سياسة الاستخدام المقبول

الإصدار: ٢٦ فبراير ٢٠٢٥ م
النسخة: ٢.٠
عامة

الوثيقة المرجعية

عنوان الوثيقة	سياسة الاستخدام المقبول			
التصنيف	✔ عامة	خاصة	سرية	سرية للغاية
الحالة	فعّال			
النوع	وثيقة			

الإعداد

رقم النسخة	التاريخ	إعداد
١.٠	١-سبتمبر- ٢٠٢١ م	م.عذى علي القرني
١.١	١١ -مايو -٢٠٢٢ م	م.فاطمة حامد الشهراني
٢.٠	١٤- يناير -٢٠٢٤ م	م.مريم الشهري

المراجعة

رقم النسخة	التاريخ	المُراجع
١.١	٢٠ - مايو- ٢٠٢٤م	م.عذى علي القرني
٢.٠	١٦-مايو-٢٠٢٥م	م.رائد عايض القحطاني

الاعتماد

رقم النسخة	التاريخ	المُعتمد
١.٠	٤-نوفمبر- ٢٠٢١م	معالي رئيس جامعة الملك خالد
١.١	٢ -يناير-٢٠٢٣م	معالي رئيس جامعة الملك خالد
٢.٠	٣٠ -ابريل- ٢٠٢٥ م	معالي رئيس جامعة الملك خالد

المحتويات

١. المقدمة

تُمَثِّل هذه الوثيقة سياسة إدارة أمن الشبكات الخاصة بجامعة الملك خالد والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من تِسعة أقسام رئيسية لِتَشمل هذه المُقَدِمَة 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 إدارة أمن الشبكات. وفى حالة عدم الاستيعاب أو عدم الفهم الكامل من قِبَل أي مستخدم لتلك الوثيقة أو لأي جزءٍ منها، فإنه يَجِب عليه التواصل في الحال مع الإدارة العامة للأمن السيبراني حتى يتسنى له فهم النِقَاط 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 أي تعديلات أو تغييرات تَتَعلَّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تَغيير رقم إصدار الوثيقة حال القِيام بأي تَعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قِبَلْ اللجنة الإشرافية للأمن السيبراني بالجامعة.

٢. الغرض

إن الغرض الرئيسي من هذه الوثيقة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة الجامعة 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.

٣. النطاق

تنطبق هذه الوثيقة على كافة الأصول المعلوماتية والتقنية والخدمات المقدمة، وكذلك كافة مستخدميها من الموظفين 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 الأصول؛ بعض هذه الأصول 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.
- التَوافُر: ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
- حادِثة: انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
- التَحَقُّق: 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 ومعالجة المخاطر.
- المخاطر: المخاطر التي تَمسّ عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد 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.
- هجوم: أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.
- 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)
- الموظفون: يشير مصطلح "الموظفون" إلى المتعاقدين والموظفين الرسميين الذين وجميع العاملين في الجامعة بصفة دائمة أو مؤقتة.

٥. الأدوار والمسؤوليات

المسؤول	الإعداد والتحديث والمراجعة	الاعتماد	النشر	الالتزام
اللجنة الإشرافية للأمن السيبراني		■		
الإدارة العامة للأمن السيبراني	■		■	
الإدارة العامة للأمن السيبراني عمادة الخدمات الإلكترونية الإدارة العامة بالموارد البشرية				■

٦. بنود السياسة

١.٦. الاستخدام المقبول لأصول التقنية والمعلومات

- يجب استخدام جميع الأصول المعلوماتية والتقنية لأغراض العمل فقط بغرض إتمام جميع المهام الوظيفية الخاصة بالعمل ويُمنع استخدام أنظمة الجامعة وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال الجامعة.
- يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة إدارة الأصول الخاصة بالجامعة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.
- 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.
- يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.
- يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.
- يمنع الإفصاح عن أي معلومات تخص الجامعة، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.
- يُمنع نشر معلومات تخص الجامعة عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.
- يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بالجامعة، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى الجامعة.
- تحتفظ الإدارة العامة للأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.
- يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.
- يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.
- يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من الإدارة العامة للأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.
- 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.
- يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.
- يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة الخدمات الإلكترونية.

