مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة الحماية من الشفرات الخبيثة			
النسخة:	١,٠			
التصنيف:	◉ عامة	○ سرية	○ سرية عالية	○ سرية للغاية
الحالة:	معتمده	**النوع :**	وثيقة	
تاريخ الإصدار:	٢٠١٥/٠٦/٢٤			
تاريخ المراجعة:	٢٠١٥/٠٦/٢٤			

النسخة رقم	التاريخ	إعداد ومراجعة	الملاحظات
١,٠	٢٠١٥/٠٦/٢٤	الإدارة العامة لتقنية المعلومات (قسم أمن المعلومات)	النسخة الأولى من الوثيقة

الموظف المختص

النسخة رقم	التاريخ	المختص	الملاحظات
١,٠	٢٠١٥/٠٦/٢٤	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 حماية نظم معلومات جامعة الملك خالد من البرامج الضارة (مثل الفيروسات والديدان و أحصنة طروادة وقنابل البريد الإلكتروني ، الخ).

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.

٥. **السياسات** :

- **استخدام حلول لمضادات الفيروسات معتمده دوليا**

- يجب أن تكوّن جامعة الملك خالد آلية واضحة المعالم لمنع وكشف الفيروسات/الشيفرات الخبيثة واستعادة النظم المصابة بطريقة سليمة وفي الوقت المناسب.
- يجب ان تمتلك جامعة الملك خالد، برامج مكافحة الفيروسات المعترف بها دوليا، تدار مركزيا تثبت وتنشط في جميع الأوقات لجميع نظم المعلومات، وكذلك النظم غير المملوكة لجامعة الملك خالد أو البنية التحتية في شبكتها.
- جميع الأجهزة المملوكة وغير المملوكة لجامعة الملك خالد يجب أن تفحص عن الفيروسات/الشيفرات الخبيثة قبل أن تتصل بشبكة الجامعة.
- يجب أن تنفذ تكنولوجيا مكافحة الفيروسات في النقاط الطرفية التي يمكن من خلالها إدخال الفيروسات/الشيفرات الخبيثة في شبكة الجامعة.
- يجب أن يتم نشر تحديثات أدوات مكافحة الفيروسات من خلال وسائل آلية في أقرب وقت من صدورها.
- يجب تهيئة أنظمة المعلومات وذلك لمنع المستخدمين من تعطيل أدوات مكافحة الفيروسات.
- يجب أن يتم التثبيت التلقائي لبرامج مكافحة الفيروسات على أي نظام معلومات يتصل بشبكة الجامعة إذا لم تكن مثبتة بالفعل.
- يجب تنفذ التدابير التقنية التالية:

- يجب تهيئة برنامج مكافحة الفيروسات للتحقق من أنه قيد التشغيل في كل وقت على أجهزة المستخدم (أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة ، الخ) عن طريق سحب حالة العميل كل ٥ دقائق. إذا تم الكشف عن عميل غير قابل للوصول في حين أن (أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة ، الخ) قابلة للوصول وهذا يعني العميل لا يعمل .
- يجب على خادم مكافحة الفيروسات منع الوصول الى شبكة الجامعة إلى أن يعمل العميل مرة أخرى.

- في الحالات التي يكون فيها الخادم لمكافحة الفيروسات الرئيسي لا يمكن الوصول إليه، يتعين على أفراد مكتب الدعم الفني توجيه المستخدمين حول كيفية تثبيت تحديثات مكافحة الفيروسات، وتوفر لهم التحديثات في شكل مناسب (مثل ملف قابل للتنفيذ أو ملف التوقيع الفيروس).
- يجب أن يتم تهيئة أدوات مكافحة الفيروسات بحيث تُمكن لمسح كافة محركات الأقراص القابلة للإزالة ووسائط التخزين المتصلة بنظم المعلومات.
- يجب أن يتم تهيئة أدوات مكافحة الفيروسات والبرامج الضارة لإجراء مسح تلقائي وبشكل دوري على جميع أجهزة الكمبيوتر الشخصية والخوادم و أجهزة الكمبيوتر المحمولة وغيرها من مكونات نظم المعلومات للجامعة على فترات دورية محددة للكشف عن الفيروسات و/أو الأكواد الضارة المحتملة.

- يجب أن يتم تكوين سجلات برامج مكافحة الفيروسات لإلتقاط أقصى مستوى من التفاصيل كما يجب عدم السماح بتنقية هذه السجلات.
- سجلات برامج مكافحة الفيروسات يجب ان تنسخ احتياطيا ويجب أن تكون متوفرة لمتطلبات التحيقيقات في حالة حدوث هجوم أو حادثة أمنية.
- تكون الإدارة العامة لتقنية المعلومات مسؤولة لضمان بقاء البنية التحتية للكشف عن الفيروسات/الأكواد الضارة نشطة و لا يمكن تعطيلها في أي نقطة دخول محتملة.

- **مسؤوليات المستخدم**

- يجب أن يتوخى المستخدمين الحذر عن تنزيل الملفات من الإنترنت.
- يجب على المستخدمين عدم فتح أو تنزيل أو تنفيذ أي ملفات أو روابط بريد إليكتروني مستلمة من قبل مصادر مجهولة أو غير موثوقة.
- يحظر المستخدمين من تغيير تكوين أو إزالة أوإلغا تفعيل أو العبث مع أي برامج الحماية ضد الفيروسات / الضارة التي تم تثبيتها على نظام المعلومات المستخدمة من قبلهم .
- يجب على المستخدمين الإبلاغ عن جميع الحوادث من الفيروسات/البرامج الضارة (تم الكشف عنها من قبل برامج الحماية) وكذلك أي سلوك غير طبيعي على الفور إلى الإدارة العامة لتقنية المعلومات.
- يجب أن يتحقق المستخدمين من فحص الوسائط المتبادلة مع الأقسام الأخرى قبل إستخدامها في أنظمتهم.

- **إزالة الفيروسات والبرامج الضارة من نظم معلومات جامعة الملك خالد**

- جميع الفيروسات والبرامج الضارة المكتشفة على أنظمة الجامعة يجب أن تزال مباشرة. كما يجب أن لا يسمح لنظم المعلومات المحتوية على فيروسات أو برامج ضارة أو على برامج مكافحة فيروسات معطلة من الإتصال بشبكة الجامعة.
- يجب أن تصمم برامج مضادات الفيروسات بحيث تتم إزالة البرامج الضارة والفيروسات المكتشفة على أنظمة الجامعة بشكل تلقائي.