني في أسرع وقت ممكن من أجل تجنب آثارها ومخاطرها على بيئة العمل.
- الإبلاغ من خلال القنوات التالية:

1. عنوان البريد الإلكتروني للإدارة العامة للأمن السيبراني بالجامعة (SOC@KKU.EDU.SA).
2. رقم الهاتف للإدارة العامة للأمن السيبراني بالجامعة (0172416665).

الأمن السيبراني

سياسة الاستخدام المقبول

الإدارة العامة للأمن السيبراني

0172416665

cyber.kku.edu.sa