- تحدد المساحة التخزينية لرفع الملفات داخل الأنظمة والخدمات الالكترونية في جامعة الملك خالد للموظفين وأعضاء هيئة التدريس بـ٥ جيجا بايت وللطلاب بـ٢.٥ جيجا بايت، وعند الحاجة لزيادة السعة التخزينية لابد من رفع المبررات الخاصة من خلال طلب الاستثناء.
    - يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي أو الأصول.
    - يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.
    - يمنع استخدام كلمات مرور مستخدمة من قبل أو متعارف عليها، بالإضافة إلى عدم مشاركة كلمة المرور الخاصة بالمستخدم لأي شخص إطلاقًا.
    - يجب ارتداء البطاقة التعريفية في جميع المرافق
    - يجب تبليغ الإدارة العامة بالأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.
    - يجب متابعة قواعد الاستخدام المقبول للمعلومات والأصول المرتبطة بأنظمة معالجة المعلومات.
    - يُمنع نقل الأصول خارج مواقعها بدون إذن مسبق من الإدارات المعنية.
- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر والاستخدام الصحيح والفعال لمتطلبات حماية الأصول المعلوماتية والتقنية الخاصة بجامعة الملك خالد.
- يجب حماية الأصول التي تون خارج المواقع مع مراعاة المخاطر المختلفة للعمل خارج مباني الجامعة.
- يجب على جميع العاملين توقيع إقرار الموافقة على الاستخدام المقبول للأصول المعتمدة لدى الجامعة.
- يجب على جميع العاملين الموافقة والإقرار على قواعد السلوك وسياسة الاستخدام المقبول عند أي مراجعة أو تحديث عليها.
- يجب تنبيه مشرفي الأصول التقنية حول تصحيحات الأمن السيبراني التي يجب تطبيقها وفقًا لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة لدى الجامعة.
- يجب على ملاك الأصول مراجعة صلاحيات وصول المستخدمين على فترات محددة ومنتظمة.
- يجب حضور الجلسات واللقاءات والمحتويات الخاصة بحملات التوعية الأمنية التي تقدمها الجامعة والالتزام بها.

٢.٦. المسؤولية عن الأصول المعلوماتية والتقنية

- يجب تحديد مالك جميع الأصول المعلوماتية والتقنية في قائمة سجل الأصول المعلوماتية والتقنية.
- يكون مالك الأصل مسؤولاً عن إدارة الأصول المعلوماتية والتقنية التي نقع تحت مسؤوليته ويجب عليه متابعة حماية سريتها وسلامتها وتوافرها.
- سيصبح مالك الأصل مسؤولاً عن تفويض شخص أو إدارة راعية ومسؤولة عن تشغيل الأصول المعلوماتية والتقنية، ويجب على الراعي أَنَّ يقوم بمنح الصلاحيات لكل المستخدمين والموظفين الذين يتوجب عليهم الوصول إلى الاصول التقنية والمعلوماتية وفقاً لأغراض واحتياجات العمل وبناءً على موافقة مالك الأصل.

- يجب أن يكون الوصول إلى أصول الجامعة وفقًا للمسؤوليات والأدوار المطلوبة لأداء المهام فقط.

٣.٦. إعادة الأصول المعلوماتية والتقنية عند الاستقالة أو إنهاء الخدمة

- يجب على الموظف حال إنهاء خدمته أو تقدمُه بالاستقالة أنْ يعيد جميع الأصول المعلوماتية والتقنية إلى الجامعة.
- يجب على عمادة الخدمات الإلكترونية أَنَّ تقوم بتهيئة (format) اي قرص صلب خاص بالحاسب الشخصي الخاص بالموظف قبل تسليمه لأي موظف آخر أو قبل حِفظُه للاستعمال لاحقاً.
- يجب على عمادة الخدمات الإلكترونية الغاء او تعطيل جميع صلاحيات الوصول الخاصة بأي موظف تم إنهاء خدمته أو تَقَدَّم باستقالته وأي موظف ينتقل من إدارة إلى إدارة أخرى.

