

### مرجعية الوثيقة

الوصف				
سياسة التوعية بأمن المعلومات		عنوان الوثيقة:		
١,٠		النسخة:		
<input type="radio"/> سرية للغاية	<input type="radio"/> سرية عالية	<input type="radio"/> سرية	<input checked="" type="radio"/> عامة	التصنيف:
وثيقة		النوع:	معتمه	الحالة:
			٢٠١٥/٠٦/٢٤	تاريخ الإصدار:
			٢٠١٥/٠٦/٢٤	تاريخ المراجعة:

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

### الموظف المختص

الملاحظات	المختص	التاريخ	النسخة رقم
تم المراجعة	محمد الشهري	٢٠١٥/٠٦/٢٤	١,٠

### الإعتماد

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

## جدول المحتويات

١. تعريف هيكلية السياسة..... ٣
٢. الهدف..... ٣
٣. نطاق العمل..... ٣
٤. الإمتثال و التنفيذ..... ٣
٥. السياسات..... ٤
- برنامج التوعية..... ٤
- التوعية بمخاطر الخدمات المقدمة عبر الانترنت..... ٤

## ١. تعريف هيكلية 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 تزويد المستخدمين لدى جامعة الملك خالد بالتوعية المناسبة فيما يتعلق بأمن المعلومات وبتحديات أمن المعلومات، وسياسات وإجراءات ومعايير أمن المعلومات لدى الجامعة بناءً على احتياجات العمل.

## 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 بيانات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

## ٤. الإمتثال والتنفيذ

في حالة مخالفة أي موظف أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لدى جامعة الملك خالد لهذه السياسة فسيعرض 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 :

### ○ برنامج التوعية

- يتعين على الجامعة نشر التوعية الفاعلة بأمن المعلومات بين موظفيها والأطراف الثالثة ذات العلاقة وعملائها، وذلك من خلال تطوير خطة رسمية للتوعية الأمنية.
- تساعد خطة التوعية الأمنية في التخطيط الفاعل لمبادرات أمن المعلومات لدى الجامعة.
- يجب أن تحدد خطة التوعية بمخاطر أمن المعلومات الأطراف المستهدفة، ورسائل أمن المعلومات التي سيتم تبليغها، وقنوات الاتصال، وجدول تنفيذ أنشطة التوعية بأمن المعلومات.
- على الإدارة العامة لتقنية المعلومات الاضطلاع بمسؤولية تطوير وإعداد وتنفيذ وابقاء خطة التوعية بأمن المعلومات.
- ينبغي على جميع موظفي ومتعاقد وموردي الجامعة أن يحضروا فعاليات وأنشطة التوعية المتعلقة بأمن المعلومات للتأكد من تحقيق مستوى مقبول من الإلتزام الأمني بسياسات أمن المعلومات لدى الجامعة.
- يجب أن يتم نشر نسخة محدثة من الوثائق الرسمية لسياسات وأحكام وشروط الخدمة وسياسات الخصوصية المتعلقة بأمن المعلومات لدى الجامعة، والتي يتم تطبيقها على العملاء والأطراف الخارجية. ينبغي نشر هذه الوثيقة في مكان واضح ومرئي ضمن الموقع الإلكتروني للجامعة.
- ينبغي على الجامعة تطبيق إجراءات محددة وقابلة للقياس للتأكد من فهم العملاء لمسؤولياتهم وإلتزاماتهم نحو أمن المعلومات.

### ○ التوعية بمخاطر الخدمات المقدمة عبر الإنترنت

- يجب تشجيع مستخدمي خدمات الإنترنت المقدمة من الجامعة على حماية أنظمة الحاسوب الخاصة بهم وأي أجهزة أخرى لديهم و التي تستخدم لتنفيذ العمليات. و يجب تأمين هذه الحماية من خلال استخدام برامج أمنية متكاملة وحديثة وقابلة للتطبيق مثل برامج مكافحة الفيروسات، برامج مكافحة التجسس، برامج مكافحة الرسائل الاحتمالية، وتقنيات برامج الحماية (جدار الحماية).
- يجب أن تقدم الجامعة برنامجاً للتوعية الأمنية يهدف إلى تعليم منسوبي الجامعة بشأن سرية أسم المستخدم وكلمة المرور الخاصة بكل فرد والتهديدات الأمنية والتدابير المضادة.
- كجزء من برنامج التوعية بأمن المعلومات الذي تقدمه الجامعة لموظفيها ومنسوبيها، فإن على الجامعة أن ترفع من وعي موظفيها ومنسوبيها بشأن عمليات الاضطهاد الإلكتروني و الهجوم على بروتوكول التوثيق باعتراض البيانات وبرامج الخداع الأخرى. كما يجب توعية الموظفين والعملاء بالدور المناط بهم في هذا الصدد (ويشمل ذلك التبليغ عن أي حادثة فوراً إلى الجامعة) إذا اشتبهوا بوجود مثل هذه الحوادث.