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 حسابات التواصل الاجتماعي وآلية النشر والاستخدام

الإصدار: اكتوبر 2022 م
النسخة: ١,١

الوثيقة المرجعية

عنوان الوثيقة	سياسة حسابات التواصل الاجتماعي			
التصنيف	✔ عامة	خاصة	سرية	سرية للغاية
الحالة	فعّال			
النوع	وثيقة			

الإعداد

رقم النسخة	التاريخ	إعداد
1.0	١٥-٠٨-٢٠٢٠ م	عذى القرني
1.1	٢٠-١٠-٢٠٢٢ م	عذى القرني

المراجعة

رقم النسخة	التاريخ	المُراجع
1.0	٩-٩-٢٠٢٠ م	عهود محمد الشوكاني
1.1	٢٤-١٠-٢٠٢٢م	فاطمة حامد الشهراني

الاعتماد

رقم النسخة	التاريخ	المُعتمد
1.0	٨-٠٧-٢٠٢١ م	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد
1.1	٢-يناير-٢٠٢٣ م	رئيس لجنة التعاملات الإلكترونية معالي رئيس جامعة الملك خالد

المحتويات

١. تعريف هيكلة السياسة

تشمل وثيقة السياسة على العناصر التالية:

الهدف: وصف مختصر لأغراض وأهداف السياسة.

نطاق العمل: تحدد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.

الامتثال والتنفيذ: تحدد تبعات ونتائج مخالفة هذه السياسة.

السياسات: يشتمل هذا القسم على وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.

٢. الهدف

تهدف هذه السياسة الى تصنيف المعلومات والمبادئ التي يجب اتباعها لحماية المعلومات، وذلك من خلال تحديد الاجراءات اللازمة لحماية البيانات وكيف ولمن يمكن نشر هذه المعلومات بتصنيف معين من أجل الحفاظ على خصوصية وسلامة وتوفر البيانات والمعلومات ب"جامعة الملك خالد". ومن خلال إنشاء هذا التصنيف، ستحدد هذه السياسات متطلبات التعامل مع البيانات لتوفير اساسيات حمايتها في جامعة الملك خالد.

٣. نطاق العمل

تسري هذه السياسة على جميع البيانات أو المعلومات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في " جامعة الملك خالد".

٤. الامتثال والتنفيذ

يجب أن يلتزم جميع موظفي جامعة الملك خالد أو الشركاء أو من يعمل مع الجامعة من جهات خارجية بهذا التصنيف الأمني للبيانات.

٥. 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.
- **حادثة**: انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
- **التحَقُّق**: التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
- **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 و معالجة المخاطر.
- **المخاطر**: المخاطر التي تمَسّ 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.
- **الثغرة**: أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يَجعَل الأمن السيبراني عُرَضَة للتهديد.
- **انتهاك أمني**: الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بقصد أو بغير بقصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح التشفير وغيرها من المعايير الأمنية السيبرانية الحرجة).
- **الثغرة**: أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يَجعَل الأمن السيبراني عُرَضَة للتهديد.
- **تهديد**: أي ظرف أو حَدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلا أحد أنظمة المعلومات عن طريق الوصول غير المُصَرَّح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
- **تأثير**: مدى الخسارة الناجمة عن استغلال تهديد لثغرة أمنية.

٦. 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 الجامعة				■

٧. السياسات

ملكية الحسابات وكيفية استخدامها

- جميع حسابات التواصل الاجتماعي وحسابات البريد الإلكتروني المرتبطة بهذه الحسابات للدخول لموقع التواصل الإجتماعي تعتبر ملك لجامعة الملك خالد، بغض النظر عن الأشخاص والمستخدمين والذين يملكون صلاحية استخدام هذه الحسابات.
- يمنع استخدام هذه الحسابات في نشاطات لا تخص طبيعة الحساب او العمل بالجامعة او أي تعدي على سياسة الاستخدام المسموح.

تسجيل الحسابات

- إدارة تقنية المعلومات هي المسؤولة عن الحفاظ على هذه الحسابات، وإدارة وتسجيل كافة التغيرات / التحديثات / المقررة عليها.
- على إدارة تقنية المعلومات تسجيل كافة المعلومات التي تخص حسابات المستخدمين لكل مستخدم على حدة ويتم التوقيع من قبل المستخدمين على هذه المعلومات.
- على إدارة تقنية المعلومات تحديث سجل المستخدمين بعد أي عملية تقييم ومراجعة من قبل إدارة الجودة وأمن المعلومات.
- تقوم إدارة تقنية المعلومات بإنشاء بريد إلكتروني مخصص لكل حساب من حسابات التواصل الاجتماعي ، ويتم ذلك بإتباع النظم المتبعة لتسمية الحسابات.

