

مرجعية الوثيقة

الوصف				
سياسة شراء وتطوير أنظمة 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:	معتمده	الحالة:
			٢٠١٥/٠٦/٢٥	تاريخ الإصدار:
			٢٠١٥/٠٦/٢٥	تاريخ المراجعة:

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

الموظف المختص

الملاحظات	المختص	التاريخ	النسخة رقم
تم المراجعة	محمد الشهري	٢٠١٥/٠٦/٢٥	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 والتفويض ٣
٥. السياسات ٤
- التخطيط المسبق لمتطلبات أمن المعلومات القائمة على المخاطر ٤
- الأمن في تطوير/تنفيذ أنظمة المعلومات ٤
- الإعدادات الأساسية ٥
- أمن وثائق النظام ٥
- اعتبارات أمنية عند إجراء تعديلات على أنظمة المعلومات ٥
- اعتبارات أمنية إضافية عند شراء أنظمة مطورة من دول أجنبية ٥

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 التأكد من التكامل الأمني طوال دورة حياة شراء وتطوير أنظمة المعلومات لدى جامعة الملك خالد.

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.

٥. السياسات :

○ التخطيط المسبق لمتطلبات أمن المعلومات القائمة على المخاطر

- يجب على جامعة الملك خالد أن تطور وتحافظ على وثيقة متكاملة لإدارة دورة حياة تطوير النظام لجميع عمليات تطوير الأنظمة والتطبيقات. وتشمل وثيقة دورة حياة تطوير النظام بحد أدنى ما يلي:
 - بدء المشروع (التخطيط).
 - تحديد المتطلبات (التحليل).
 - تصميم النظام.
 - تطوير النظام.
 - الفحص.
 - التنفيذ والدعم.
- يجب تحديد المتطلبات الأمنية لأنظمة معلومات جامعة الملك خالد بشكل مسبق كجزء من مرحلة التخطيط وتحليل المتطلبات في دورة حياة تطوير/شراء النظام.
- يجب تبرير المتطلبات الأمنية والموافقة عليها وتوثيقها كجزء من الدراسة العملية الشاملة لكل نظام من أنظمة المعلومات.
- يجب على جامعة الملك خالد أن تقوم بتخطيط متطلبات أمن المعلومات استناداً إلى المخاطر. وعليه فإنه ينبغي التخطيط لمتطلبات أمن المعلومات لكل من أنظمة المعلومات بناءً على مستويات تصنيفها الأمني (عامة، سرية، سرية عالية، سرية للغاية) وكذلك الأخذ بكل من الضوابط في المعايير الأمنية المحددة لكل نظام لدى الجامعة وأفضل الممارسات المطبقة بهذا الصدد.
- على الإدارة العامة لتقنية المعلومات أن تقوم بتحديد المتطلبات الأمنية لأنظمة المعلومات لدى الجامعة.

○ الأمن في تطوير/ تنفيذ أنظمة المعلومات

- يجب أن تتأكد الإدارة العامة لتقنية المعلومات من التطبيق الملائم للمتطلبات الأمنية المحددة لنظام المعلومات أثناء دورة حياة تطوير/شراء ذلك النظام.
- يجب أن تخضع أنظمة المعلومات لدى جامعة الملك خالد إلى التقييم/ الفحص الأمني في مرحلة التنفيذ. ويتم إجراء التقييم/ الفحص الأمني وفقاً لتصنيف المخاطر لنظام المعلومات، ومعايير الأمن المحددة للنظام المعني وأفضل الممارسات المطبقة بهذا الصدد لدى الجامعة.
- يجب أن يتم تغيير أسماء المستخدمين وكلمات المرور الافتراضية لجميع أنظمة المعلومات عند إعداد الأنظمة التي تم شراؤها وقبل تطبيقها.
- يجب أن يتم مراقبة نتائج الاختبارات الأمنية وحمايتها من الدخول غير المصرح به إليها.

○ الإعدادات الأساسية

- يجب على جامعة الملك خالد تطوير وتوثيق والحفاظ على وجود إعدادات أساسية حديثة لنظام المعلومات الجديد.
- يجب على جامعة الملك خالد تحديث الإعدادات الأساسية لنظام المعلومات كجزء متكامل من عملية تركيب أجزاء نظام المعلومات.

○ أمن وثائق النظام

- يجب أن يقتصر الوصول إلى وثائق تصميم وتطوير عمليات النظام على الأشخاص المصرح لهم فقط والذين يؤدون مهام رسمية.

○ اعتبارات أمنية عند إجراء تعديلات على أنظمة المعلومات

- يجب أن تقوم الإدارة العامة لتقنية المعلومات بالتأكد من أن التغييرات الأساسية في الأنظمة تطبق وفقاً لسياسة التغيير لدى الجامعة (راجع السياسات الأمنية العامة) و لهذا ينبغي تحديد التعامل مع عواقب أمن المعلومات المتعلقة بذلك التغيير قبل إجرائه.

○ اعتبارات أمنية إضافية عند شراء أنظمة مطورة في دول أجنبية

- قبل شراء أي نظام من أنظمة المعلومات، فإنه يجب على جامعة الملك خالد أن تتأكد من الإلتزام بالأنظمة والقوانين واللوائح المتعلقة بهذا الصدد و كذلك الإلتزام بإجراءات المشتريات الحكومية المتبعة في المملكة العربية السعودية بخصوص حيازة، أو شراء، أو تطوير، أو تصنيع أنظمة المعلومات من الدول الأجنبية.
- لا يحق للجامعة شراء أي نظام معلومات تم تطويره/تصنيعه لدى دولة غير صديقة وفقاً للسياسات والإجراءات الحكومية في المملكة العربية السعودية.
- يتطلب قيام طرف ثالث بتطوير/تنفيذ أنظمة معلومات ذات مخاطر حساسة أو ذات مخاطر عالية ما يلي:
 - إخضاع نظام المعلومات قبل قبوله إلى الإختبارات الأمنية الدقيقة (بما في ذلك مراجعة الشفرة المصدرية حينما ينطبق ذلك).
 - أن يكون لدى موظفي تصميم/تنفيذ النظام المعني التابعين للطرف الثالث تصاريح أمنية للعمل في المشاريع الحكومية السعودية.