٤.٦. سياسة المكتب النظيف والشاشة الخالية

- يجب في حالة عدم تواجد الموظف المُصَرَّح له في مكتبه أو مكان عمله، إزالة جميع الوثائق الورقية ووسائط تخزين البيانات، التي تحتوي على أي بيانات أو معلومات سرية من المكتب أو أي أماكن أخرى مثل الطابعات وأجهزة الفاكس وآلات التصوير وما إلى ذلك لضمان مَنْع أي وصول غير مُصرح به.
- يجب حفظ تلك المستندات والوسائط في أماكن آمنة مثل الخزائن المقفلة، أو الخِزَن، إذا اقتضت الحاجة.
- يجب حفظ أي وثائق سرية بعيدًا عند عدم الحاجة إليها خاصةً عندما يكون المكتب فارغًا (يُفضَّل حفظها داخل خزانة أو خزانة مقاومة للحريق كخيار مثالي).
- يجب مسح أي ملفات موجودة على سطح المكتب وذلك وفقاً لمتطلبات سياسة الشاشة الخالية.
- يجب تطبيق سياسة المكتب النظيف والشاشة الخالية عند ترك أي موظف حاسبه الشخصي، أو في حالة عدم استخدام الحاسب الشخصي لفترة معينة أو لبعض الوقت، كما يجب تطبيق سياسة شاشة التوقف واستخدام كلمة مرور لحماية البيانات والمعلومات من التسريب.
- يمنع ترك أبواب المكتب والخزانات التي تحتوي على معلومات مصنفة وحساسة مفتوحة.

٥.٦. مسؤولية المستخدم عن بيانات الهوية

- غير مُصرَّح لجميع مستخدمي أو موظفي الجامعة السماح بشكل مباشر أو غير مباشر لشخص (أو أشخاص) آخرين باستخدام حقوق الوصول الخاصة بهم مثل اسم المستخدم وبطاقة الدخول وأيضاً حقوق الوصول والصلاحيات المخصصة للمستخدم.
- يُمنَع منعاً باتاً مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية، او مع مستخدمين آخرين لأي أسباب.
- يُعتبَر الموظف هو مالك حساب المُستخدِم الخاص به ويكون مسؤول عن استخدامه وعن أي معاملات أو أنشطة يتم القيام بها بواسطة هذا الحساب.
- يجب على جميع المستخدمين اختيار كلمة مرور مُعقَّدة للتأكد من أَنَّ كلمات المرور الخاصة بهم لن يتم توقعها أو تخمينها بسهولة.
- يجب تغيير كلمة المرور من قِبَل جميع الموظفين بعد تسجيل الدخول لأول مرة.
- يجب تغيير كلمة المرور بشكل دوري وفقًا لمتطلبات سياسة كلمة المرور، أو عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

- يجب على المستخدمين استخدام حساباتهم لأغراض العمل الخاصة بالجامعة فقط ولا يجوز استعمالها استعمال شخصي.
- يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة الجامعة وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

٦.٦. سياسة استخدام الإنترنت

- يجب على جميع المستخدمين استخدام خدمات الإنترنت لأغراض العمل فقط وليس للاستعمال الشخصي.
- يجب إبلاغ الإدارة العامة للأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.
- يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.
- يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.
- يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.
- يجب الوصول إلى خدمات الإنترنت الخاصة بالجامعة باستخدام أجهزة الحاسب وذلك بعد تثبيت تطبيقات الحماية من البرامج الضارة والتأكد من إجراء آخر تحديث لها.
- يجب على عمادة الخدمات الإلكترونية أن تقوم بتثبيت خدمة وكيل الشبكة web proxy لتنقية وفحص جميع طلبات المستخدمين للوصول إلى الإنترنت والسماح فقط لأي طلبات ذات صلة بأغراض العمل.
- يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.
- يُمنع تحميل البرمجيات والأدوات أو تثبيتها على أصول جامعة الملك خالد دون الحصول على تصريح مسبق من الإدارة العامة بالأمن السيبراني.
- يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.
- يجب أن تكون الضوابط الآتية قيد التطبيق، فيما يَخُصّ خدمة الوصول إلى الإنترنت داخل الجامعة:
- يجب أَنَّ يَمْنَع، الوصول المُفَلتر إلى الإنترنت المستخدمين من الوصول إلى أي مواقع إلكترونية أو أي عناوين URL ليس لها علاقة بالعمل في الجامعة، على سبيل المثال لا الحصر، المواد الإباحية، والكراهية، والتمييز، والعنف.
- يجب أن يَمنع المستخدمين من الوصول إلى أي مواقع ضارة أو مشبوهة مُبلَغْ عنها.
- يَلْزَم التحكم في قدرة وصول المستخدمين إلى الخدمة ولابد أيضاً من تسجيل الأنشطة (سواء تم الوصول إليها أو تم حظرها).
- يُسمح بالوصول إلى شبكة الإنترنت فقط عبر شبكة الجامعة وباستخدام البنية التحتية المتضمنة لضوابط الحماية المناسبة.
- يُمنع الوصول إلى الإنترنت بواسطة أجهزة المودم أو الإنترنت عبر الهاتف المحمول أو أي أجهزة أخرى بهدف الاتصال المباشر بالإنترنت.
- يحظر الوصول المجهول (anonymous access) إلى أي مواقع ويب محظورة باستخدام خدمة وكيل الشبكة المثبتة بشكل شخصي أو برامج الشبكة الخاصة الافتراضية VPN.