إدارة الحسابات

- على مستخدمي حسابات التواصل الاجتماعي الالتزام باستخدام هذه الحسابات حسب ما تنص عليه سياسةالاستخدام.
- الالتزام بسياسة كلمات المرور وتطبيقها على حسابات التواصل الاجتماعي.
- يمكن استخدام التطبيقات الخاصة بإدارة كلمات المرور وذلك للمساعدة في إنشاء كلمات المرور، ولكن يجب ان تراجع هذه التطبيقات من قبل إدارة تقنية المعلومات.

- على جميع المستخدمين التعاون مع إدارة تقنية المعلومات وذلك بمدها بالمعلومات التي تساعد في تحديث ارقام الهواتف والأجهزة.
- على إدارة تقنية المعلومات الالتزام بسياسة كلمات المرور وذلك بالنسبة لكلمات المرور المخصصة لحسابات البريد الإلكتروني.
- إذا كان هناك حساب بريد إلكتروني يحتاج إلى تحديث او تعديل، على إدارة تقنية المعلومات إنشاء حساب جديد لهذا الغرض.

التحقق من الدخول

- يجب تمكين خاصية التحقق من الدخول لحسابات التواصل الاجتماعي ، وذلك باستخدام رمز التحقق وإرساله إلى رقم الهاتف المرتبط بالحساب الذي يريد الدخول عليه.
- إذا كان موقع التواصل الاجتماعي يوفر خاصية المصادقة بعاملين من أجل تمكين الدخول على الحساب، فيجب تفعيل هذه الخاصية لرفع مستوى حماية الحساب من الدخول الغير مصرح به عن طريق إرسال رمز تفعيل عند كل عملية تسجيل دخول من جهاز مختلف.

الربط بين البريد الإلكتروني ورقم الهاتف المحمول

- على جميع المستخدمين التواصل مع إدارة تقنية المعلومات وذلك بغرض التحقق وربط حسابات التواصل الاجتماعي مع حسابات البريد الإلكتروني، للتحقق من عملية التسجيل الدخول أو لأغراض استعادة الحساب.
- على إدارة تقنية المعلومات تسجيل بيانات البريد الإلكتروني المستخدم مع حسابات التواصل الاجتماعي بالنسبة لكل المستخدمين في ملف تسجيل حسابات التواصل الاجتماعي.
- يمنع ربط حسابات البريد الإلكتروني الشخصية مع حسابات التواصل الاجتماعي التي تخص جامعة الملك خالد.
- على جميع المستخدمين ربط حسابات التواصل الاجتماعي برقم الهاتف المحمول لديهم وذلك لأغراض التحقق من بيانات الحسابات عند الدخول على مواقع التواصل الاجتماعي ،ايضاً عملية الاستعادة الحسابات عند حدوث موانع تمنع عملية الدخول إلى تلك المواقع
- على جميع المستخدمين تقديم بيانات رقم الهاتف المحمول المراد ربطه مع حسابات التواصل الاجتماعي إلى إدارة تقنية المعلومات وذلك لغرض تسجيله في ملف تسجيل حسابات التواصل الاجتماعي مع بيانات الحساب المراد الربط به .

استخدام البريد الإلكتروني الجامعي لإنشاء الحساب

١. اعتماد اسم الحساب حسب نموذج مفاتيح الترميز المعطى من إدارة تقنية المعلومات
٢. الاعتماد النهائي للحساب حسب المعطيات الإعلامية من الإدارة العامة للعلاقات والإعلام
٣. تخصيص حساب واحد فقط لكل جهة في جميع شبكات التواصل الاجتماعي.
٤. عند إنشاء حساب في (تويتر إنستغرام ، فيس بوك ، يوتيوب) يراعي استخدام وإبراز الوان هوية الجامعة المعتمدة وشعارها الرسمي بدقة عالية
٥. عند التعريف بالحساب يراعي ذكر اسم الجهة كاملة وتبعيته لجامعة الملك خالد وذكر الموقع الجغرافي

