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

السياسة العامة للأمن السيبراني

الإصدار: يناير ٢٠٢٤ م
النسخة: ١,٢
عامة

KKUCYBERSECURITY
الإدارة العامة للأمن السيبراني
GENERAL ADMINISTRATION OF CYBERSECURITY

الوثيقة المرجعية

عنوان الوثيقة	السياسة العامة للأمن السيبراني			
التصنيف	✓ عامة	خاصة	سرية	سرية للغاية
الحالة	فعّال			
النوع	وثيقة			

الإعداد

رقم النسخة	التاريخ	إعداد
1.0	اسبتمبر ٢٠٢١م	م. عذى علي القرني
1.1	٩ مايو ٢٠٢٢م	م. فاطمة حامد الشهراني
1.2	١ يناير ٢٠٢٤ م	م. مريم الشهري

المراجعة

رقم النسخة	التاريخ	المُراجع
1.0	٢٠ أكتوبر ٢٠٢١م	م. محمد الغانم
1.1	١٦ مايو ٢٠٢٢ م	م. بدرية موسى القحطاني
1.2	٢٠ يناير ٢٠٢٤ م	م.ريناد الشهراني

الاعتماد

رقم النسخة	التاريخ	المُعتمد
1.0	٤ نوفمبر ٢٠٢١ م	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد
1.1	٢٥ مايو ٢٠٢٢م	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد
1.2	١٢ فبراير ٢٠٢٤ م	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد

المحتويات

١. المقدمة

تُمَثِّل هذه الوثيقة السياسة العامة للأمن السيبراني الخاصة بجامعة الملك خالد والمشار إليها بالجامعة داخل هذه الوثيقة.

تتكوَّن هذه الوثيقة من عشرة أقسام رئيسية لتشمل هذه المُقَدَمَة يليها الغَرَض، والنطاق، والمصطلحات والتعريفات، والأدوار والمسؤوليات، وبنود السياسة، ومراجعة سياسات الامن السيبراني والمرجعيات، والالتزام، وأخيراً معايير الاستثناءات.

على جَمَيع المستخدمين القيام بالقراءة المُتأنية والفهم الجيد والالتزام الكامل بالسياسة العامة للأمن السيبراني. وفى حالة عدم الاستيعاب أو عدم الفهم الكامل من قبَل أي مستخدم لتلك الوثيقة أو لأي جزءٌ منها، فإنه يَجَب عليه التواصل في الحال مع الإدارة العامة للأمن السيبراني حتى يتسنى له فهم النقاط الغير واضحة بالنسبة له.

تُعَدُ الإدارة العامة للأمن السيبراني بالجامعة هي المالكة لهذه 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، و أيضاً يجوز تحديثها فور حُدوث أي تعديلات أو تغييرات تتعلّق بالمُتطلبات التشريعية والتنظيمية ذات العلاقة. ويَتم تغيير رقم إصدار الوثيقة حال القيام بأي تعديل سواء كان جوهرياً أو ثانوياً. ويَنبغي اعتماد تلك التحديثات أو التعديلات من قبَلْ اللجنة الإشرافية للأمن السيبراني بالجامعة.

٢. الغرض

إن الغرض الرئيسي من هذه الوثيقة هو تأكيد وبيان التزام الإدارة العليا بدعم أهداف ومبادئ الأمن السيبراني بما يتوافق مع إستراتيجية الأمن السيبراني الخاصة بالجامعة. وكذلك توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام الجامعة بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

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.
- **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 ومعالجة 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 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 قصد. 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).