- لا يجوز للمستخدم أن يقوم بتنزيل أي برنامج على شبكة الإنترنت قبل الحصول على إذن مُسبَق من عمادة الخدمات الإلكترونية.
- يكون المُستخدِم مسؤولاً عن جميع الآثار المُحتمَلة الناتجة عن أي دخول غير مُصرَح به أو استخدام لخدمات الإنترنت.
- يجب حَظْر المواقع الإلكترونية المرتبطة بالتصنيفات التالية: الملفات الضارة، والمواقع الإلكترونية الخبيثة، ومواقع التصيد الاحتيالي، وغيرها، لأنها من مصادر تهديدات الأمن السيبراني، وقد تؤدي إلى المساس بسرية وسلامة وتَوافر الأصول المعلوماتية والتقنية بالجامعة.
- يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بالجامعة دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).
- يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.
- يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات الجامعة وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني
- يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من الإدارة العامة للأمن السيبراني.
- يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

٧.٦. سياسة استعمال البريد الإلكتروني

- يجب استخدام حسابات وخدمات البريد الإلكتروني للجامعة في أعمال تتعلق فقط بالجامعة وليس الاستعمال الشخصي.
- يُمنع استخدام الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.
- يجب القيام بعمل الفحص الآمن لجميع رسائل البريد الإلكتروني الواردة والصادرة سواء داخليًا أو خارجيًا.
- يَحظُر على جميع موظفي الجامعة استخدام أي عناوين بريد إلكتروني غير عناوين الجامعة للبريد الإلكتروني في جميع أغراض العمل الخاصة بالجامعة.
- يجب توقيع موظف الجامعة على جميع رسائله الإلكترونية المرسلة من خدمات البريد الإلكتروني بالجامعة على أن تشمل الاسم الأول والأخير والمسمى الوظيفي والإدارة التابع لها.
- يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالجامعة في أي موقع ليس له علاقة بالعمل.
- يُمنَع إرسال رسائل عبر حساب البريد الإلكتروني الخاص بأي مستخدم آخر.
- يجب على جميع الموظفين ألا يقوموا بفتح أي مرفقات او روابط داخل رسائل البريد إلكتروني إلا إذا كانت مرسلة من أشخاص أو جهات مَوْثوق بها ومعروفة وغير مجهولة.
- يجب على موظفي الجامعة ألا يعيدوا إرسال أي رسالة بريد إلكتروني لأي عنوان خارج الجامعة إلا بعد الموافقة المُسبقة لمالك المعلومة أو من أنشأها أو إذا كانت المعلومة عامة بطبيعتها وبشكلٍ واضح.