٦. يجب اختيار كلمة مرور قوية ومختلفة عن كلمة المرور للبريد الإلكتروني وتكون من ثمان خانات تحتوي أحرفا وأرقاما ورموزا حسب المعايير المحددة .
٧. عند إنشاء حساب في (سناب شات) يراعي استخدام وإبراز لوان هوية الجامعة المعتمدة وشعارها الرسمي وذلك كملصق مصمم لهذا الغرض

ضوابط حسابات التواصل الاجتماعي التابعة لجامعة الملك خالد :

١. يعد حساب الجهة ملكاً خاصاً للجامعة
٢. يتحمل مشرف حساب الجهة كافة المسؤولية عما ينشر (مسؤول الجهة والحساب) .
٣. يعتبر حساب الجهة حسابا أحادي التواصل ، ويكون قناة تواصل لنشر الأخبار العامة المتعلقة بالجهة داخلياً فقط
٤. يجب ألا يتم عمل إعادة نشر للحسابات الشخصية وتختصر فقط على الحسابات الرسمية (الموضحة سابقا) وكذلك عدم نشر إي إعلان خاص بالجامعة قبل نشره من الحساب الرسمي ، ويمكن إعادة النشر لحسابات الجهات الأخرى بالجامعة حين توفر محتوى له ارتباط يفيد متابعي حساب الجهة
٥. عدم التسويق لجهات أخرى أو أشخاص خارج الجامعة بإعادة نشر محتوى مشاركاتهم
٦. عدم متابعة أي حسابات لا علاقة لها بأنشطة الجامعة أو الانضمام إلى نشاط اجتماعي .
٧. يجب على مسؤول حسابات التواصل الاجتماعي الخاصة بالجهة أن يخصص الوقت المناسب لمراجعة حسابات التواصل الاجتماعي بهذه الجهة يوميا مع إضافة محتويات جديدة مرة أسبوعيا على الأقل حتى يكون الحساب فعال بصورة نشطة
٨. يجب على مسؤول الجهة التأكد من أن المعلومات والمحتويات التي يتم نشرها على حسابات التواصل الاجتماعي مناسبة للجمهور وتعكس وجهة نظر الجهة ورؤية الجامعة.
٩. يجب أن يأخذ الشكل العام والمعلومات الشخصية للحساب الطابع الرسمي في العبارات والرسومات والصور المستخدمة بما لا يتنافى مع حقوق وسياسات النشر

تأمين عملية تسجيل الدخول إلى مواقع التواصل الاجتماعي والأجهزة المستخدمة لذلك

- على جميع المستخدمين الالتزام بسياسة الاستخدام المسموح المرفقة وذلك لضمان أمان عملية تسجيل الدخول إلى أي موقع على شبكة الإنترنت بواسطة المتصفحات المتوفرة لذلك الغرض.
- على جميع المستخدمين عدم استعمال أي أجهزة حتى ان كانت هذه الأجهزة شخصية حتى تتم مراجعتها والموافقة عليها من قبل إدارة الأمن السيبراني .

تغيير الاجهزة أو التخلص منها

- على جميع المستخدمين الذين يرغبون في التخلص وتغير أجهزتهم الشخصية المستخدمة للأغراض أعلاه تقديم طلب إلى إدارة الأمن السيبراني وذلك للتأكد من أن جميع البيانات والحسابات التي تخص الجامعة على الجهاز قد تم مسحها وإزالتها بصورة كاملة وصحيحة.

مسؤولية المستخدمين

- تقع المسؤولية المباشرة لحسابات التواصل الإجتماعي على المستخدمين الذين يستخدمون هذه الحسابات، لذا عليهم اتخاذ الخطوات اللازمة لضمان أمان هذه الحسابات .
- على جميع المستخدمين إبلاغ إدارة الأمن السيبراني عن أي نشاط مشبوه على حساباتهم أو فقدان او سرقة أجهزتهم سواء التي تخص الجامعة أو الأجهزة الشخصية .
- قبل تثبيت وتنصيب برامج او تطبيقات التواصل الإجتماعي على الأجهزة المستخدمة على جميع المستخدمين أخذ الموافقة أولاً من إدارة الأمن السيبراني.