٥. الأدوار والمسؤوليات

- **الإدارة العليا**
  - إنشاء اللجنة الإشرافية للأمن السيبراني بالجامعة.
- **اللجنة الإشرافية للأمن السيبراني**
  - اعتماد جميع سياسات وإجراءات الأمن السيبراني وأمن المعلومات الجديدة أو التي تم تعديلها أو تحديثها.
  - الإلزام بنشر وتطبيق سياسات وإجراءات الأمن السيبراني داخل الجامعة بهدف حماية سرية وسلامة وتوافر جميع البيانات والمعلومات والأصول المعلوماتية والتقنية الخاصة ببيئة العمل.
  - تقديم الدعم اللازم لكل مبادرات وأهداف الأمن السيبراني.
  - تقديم الدعم اللازم لتطبيق نظام إدارة أمن المعلومات ومتطلبات الأمن السيبراني بالجامعة الذي يَشمل سائر الموارد المطلوبة مثل الموارد البشرية والتقنية والمالية.
  - متابعة تطبيق نظام إدارة أمن المعلومات ومتطلبات الأمن السيبراني بالجامعة وذلك لضمان فاعليته وكفاءتُه.
- **الإدارة العامة للأمن السيبراني**
  - الحصول على موافقة اللجنة الإشرافية للأمن السيبراني بالجامعة على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري
  - إعداد ومُراجَعة وتحديث جميع سياسات الأمن السيبراني.
  - رَفْع التقارير الدورية عن فعالية وكفاءة نظام إدارة أمن المعلومات وكذلك متطلبات وضوابط الأمن السيبراني إلى الإدارة العليا.
  - التأكُّدْ من أن نظام إدارة أمن المعلومات يتوافق مع متطلبات المعايير الدولية ISO/IEC 27001.
  - التأكُّدْ من أن سياسات الأمن السيبراني تتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة التي تنطبق على الجامعة.
  - توضيح سياسات الأمن السيبراني لجميع موظفي الجامعة، والتأكُّدْ من فَهْمَهم واستيعابهم لجميع متطلبات الأمن السيبراني.
  - عَقْد جلسات توعوية للتوعية بأهمية تطبيق متطلبات وضوابط الأمن السيبراني، وكذلك نظام إدارة أمن المعلومات لجميع الموظفين ذات العلاقة.
- **إدارة الشؤون القانونية**
  - التأكد من أن شروط ومتطلبات الأمن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين بالجامعة والاطراف الخارجية.
- **إدارة المراجعة الداخلية**
  - مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

- إدارة الموارد البشرية
  - التأكد من أن كافة الموظفين الجدد قد تلقوا التوعية المطلوبة حول سياسات الأمن السيبراني، وضمان تفهمهم لمتطلبات الأمن السيبراني ولمسؤولياتهم تجاه منظومة الأمن السيبراني.
  - تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين داخل الجامعة.
- مديري ورؤساء الإدارات الأخرى
  - دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة للجامعة.
- العاملين والموظفين
  - المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في الجامعة، والالتزام بها.

المسؤول	الإعداد والتحديث والمراجعة	الاعتماد	النشر	الالتزام
اللجنة الإشرافية للأمن السيبراني		■		
الإدارة العامة للأمن السيبراني	■		■	
جميع موظفي الجامعة وجميع الأطراف المعنية الداخلية والخارجية				■

٦. بنود السياسة العامة للأمن السيبراني

- يتعين على الإدارة العليا بالجامعة والمُمثلة في اللجنة الإشرافية للأمن السيبراني التأكيد على أهمية ضوابط ومتطلبات الأمن السيبراني ونظام إدارة أمن المعلومات والتأكيد على ضرورة التزام جميع الأطراف المعنية سواء كانت داخلية او خارجية بمتطلبات وضوابط الأمن السيبراني لضمان حماية سرية وسلامة وتوافر كافة البيانات والمعلومات والأصول المعلوماتية والتقنية الخاصة بالجامعة.
- يجب على الإدارة العليا أن تدعم بقوة تحقيق استراتيجية الأمن السيبراني الخاصة بالجامعة.
- يجب أن تتماشى استراتيجية الأمن السيبراني مع الاستراتيجية العامة للجامعة وترتبط بها ارتباطاً وثيقاً لضمان تحقيق رؤية الإدارة العليا بما يتوافق مع القوانين والتشريعات والتنظيمات ذات العلاقة وبما يتوافق أيضاً مع رؤية المملكة العربية السعودية لعام ٢٠٣٠ وسيتم إعداد الاستراتيجية الخاصة بالأمن السيبراني في وثيقة منفصلة "استراتيجية الأمن السيبراني" لتحديد الأهداف الاستراتيجية وكيفية قياسها بشكل دوري.
- يجب أن تزود الإدارة العليا نظام إدارة أمن المعلومات وبيئة الأمن السيبراني بجميع الموارد المطلوبة مثل الموارد البشرية والتقنية والمالية.
- يجب أن تدعم الإدارة العليا تحديد برنامج لبدء مراقبة ومراجعة نظام وبيئة الأمن السيبراني وفقًا للوضع الحالي في الجامعة وبالتوافق مع المتطلبات التنظيمية والتشريعية ذات العلاقة.
- يجب أن توفر الإدارة التوجيه والدعم لتنفيذ متطلبات الأمن السيبراني عبر بيئة العمل بالجامعة.