- على جميع الموظفين عدم استخدام خدمات البريد الإلكتروني للمشاركة في مجموعات المناقشة أو أي منتديات إلكترونية عامة إلا بعد الحصول على إذن صريح بذلك من قِبَل الإدارة العليا بالجامعة.
- يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.
- يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.
- يجب تبليغ الإدارة العامة للأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة أو أصولها.
- تحتفظ الجامعة بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية والإدارة العامة للأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.
- يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.
- في حال انتهاء علاقة مستخدم البريد الإلكتروني بالجامعة، يتم إغلاق البريد الإلكتروني في مدة أقصاها ستة أشهر للطالب المتخرج وثلاثة أشهر للموظف بعد انتهاء علاقته بالجامعة. حيث يتم إشعارهم بضرورة رفع جميع الملفات الخاصة بهم قبل انتهاء المدة المحددة. وذلك لضمان تجنب المخاطر الأمنية التي قد تنشأ من بقاء البريد الإلكتروني فعالاً.

٨.٦. مسؤولية النسخ الاحتياطي للبيانات والمعلومات

- يقع على عاتق جميع موظفي الجامعة مسؤولية أَخْذ نُسخ احتياطية لبيانات ومعلومات عملهم.
- في حالة وجود أية بيانات أو معلومات سرية أو حساسة لابد من أخذ نسخ احتياطية من هذه البيانات والمعلومات وتخزينها في وسائط تخزين مستقلة.
- يجب قيام عمادة الخدمات الإلكترونية بعملية النسخ الاحتياطي لبيانات العمل الحساسة وتخزينها في وسائط تخزين مؤمنة.

٩.٦. الاتصالات و الإجتماعات المرئية والمسموعة والاتصالات القائمة على شبكة الإنترنت

- يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.
- يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.
- يُمنع عقد اجتماعات تتعلق بالعمل في أماكن عامة لخطورة تسريب معلومات مصنفة

أولًا: المتطلبات الفنية والأمنية الأساسية

المجال	المتطلب
التحكم بالوصول (Access Control)	تقييد الوصول لتسجيلات المكالمات للأشخاص المخولين فقط وفق مبدأ أقل صلاحية (Least Privilege).
التشفير (Encryption)	تشفير المكالمات أثناء النقل (in-transit) وبعد التخزين (at-rest) باستخدام بروتوكولات ومعايير معتمدة مثل TLS و-AES 256.
سجلات الدخول والتدقيق (Audit Logs)	تمكين تسجيل كل عمليات الوصول والاستماع والنسخ للمكالمات، وتخزينها بطريقة آمنة لمدة محددة حسب السياسة.
الاحتفاظ والتخزين (Storage & Retention)	تحديد فترة احتفاظ واضحة لتسجيلات المكالمات (مثلاً ٩٠ يومًا أو حسب الحاجة) وفق سياسة تصنيف البيانات.
النسخ الاحتياطي (Backup)	توفير آلية نسخ احتياطي مؤمّنة ومشفرة لتسجيلات المكالمات لضمان استعادتها عند الحاجة.
الحذف الآمن (Secure Disposal)	حذف التسجيلات بشكل آمن عند انتهاء فترة الاحتفاظ أو انتهاء الغرض الأمني / التشغيلي.

ثانيًا: الامتثال والتصنيف

المجال	المتطلب
تصنيف البيانات	تصنيف تسجيلات المكالمات حسب حساسيتها (حساسة - سرية - علنية) وتطبيق ضوابط ملائمة لكل تصنيف.
الامتثال للأنظمة	الالتزام بالضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني (مثل: ضوابط حماية البيانات، ECC-1 و ECC-2)، إضافة إلى أي أنظمة وطنية أخرى مثل نظام حماية البيانات الشخصية.
الخصوصية	إبلاغ المستخدمين أو الموظفين بأن المكالمات قد تكون مسجلة لأغراض تنظيمية أو أمنية، مع الحصول على الموافقة إذا لزم.

ثالثًا: التكامل مع أنظمة الأمن

المجال	المتطلب
SIEM Integration	ربط نظام تسجيل المكالمات مع نظام إدارة الأحداث الأمنية (SIEM) لمراقبة الأنشطة غير الاعتيادية أو محاولات الوصول غير المصرح به.
إدارة الهوية (IAM)	ربط الخدمة بمنصة إدارة الهويات والتحقق متعدد العوامل للوصول إلى التسجيلات.
الاختبارات الدورية	إجراء اختبارات أمنية دورية (مثل اختبار اختراق النظام وتقييم نقاط الضعف) لخدمة المكالمات.