تعليمات كلمات المرور

الحد الأقصى لعمر كلمة المرور : ٩٠ يوم

الحد الأدنى لطول كلمة المرور : ٨ احرف

تعقيدات كلمة المرور : يحوي حرف كبير ، حرف صغير ، رقم واحد ، رمز

كلمات المرور القديمة : عدم إعادة استخدام آخر ٥ كلمات مرور سابقة

عند انشاء الحسابات يجب مراعاة مايلي :

- استخدام بريد إلكتروني تم إنشاؤه على النطاق الرسمي للجامعة لهذا الغرض
- استخدام رقم هاتف مخصص لهذه الحسابات فقط وربط الحسابات به .

الهوية البصرية :

يجب استخدام ما يشير إلى الهوية البصرية للجامعة حسب ما هو متاح في كل منصة من منصات التواصل الاجتماعي ، إضافة إلى شعار رؤية المملكة ٢٠٣٠ ، ويضاف باختصار النص التعريفي بالجهة .

تعدد الحسابات وحذفها :

يتم الاقتصار على حسابات الجامعة الرسمية وحسابات الجهات التابعة لها مما ورد ذكره في هذا الدليل ، أو ما يراه رئيس الجامعة محققا للمصلحة العليا .

وعند إغلاق أو دمج كليات أو عمادات أو أندية طلابية تخطر الإدارة العامة للعلاقات والإعلام قبل ذلك ؛ لاتخاذ ما يلزم إجرائيا بخصوص حسابات التواصل الاجتماعي لتلك الجهات .

البث المباشر:

لا يسمح بعمل بث مباشر من أي منصة ، إلا بعد موافقة خطية من الإدارة العامة للعلاقات والإعلام .

تنبيهات قانونية :

- المسؤول عن إدارة الحساب يلتزم بالحرص والتنبه وألا يخالف السياسات والأحكام الخاصة بمنصات التواصل الاجتماعي ، وأن تكون لديه الخبرة والمعرفة القانونية بشأن وسائل التواصل الاجتماعي .
- استخدام هذه الحسابات خاضع لنظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية .
- التأكيد على أن المصدر الوحيد لكل أخبار الجامعة هي الحسابات الرسمية للجامعة فقط .

- ضمان وحفظ حقوق الملكية الفكرية ، وحقوق المؤلف.

الية النشر في حسابات التواصل الاجتماعي :

إن الاشتراك في مواقع التواصل الاجتماعي يزيد من امكانية التعرض لعمليات اختراق الخصوصية وهي التي تكون بالاستخدام غير السليم للمعلومات الحكومية من جانب الأشخاص غير المصرح لهم بالاطلاع على تلك المعلومات ، عليه ينبغي اتخاذ جميع الإجراءات اللازمة لضمان حماية خصوصية البيانات والمعلومات الحكومية من أي أخطار محتملة على الخصوصية .

وبناء على ذلك يفضل التزام الحسابات الرسمية بالتالي في منصات التواصل الاجتماعي :

١. استخدام الحساب وفقا للصورة الرسمية فقط ، مع مراعاة حقوق الملكية الفكرية والخصوصية والاستخدام المقبول بشبكات التواصل الاجتماعي .
٢. عدم نشر أي صور للخطابات الرسمية .
٣. عدم نشر أرقام الهاتف أو البريد الإلكتروني الشخصي .
٤. عدم الإفصاح عن أي معلومات شخصية للأفراد أو المؤسسات .
٥. عدم مناقشة أي مواضيع لها الطابع الشخصي .
٦. عدم نشر أو إفشاء بيانات الحساب البنكي الإلكتروني أو أرقام حسابات أو أرقام بطاقات بنكية أو ائتمانية.

في حال وجود تعريف لمركزه أو مسماه الوظيفي أو اسم أو وسم الجامعة في ملف التعريف في حسابه على شبكات التواصل فتطبق عليه السياسات العامة لحوكمة شبكات التواصل الاجتماعي وهي كالتالي :

١. عدم الرد على استفسارات الجمهور في أي شأن يخص الجامعة .
٢. . عدم التطرق أو الخوض في الأمور السياسية أو المواضيع ذات الجدل في شبكات التواصل الاجتماعي .
٣. عدم إفشاء أي أمر يتعلق بالجامعة أو حدث فيها أو إفشاء مضمون التعاميم أو الخطابات أو الخطوات المستقبلية التي تخص الجامعة .
٤. التحلي بالمسؤولية المهنية وأن لا يعرض الجامعة للانتقاد أو يعرض صورتها الذهنية لدى الجمهور الخارجي إلى التشويه .
٥. عدم توجيه النقد إلى الجامعة وجميع ما يتعلق بها من آليات العمل أو السياسات العامة على شبكات التواصل الاجتماعي ، فالجامعة تمتلك جميع القنوات التي يستطيع فيها الموظف / الموظفة إلى إيصال انتقاداتهم أو توجيه شكواهم .
٦. عدم ذكر أسماء القيادات العليا أو المسؤولين أو الموظفين بالجامعة من باب النقد أو الاتهام أو الخلاف ويتم ذلك عن طريق القنوات الرسمية بالجامعة وعن طريق الإدارات ذات الاختصاص
٧. عدم نشر الأخبار أو الإعلانات أو الفعاليات التي تخص الجامعة قبل نشرها في الحساب الرسمي أو حساب المتحدث باسم الجامعة .

