مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة تطبيقات البريد الإلكتروني			
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 ٣
٢. الهدف ٣
٣. نطاق العمل ٣
٤. الإمتثال و التنفيذ ٣
٥. السياسات ٤

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 والسياسات ذات العلاقة هو، تقديم الإرشادات الأمنية التي تتيح للطلاب والموظفين بالجامعة التواصل بفعالية ومسؤولية من خلال تطبيقات البريد الإلكتروني.

٣. نطاق العمل

تطبق هذه السياسة على جميع مستخدمين خدمة البريد الإلكتروني المقدمة من قبل جامعة الملك خالد.

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 :

- يجب القيام بالكشف عن ومنع الشفرات الخبيثة من الوصول إلى تطبيقات البريد الإلكتروني وفقاً لسياسة الكشف عن الشفرات الخبيثة لدى الجامعة (يرجى الرجوع الى السياسات العامة لأمن المعلومات).
- يجب استخدام برنامج مكافحة الفيروسات (إلزامي)، برنامج مكافحة التجسس، نظام الكشف عن الاختراقات المعتمد على المضيف (Host based IDS)، جدار الحماية لأجهزة سطح المكتب، و نظام منع الاختراقات (IPS).
- يجب ألا تكشف رسائل الأخطاء الصادرة من تطبيقات البريد الإلكتروني عن أية معلومات لا يُرغب الكشف عنها مثل تفاصيل أنظمة التشغيل، إطار التطوير، أو أخطاء قاعدة البيانات.
- يجب أن تحظى تطبيقات البريد الإلكتروني بالقدرة على معالجة وتخزين المعلومات الحساسة بصيغة نصوص مشفرة في التطبيق، مثل المعلومات الشخصية وسجلات الطلاب.
- يجب أن تحتفظ تطبيقات البريد الإلكتروني بختم زمني لجميع العمليات.
- يجب الكشف عن مرفقات البريد الإلكتروني، بصرف النظر عن مصدرها أو محتواها، للتأكد من عدم احتوائها على فيروسات أو أي برامج تجسس أو برامج خبيثة قبل تنفيذها أو تخزينها.
- يجب إعداد تطبيق البريد الإلكتروني بحيث يتضمن البريد الإلكتروني الصادر على بيان إخلاء المسؤولية، مثل النص التالي: "تنويه: إن هذا البريد الإلكتروني وما يحويه من ملفات مرفقه تعتبر سرية، ويقصد منها الإستخدام الحصري من قبل الشخص أو الأشخاص المرسلة إليهم، والوصول إلى هذا البريد من قبل أي شخص آخر يعتبر غير مصرح به. إذا لم تكن الشخص المقصود؛ يرجى حذف البريد الإلكتروني وتدمير أي نسخ منه، أي كشف أو نسخ أو توزيع لمحتوى هذا البريد محضور ويتعبر مخالفة قانونية. محتوى هذا البريد ومرفقاته يمكن أنه تم تغييرها، العبارات والآراء الواردة في هذا البريد تعبر عن المرسل ولا تعكس بالضرورة آراء جامعة الملك خالد."
- يجب أن تتأكد تطبيقات البريد الإلكتروني من عدم إنكار الاتصال/ التعامل باستخدام تقنية مناسبة مثل التصديق/التوقيع الرقمي.