رابعًا: الإجراءات الإدارية

- **سياسة مكتوبة لتسجيل المكالمات**: توضح الأهداف، الجهات المسؤولة، الفئات المسموح تسجيل مكالماتها، وآلية الحماية.
- **تدريب العاملين**: تأهيل المستخدمين والمسؤولين على كيفية استخدام النظام بما يضمن الخصوصية والأمان.
- **اتفاقيات عدم إفشاء (NDA)**: توقيع المشغلين والمخولين بالوصول إلى التسجيلات على اتفاقيات سرية.

خامساً: أغراض الاستخدام المصرّح بها للتسجيلات:

التدريب والتطوير: تُستخدم بعض التسجيلات كمحتوى تدريبي، مع إخفاء البيانات الحساسة.
التحقيق الأمني أو الإداري: تُستخدم كأداة دعم في التحقيقات بعد موافقة الجهات المخولة.
الإجراءات القانونية أو النزاعات: تُستخدم كأدلة قانونية عند الحاجة وبموافقة الجهات القانونية.
التوثيق التنظيمي: توثيق الاجتماعات والمكالمات التنظيمية الرسمية.

سادساً: نقاط الحماية والضمانات

- الخصوصية: إشعار الأطراف قبل التسجيل.
- التحكم في الوصول: الوصول مقيد ومراقب وفق صلاحيات محددة.
- الاحتفاظ والحذف: حذف التسجيلات بعد ٦ اشهر كحد اقصى أو حسب النظام.
- الامتثال والمراجعة: تدقيق دوري من وحدة الامتثال.

١٠.٦. الإبلاغ عن حوادث الأمن السيبراني

- يجب على جميع الموظفين والمتعاقدين والموردين أن يقوموا بإبلاغ الإدارة العامة للأمن السيبراني حال حدوث أو اكتشاف حوادث أو نقاط ضعف أو أحداث تخص الأمن السيبراني وذلك بهدف تنشيط إجراءات إدارة الحوادث والعمل على حل حوادث الأمن السيبراني في أقرب وقت ممكن حتى يتم تفادى تأثيراتها على بيئة عمل الجامعة.
- يجب أن يتم الإبلاغ عن جميع التفاصيل والأدلة الخاصة بجميع حوادث الأمن السيبراني، وكذلك نقاط الضعف أجل تسهيل عملية التحقيق في الحوادث ومعرفة أسبابها.
- يجب أن يَقوم جميع موظفي الجامعة بالإبلاغ عن أي حوادث أو معلومات تتعلق بهم من خلال القنوات التالية:
- عنوان البريد الإلكتروني للإدارة العامة للأمن السيبراني بالجامعة (Soc@kku.edu.sa للإدارة العامة للأمن السيبراني).
- رقم الهاتف أو الرقم الداخلي الخاص بالإدارة العامة للأمن السيبراني بالجامعة (٠١٧٢٤١٦٦٦٥الإدارة العامة للأمن السيبراني).

١١.٦. الحوسبة السحابية

- يجب تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة (بصيغة قابلة للاستخدام) عند انتهاء الخدمة.
- يجب فصل البيئة الخاصة بجامعة الملك خالد (وخصوصًا الخوادم الافتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
- يجب أن يكون موقع استضافة وتخزين معلومات الخاصة بالجامعة داخل المملكة، وأن يكون التخزين وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
- يجب أن تغطي متطلبات الأمن السيبراني الخاصة بحماية بيانات ومعلومات المشتركين في الحوسبة السحابية وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، بحد أدنى ما يلي:
  - وجود ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة مع مقدم الخدمة (Exit Strategy).
  - استخدام وسائل آمنة لتصدير ونقل البيانات والبنية التحتية الافتراضية.

