مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة مراقبة أمن المعلومات			
النسخة:	١,٠			
التصنيف:	◉ عامة	○ سرية	○ سرية عالية	○ سرية للغاية
الحالة:	معتمده	**النوع :**	وثيقة	
تاريخ الإصدار:	٢٠١٥/٠٦/٢٥			
تاريخ المراجعة:	٢٠١٥/٠٦/٢٥			

النسخة رقم	التاريخ	إعداد ومراجعة	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	الإدارة العامة لتقنية المعلومات (قسم أمن المعلومات)	النسخة الأولى من الوثيقة

الموظف المختص

النسخة رقم	التاريخ	المختص	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	محمد الشهري	تم المراجعة

الإعتماد

النسخة رقم	التاريخ	المعتمد/ المعتمدين	الملاحظات
١,٠	٢٠١٥/٠٧/٠٨	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد	

جدول المحتويات

١. تعريف هيكلة السياسة

تشتمل 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.
- **الإمتثال والتنفيذ:** تحدد تبعات ونتائج أية مخالفة لهذه الساسة.
- **السياسات:** يشتمل هذا القسم على وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.

٢. الهدف

الغرض من هذه السياسة هو التأكد من أن مراقبة حالة أمن المعلومات المتعلقة بأنظمة معلومات جامعة الملك خالد تتم بشكل دائم من خلال تخطيط ونشر أساليب أمنية ملائمة بما يتوافق مع المخاطر ومدى حساسية وأهمية أنظمة المعلومات.

٣. نطاق العمل

تطبق هذه السياسة على جميع الموظفين، والموردين، وشركاء العمل، والموظفين المتعاقدين، والوحدات الوظيفية لدى جامعة الملك خالد سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم. كما تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٤. الإمتثال و التنفيذ

في حالة مخالفة أي موظف أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لدى جامعة الملك خالد لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر- نظام العمل والعمال، ونظام مكافحة الجرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٥. **السياسات** :

- **مراقبة أمن المعلومات بناءً على المخاطر**

- يجب أن تقوم جامعة الك خالد بمراقبة أمن المعلومات بناءً على المخاطر التي تم اكتشافها.
- يجب أن تقوم الإدارة العامة لتقنية المعلومات بالتخطيط لأنشطة المراقبة الأمنية باستخدام إجراءات مراقبة وتقييم أمن المعلومات.
- يجب أن يتم تخطيط وتنفيذ مراقبة أمن المعلومات لأنظمة المعلومات بناءً على حساسية وأهمية وتصنيف المخاطر المتعلقة بأنظمة معلومات الجامعة حسبما تتقضي درجات التصنيف الأمني المعطاة لتلك الأنظمة (عامة، سرية، سرية عالية، سرية للغاية).
- يجب أن تحدد في وثيقة خطة المراقبة الأمنية المبنية على المخاطر الأشخاص الرئيسيين المعنيين والعمليات والضوابط المتعلقة بالتقنية الواجب مراقبتها بالنسبة لأي نظام مفرد أو مجموعة من أنظمة المعلومات، وذلك حسبما هو محدد في السياسة الأمنية المتعلقة بذلك النظام أو تلك الأنظمة والمتطلبات القانونية والنظامية الواجب تطبيقها وأفضل الممارسات الأخرى في هذا الصدد.
- يجب أن تكون الإدارة العامة لتقنية المعلومات مسؤولة عن مراقبة أمن المعلومات لأنظمة معلومات الجامعة بناءً على مسئولياتها المخطط لها والمتعلقة بالمراقبة الأمنية.

- **إدارة التحديثات و ملفات الرقع الأمنية**

- يجب أن تقوم الإدارة العامة لتقنية المعلومات بالتأكد من أنه تم تحديد وفحص وتطبيق كافة الرقع والتحديثات الأمنية لكافة أنظمة المعلومات بالسرعة الواجبة.
- عندما يتطلب الأمر، وفي حالة الخدمات الإلكترونية الحساسة المنشورة على موقع الجامعة، فإنه يمكن للجامعة الإشتراك في خدمات مراقبة أمن المعلومات لدى طرف ثالث معتمد بحيث يصل للإدارة العامة لتقنية المعلومات إشعارات بشأن الأنشطة الغير مصرح بها عبر الموقع.
- يجب على جامعة الملك خالد أن تتأكد من وجود آليات مناسبة في أنظمة معلوماتها لتسجيل الحوادث الأمنية تقتضيه خطط المراقبة الأمنية لتلك الأنظمة، ويشمل ذلك دون حصر:
  - سجلات محاولات دخول النظام الناجحة والمرفوضة.
  - سجلات المحاولات الناجحة والمرفوضة للوصول للبيانات والموارد الأخرى.
  - التغييرات على إعدادات النظام.
  - استخدام الامتيازات.
  - استخدام وسائل وتطبيقات النظام.
  - الملفات التي تم الوصول إليها ونوع الوصول.
  - عناوين وبروتوكولات الشبكة المستخدمة.

- تنشيط وتعطيل أنظمة الحماية مثل أنظمة مكافحة الفيروسات.
- سجلات الكشف عن/ منع الإختراقات إلى النظام.
- سجلات جدار الحماية.
- سجلات أخطاء النظام.
- النسخ الاحتياطية من البيانات وسجلات الاسترجاع.
- الأنشطة الهاتفية - تقارير تفاصيل المكالمات.

- **التقارير الإدارية**

- يجب أن يتم استخراج عدد ملائم من التقارير الإدارية بصفة شهرية وفي الأوقات المحددة، ومن ثم تقديمها إلى الإدارة العامة لتقنية المعلومات لإطلاعهم بشأن الوضع الأمني الخاص بأنظمة المعلومات لدى الجامعة بشكل مستمر.