٨. وعند مخالفة ما ينص عليه دليل حوكمة حسابات التواصل الاجتماعي أعلاه يكون الموظف / الموظفة عرضة لتطبيق لائحة المخالفات المتبعة في الجامعة والخاضعة لنظام مكافحة الجرائم المعلوماتية المطبق بالمملكة العربية السعودية .

٩. يجب التواصل مع الإدارة العامة للأمن السيبراني في حالة الاشتباه بوجود اختراق لحسابات التواصل الاجتماعي أو انتحال لحساب لايتبع للجامعة بصلة عن طريق احدى القنوات التالية:

١. الرقم (6665)

٢. البريد الالكتروني (Soc@kku.edu.sa)

تفاصيل الحسابات.

الاسم	الجوال	البريد الالكتروني	Twitter	Snapchat	Instagram	Facebook	أخرى

الية انشاء حسابات التواصل الاجتماعي في جامعة الملك خالد

حسب ضوابط الهيئة الوطنية للأمن السيبراني لحسابات التواصل الاجتماعي للجهات ولتقليل من هذه المخاطر وتعزيز حماية حسابات التواصل الاجتماعي الرسمية في جامعة الملك خالد، بهدف الوصول الى فضاء سيبراني سعودي آمن وموثوق؛ قامت الإدارة العامة للامن السيبراني بجامعة الملك خالد ،بإعداد ضوابط الامن السيبراني حسب ضابط الهيئة (OSMACC - ١-٢٠٢١) لوضع الحد الأدنى من متطلبات الامن السيبراني لتتمكن الإدارات في جامعة الملك خالد من استخدام شبكات التواصل الاجتماعي بطريقة آمنة. وتوضح هذه الوثيقة تفاصيل ضوابط الامن السيبراني ، أهدافها ، نطاق العمل ، الية الالتزام والمتابعة .

ضوابط انشاء حسابات التواصل الاجتماعي في جامعة الملك خالد :

- استخدام حسابات التواصل الاجتماعي مخصصة للجهات، وليس للافراد.
- التسجيل باستخدام معلومات رسمية بريد الكتروني رسمي صادر من الجامعة خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي وعدم استخدام معلومات شخصية.
- توثيق حسابات التواصل الاجتماعي والمحافظة على هوية متسقة في انشاء جميع حسابات التواصل الاجتماعي المستخدمة في جامعة الملك خالد لتسهيل معرفة الحسابات الرسمية واكتشاف حسابات الاحتيال
- استخدام كلمة مرور آمنة وخاصة لكل حسابات التواصل الاجتماعي واجبار مسؤول الحساب تغيرها فوراً حال استلام إدارة الحساب .
- تغير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل.
- استخدام التحقق من الهوية متعدد العناصر Melty Factor Authentication لعمليات الدخول على حسابات التواصل الاجتماعي .
- تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن لكل حساب من حسابات التواصل الاجتماعي في جامعة الملك خالد.
- إدارة صلاحيات المستخدمين ً لحسابات التواصل الاجتماعي بناء على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، ونوعية الأجهزة والأنظمة المستخدمة .
- حصر إمكانية تسجيل الدخول من اكثر من جهاز لحسابات التواصل الاجتماعي.
- رفع الوعي الأمني لدى مسؤولي حسابات التواصل الاجتماعي في الجهات .
- التشديد بعدم تصفح الحسابات الشخصية من خلال الحسابات الرسمية .