- يجب أن يتم توجيه إنشاء برنامج الأمن السيبراني وفقاً للوائح الوطنية والمواصفات الدولية وأفضل الممارسات المعروفة عالمياً لضمان ما يلي:
  - الوصول إلى المعلومات من قبل الأفراد المصرح لهم فقط، الذين لديهم صلاحية الوصول المناسبة والمعتمدة.
  - حماية سرية وسلامة وتوافر جميع البيانات والمعلومات والأصول المعلوماتية والتقنية بجميع الضوابط اللازمة.
  - تغيير وتعديل المعلومات و / أو تحديثها من قبل الأفراد المصرح لهم الذين لديهم التفويض المناسب والمعتمد.
  - أن تكون المعلومات متاحة دائمًا لجميع الأفراد المُخول لهم الوصول لتلك المعلومات واستخدامها.
- يجب إعداد ومراجعة وتحديث سياسات الأمن السيبراني من قبل الإدارة العامة للأمن السيبراني، واعتمادها من قبل اللجنة الإشرافية للأمن السيبراني، ونشرها لجميع الأطراف المعنية الداخلية والخارجية.
- يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تأمين تقنية مثل، على سبيل المثال لا الحصر، نظام التشغيل وقواعد البيانات والجدران النارية.
- يجب على الإدارة العامة للأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها وفقاً للضوابط الأساسية للأمن السيبراني ولجميع المتطلبات التشريعية والتنظيمية ذات العلاقة.
- يجب على الإدارة العامة للأمن السيبراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام الجامعة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجامعة، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل اللجنة الإشرافية للأمن السيبراني بالجامعة. كما يجب إطلاع العاملين المعنيين في الجامعة والأطراف ذات العلاقة عليها
- يجب على الإدارة العامة بالأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:
  ١. **برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
  ٢. **أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)** لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني.
  ٣. **برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية، وذلك وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.
  ٤. **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Projects)** للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة المشاريع وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٥. **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Regulatory Cybersecurity Compliance)** للتأكد من أن برنامج الأمن السيبراني متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٦. **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)** للتأكد من أن ضوابط الأمن السيبراني مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً.

٧. **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٨. **برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)** للتأكد من أن العاملين لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٩. **سياسة إدارة الأصول (Asset Management)** للتأكد من أن جامعة الملك خالد لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة، من أجل دعم العمليات التشغيلية ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها ودقتها وتوافرها.

١٠. **سياسة إدارة هويات الدخول والصلاحيات (Identity and Access Management)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجامعة الملك خالد

١١. **سياسة حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)** لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية من المخاطر السيبرانية.

١٢. **سياسة حماية البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني من المخاطر السيبرانية.

١٣. **سياسة إدارة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات من المخاطر السيبرانية.

١٤. **سياسة أمن الأجهزة المحمولة (Mobile Devices Security)** لضمان حماية الأجهزة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بالأعمال وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين (مبدأ "BYOD").

١٥. **سياسة حماية البيانات والمعلومات (Data and Information Protection)** لضمان حماية السرية، وسلامة البيانات والمعلومات ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١٦. **سياسة التشفير ومعياره (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية وذلك وفقاً للسياسات، والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١٧. **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية البيانات والمعلومات، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

١٨. **سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على الأعمال.

١٩. **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢٠. **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)** لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على الأعمال أو تقليلها.

٢١. **سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)** لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على الأعمال مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤٣٨\٨\١٤هـ.

٢٢. **سياسة الأمن المادي (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢٣. **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية من المخاطر السيبرانية.

٢٤. **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Resilience Cybersecurity)** لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية الأعمال، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

٢٥. **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing Cybersecurity)** لضمان حماية الأصول من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة " Managed Services") وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢٦. **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (Cloud and Computing Hosting Cybersecurity)** لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

٢٧. **سياسة أمن الخوادم (Servers Security)** لضمان حماية خوادم جامعة الملك خالد من المخاطر السيبرانية.

٢٨. **سياسة إدارة حزم التحديثات والإصلاحات (Patch Management)** لضمان ادارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بجامعة الملك خالد وتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

٢٩. **سياسة أمن قواعد البيانات (Database Security)** لضمان حماية قواعد البيانات لجامعة الملك خالد من المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

٣٠. **سياسة الحماية من البرمجيات الضارة (Anti-Malware security)** لضمان حماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بجامعة الملك خالد من تهديدات البرمجيات الضارة