١٢.٦ بنود الجامعة حول الحسابات وحفظ البيانات بعد التخرج أو انتهاء الخدمة

- يتم إيقاف البريد الإلكتروني للطالب بعد مرور شهر واحد من تاريخ تخرجه من الجامعة.
- تحتفظ الجامعة ببيانات البريد الإلكتروني للطالب لمدة ثلاثة أشهر بعد التخرج، وبعد انقضاء هذه المدة تُحذف البيانات بشكل نهائي ولا يمكن استرجاعها.
- يُوقف حساب الموظف على أنظمة الجامعة بما في ذلك البريد الإلكتروني بعد ثلاثة أشهر من تاريخ انتهاء العلاقة التعاقدية أو الوظيفية مع الجامعة.
- تحتفظ الجامعة ببيانات البريد الإلكتروني واسم المستخدم للموظف لمدة ستة أشهر من تاريخ الإيقاف.
- بعد انقضاء فترة الاحتفاظ المحددة، تُحذف جميع البيانات بشكل نهائي دون إمكانية استرجاعها.
- يتحمل المستخدم مسؤولية أخذ نسخة احتياطية من بياناته قبل انتهاء فترة الاحتفاظ المحددة.
- الجامعة غير مسؤولة عن فقدان أي بيانات بعد انتهاء فترات الاحتفاظ المشار إليها أعلاه.
- يُمكن للمستخدمين التواصل مع وكالة عمادة الخدمات الالكترونية لتقنية المعلومات خلال فترة الاحتفاظ للاستفسارات أو طلب نقل البيانات إن لزم الأمر.

٧. المرجعيات

- ISO/IEC 27001:2022, A.5.37
- ISO/IEC 27001:2022, A.8.32
- ISO/IEC 27001:2022, A.8.6
- ISO/IEC 27001:2022, A.8.31
- ISO/IEC 27001:2022, A.8.7
- ISO/IEC 27001:2022, A.8.13
- ISO/IEC 27001:2022, A.8.15
- ISO/IEC 27001:2022, A.8.17
- ISO/IEC 27001:2022, A.8.19
- ISO/IEC 27001:2022, A.8.8
- ISO/IEC 27001:2022, A.8.19
- ISO/IEC 27001:2022, A.8.34
- ISO/IEC 27001:2022, A.5.14
- ECC-2:2024, 2-9
- ECC-2:2024, 2-10
- ECC-2:2024, 2-11
- ECC-2:2024, 2-12

٨. الالتزام

- يجب أن تتوافق سياسة الأمن السيبراني للتشغيل مع الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني (ECC-2:2024) ومع جميع متطلبات معيار الأيزو العالمي لأمن المعلومات (ISO/IEC 27001:2013).
- ينبغي الالتزام بسياسة الأمن السيبراني للتشغيل من قِبَل جميع المستخدمين والموظفين والأطراف المعنية ذات العلاقة، ويجب على جميع مدراء الإدارات والأقسام التَأَكُد من الالتزام المُستَمر بتطبيقها.
- يَنبغي مُراجعة الالتزام بتَطبيق السياسة دَورياً بواسطة الإدارة العامة للأمن السيبراني، كما يَجِب على الإدارة العليا اتخاذ كافة الإجراءات التصحيحية اللازمة حال حدوث أي انتهاك للسياسة. ويجب أنَّ تتكافأ حِدّة الإجراءات التأديبية مع حجم الانتهاك أو جَسامة الحادِث المُرتَكَب، ويَتَحَدَّدْ ذلك بعد الانتهاء من التحقيقات اللازمة والتي بِدورها قد تُسفِر عن التالي، على سبيل المثال لا الحصر:
  - فَقْدْ امتيازات الوصول إلى الأصول المعلوماتية والتقنية.
  - عقوبات، قَدْ تَكُون مَالية، وقد تَصِل إلى إنهاء خِدمة المُوظَف، أو النزول بمستواه الوظيفي إلى درجة أقل، وذلك حَسبما تَراه الإدارة العليا مناسباً وفق الأنظمة والتعليمات والقوانين الرسمية.
  - في حال عدم الالتزام بأحد البنود يجب على جامعة الملك خالد تقديم مبررات وذكر أسباب عدم الالتزام.

٩. معايير الاستثناءات

- تَهْدُف هذه الوثيقة إلى تَلبِية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه، يَجِب تَقديم طَلَبْ رَسمِي، عند الحاجة إلى الحُصول على استثناء. ويُقَدَّم الطَلب 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.
- تَصِل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى، إلَّا أنَّه يُجوز إعادة تقييم طَلَب الاستثناء وتَجدِيد المُوافقة عليه بحد أقصى ثلاثة أعوام متتالية إذا اقتضَى الأَمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثَلاثة أعوام السالِف ذِكْرِهَا.