- اطلاع مسؤولي إدارة حسابات التواصل الاجتماعي على ضوابط الهيئة الوطنية للأمن السيبراني الخاصة بحسابات التواصل الاجتماعي .
- متابعة حسابات التواصل الاجتماعي و مراقبتها للتأكد من عدم نشر أي محتوى غير مصرح، أو تسجيل أي دخول غير مصرح.
- متابعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الجهة. المراقبة الالية لاي تغير في نمط الحسابات أو مؤشرات اختراق أو نشر أي محتوى غير مصرح أو انتحال هوية الجهة.
- التعاون مع فريق الأمن السيبراني وابلاغهم في حال حدوث أي مما ذكر أعلاه .
- حصر حسابات التواصل الاجتماعي وتحديثها وتوثيقها ومراجعتها كل ٦ اشهر وتزويد الإدارة العامة للأمن السيبراني بنسخة من الحصر

مسؤوليات مدير حسابات التواصل الاجتماعي في جامعة الملك خالد

- التوقيع على بنود المحافظة على سرية المعلومات
- Non-Disclosure Clauses
- حذف الحسابات وبيانات الجهة من قبله عند انتهاء تكليفه أو نقله لجهة أخرى .
- تسليم الحسابات وكلمات المرور واسئلة الأمان السرية والبريد الالكتروني الرسمي للجهة حال النقل .
- الابلاغ عن الثغرات او في حال اكتشاف حادثة أمنية أو انتحال شخصية او نشر محتوى غير مصرح به على حسابات التواصل الاجتماعي التي يديرها
- عدم تصفح الحسابات الشخصية من خلال حسابات التواصل الاجتماعي الرسمية .
- تجنب الدخول لحسابات التواصل الاجتماعية الرسمية من خلال شبكة عامة أو شبكة غير موثوقة .
- الحفاظ على الية استعادة حسابات التواصل الاجتماعي والاسئلة السرية في مكان امن .
- ابلاغ الجهة فوراً في حال فقد الأجهزة المستخدمة في حسابات التواصل الاجتماعي .
- عدم نشر محتوى غير مصرح به والالتزام بنشر كل ما هو مصرح به فقط من قبل الجامعة .
- عدم نشر محتوى مصنف بالسرية أو محاولة نشر وثائق رسمية من خلال حسابات التواصل الاجتماعي.

المرجعيات .

- ISO/IEC 27001:2013, A.6.1
- ISO/IEC 27001:2013, A.6.2
- ECC-1:2018, 1-4
- ECC-1:2018, 1-6
- ECC-1:2018, 2-2-3-2
- ECC-1:2018, 2-6

٨. الالتزام

- يجب أن تتوافق سياسة تنظيم الأمن السيبراني 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 تنظيم الأمن السيبراني من قِبَل جميع المستخدمين والموظفين والأطراف المعنية ذات العلاقة، ويجب على جميع مدراء الإدارات والأقسام التأكُد من الالتزام المُستمر بتطبيقها.

- يَنبغي مُراجعة الالتزام بتطبيق السياسة دَورياً بواسطة الإدارة العامة للأمن السيبراني، كما يَجَب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك للسياسة. ويجب أنَّ تتكافئ حَدِّة الإجراءات التأديبية مع حجم الانتهاك أو جَسامة الحادَث المُرتكَب، ويَتحَدَّدْ ذلك عَقب الانتهاء من التحقيقات اللازمة والتي بَدورها قد تُسفَر عن التالي، على سبيل المثال لا الحصر:
- فَقْدْ امتيازات الوصول إلى الأصول المعلوماتية والتقنية.
- عقوبات، قَدْ تكُون مَالية، وقد تصَل إلى إنهاء خَدمة المُوظَف، أو النزول بمستواه الوظيفي إلى درجة أقل، وذلك حَسبما تراه الإدارة العليا مناسباً وفق الأنظمة والتعليمات و القوانين الرسمية.

٩. معايير الاستثناءات

- تهْدُف هذه الوثيقة إلى تلبَية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه، يَجَب تقديم طَلَبْ رَسمَي، عند الحاجة إلى الحُصول على استثناء. ويُقَدَّم الطَلب إلى الإدارة العامة للأمن السيبراني، مع ذَكْر حيثيات طلب الاستثناء بوضوح، وعَرْض الفوائد المَرْجُوَّة من هذا الاستثناء، ليتم البَتّ فيه ومَنْح الموافقة النّهائية من قَبَلْ اللجنة الإشرافية للأمن السيبراني.
- تصَل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى، إلَّا أنَّه يُجوز إعادة تقييم طَلَب الاستثناء وتجدَيد المُوافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضَى الأَمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثّلاث أعوام السالَف ذَكْرَهُم.