- يحق للإدارة العامة بالأمن السيبراني الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.
- يجب على جميع موظفي الجامعة الالتزام والتوافق مع جميع سياسات الأمن السيبراني.
- يجب استخدام البيانات والمعلومات لأغراض العمل المصرح بها فقط.
- جميع الوثائق الخاصة بالأمن السيبراني والتي تشمل السياسات والإجراءات يجب ان تصنف على انها خاصة.
- يجب على الإدارة العامة للأمن السيبراني تقديم جلسات توعوية عن سياسات الأمن السيبراني وأهميتها لجميع موظفي الجامعة.
- يجب على الإدارة العامة للأمن السيبراني القيام بنشر جميع السياسات التي تم اعتمادها لجميع موظفي الجامعة وجميع الأطراف المعنية ذات الصلة.
- يجب على الإدارة العامة للأمن السيبراني القيام باستخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لجميع ضوابط ومتطلبات الأمن السيبراني بالجامعة لضمان التطوير المستمر لها ويشمل ذلك جميع السياسات والإجراءات والمعايير التقنية والمنهجيات والأطر وغيرها من ضوابط ومتطلبات الأمن السيبراني. كما يجب على الإدارة العامة للأمن السيبراني استخدام هذه المؤشرات بصورة دورية مستمرة على الأقل مرة كل عام للتأكد من تطبيق جميع الضوابط والمتطلبات.

[ISO/IEC 27001:2013, A.5.1.1]

٧. مراجعة سياسات الأمن السيبراني

- يجب ان يتم مراجعة وتحديث السياسات والإجراءات والمعايير التقنية وكافة الضوابط والمتطلبات الخاصة بالأمن السيبراني على الأقل مرة واحده كل عام أو عند حدوث أية تغييرات في القوانين والتشريعات ذات الصلة. ويجب اعتماد هذه التحديثات او التغييرات بواسطة اللجنة الإشرافية للأمن السيبراني وتوثيقها.
- يجب على الإدارة العامة للأمن السيبراني بالجامعة قياس فاعلية تطبيق ضوابط الأمن السيبراني على الأقل مرة واحدة سنوياً لتفادي حدوث أية حوادث خاصة بالأمن السيبراني ولتقليل التأثير الناتج عنها، ويجب أخذ القياسات التالية في الاعتبار:
    - ملاحظات وتعليقات جميع الإدارات ذات الصلة.
    - تقارير حوادث الأمن السيبراني التي تم الإبلاغ عنها.
    - نتائج مراجعات الإدارة العليا المستقلة.
    - مخاطر الأمن السيبراني ذات الصلة.
- يجب الحصول على موافقة اللجنة الإشرافية للأمن السيبراني على سياسات الأمن السيبراني وتوثيق الموافقة والاعتماد من خلال اجتماعات اللجنة الإشرافية للأمن السيبراني الرسمية أو من خلال التوقيع على قائمة الوثائق الرئيسية التي تتضمن تفاصيل حول السياسات والإجراءات والمستندات الأخرى مع الاسم والإصدار والمالك والتصنيف وما إلى ذلك.
- يجب مراجعة طلبات الاستثناءات قبل الموافقة عليها ولا يمكن الموافقة عليها تلقائيًا. لا ينبغي الموافقة على طلبات الاستثناءات التي قد تسبب مخاطر كبيرة لبيئة الأعمال دون وجود ضوابط بديلة. كما يجب أيضاً مراجعة طلبات الاستثناءات المعتمدة بشكل دوري للتأكد من أن الافتراضات أو ظروف العمل لم تتغير.

[ISO/IEC 27001:2013, A.5.1.2]

٨. المرجعيات

- ISO/IEC 27001:2013, A.5.1
- ECC-1:2018, 1-3

٩. الالتزام

- يجب أن تتوافق السياسة العامة للأمن 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 بالسياسة العامة للأمن السيبراني 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 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 تُسفر 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 والقوانين الرسمية.

١٠. معايير الاستثناءات

- تهْدُف هذه الوثيقة إلى تلبَية جميع مُتطلّبات الأمن السيبراني. وبُنَاءً عليه، يَجَب تقديم طلَبْ رَسمَي، عند الحاجة إلى الحُصول على استثناء. ويُقدَّم الطلَب إلى الإدارة العامة للأمن السيبراني، مع ذكْر حيثيات طلب الاستثناء بوضوح، وعَرْض الفوائد المَرْجُوَّة من هذا الاستثناء، ليتم البَتّ فيه ومَنْح الموافقة النّهائية من قِبَلْ اللجنة الإشرافية للأمن السيبراني.
- تصَل فترة الاستثناء لمُدَّة عام واحد كَحدّ أقصى، إلّا أنّه يُجوز إعادة تقييم طلَب الاستثناء وتجدَيد المُوافقة عليه بحد أقصى ثلاث أعوام متتالية إذا اقتضَى الأمر، ولا يَجُوز مَدّ العَمَل بالاستثناء لفترات أُخرى بعد انتهاء الثلاث أعوام السالف ذكْرَهُم.