

مرجعية الوثيقة

الوصف				
سياسة إدارة مخاطر أمن 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:	معمده	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 والتفويض ٣
 ٥. السياسات ٤
- إلزام جامعة الملكة خالد بإدارة مخاطر أمن المعلومات ٤
 - تقييم المخاطر استنادا على سير العمل ٤
 - تخفيف المخاطر و القبول بها 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 قيام جامعة الملك خالد باكتشاف و تحديد مخاطر أمن المعلومات المتعلقة بأنظمة المعلومات لديها مع الأخذ في الاعتبار التهديدات ونقاط الضعف التي تعاني منها تلك الأنظمة وأثر ذلك على سير العمل. كما تقوم الجامعة بالتخطيط لاتخاذ مبادرات مناسبة لمعالجة مخاطر أمن المعلومات التي تم تحديدها.

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

○ التزام جامعة الملكة خالد بإدارة مخاطر أمن المعلومات

- على إدارة الجامعة أن تتأكد من أنه تم تحديد مخاطر أمن المعلومات لدى الجامعة وإدارتها بشكل فاعل وبكفاءة وبالسرعة الواجبة مع الأخذ في الاعتبار آثار تلك المخاطر على نشاط الجامعة.
- يجب تقييم مخاطر أمن المعلومات وإدارتها كجزء من أنشطة العمل لدى الجامعة، ومثال ذلك العمليات اليومية لسير العمل، حيازة أنظمة المعلومات، التطوير والتنفيذ، عمليات أنظمة المعلومات، وغير ذلك، من خلال التأكد من التطبيق المناسب لسياسات ومعايير أمن المعلومات لدى الجامعة.

○ تقييم المخاطر استنادا على سير العمل

- يمكن تقييم المخاطر على مستويات متعددة اعتمادا على غزارة التفاصيل المطلوبة. يجب أن يعتمد أسلوب موظفي جامعة الملك خالد والأطراف الثالثة المعنية لتقييم مخاطر أنظمة المعلومات لدى الجامعة على مدى حساسية وأهمية تلك الأنظمة للجامعة أي بأخذ درجة التصنيف المعطاة لأمن تلك الأنظمة بعين الاعتبار.
- يجب أن يتم تقييم مخاطر أمن جميع أنظمة المعلومات من خلال:
 - فهم التصنيف الأمني لنظام المعلومات طبقاً لسياسة الجامعة.
 - تحديد الضوابط الأمنية المطلوبة لأنظمة المعلومات (بناءً على نوعها ومستوى تصنيفها الأمني) بالرجوع إلى سياسات أمن المعلومات لدى الجامعة والمعايير المحددة للنظام وأفضل الممارسات الأخرى في هذا الصدد.
 - تقييم حالة تلك الضوابط من خلال مناقشتها مع أصحاب المصالح الرئيسية المعنيين بالأمر أو إجراء أساليب فحص أمنية مناسبة.
- يجب ان تقوم جامعة الملك خالد بإجراء تنقيح تفصيلي لمعايير الأمن المحددة لأنظمة المعلومات المصنفة على أنها ذات مخاطر عالية وذلك من خلال إتباع منهجية تقييم رسمية لمخاطر أمن المعلومات. قد تتطلب هذه المنهجية إجراء تحليل تفصيلي لبيئة وخواص أنظمة المعلومات، والتهديدات ونقاط الضعف المحددة في تلك الأنظمة، والتصنيف الأمني المتعلق بالملاحظات المحددة، مع الأخذ في الاعتبار أثر ذلك على أعمال الجامعة.
- يضطلع المسئول عن أنظمة المعلومات بالاشتراك مع الإدارة العامة لتقنية المعلومات حسبما ينطبق بمسئولية تخطيط وإجراء تقييم لمخاطر تلك الأنظمة المسئولين عنها.

○ تخفيف المخاطر و القبول بها

- ينبغي على جامعة الملك خالد التعامل بشكل مناسب مع مخاطر أمن المعلومات التي تم اكتشافها و تحديدها كجزء من عملية تقييم المخاطر.
- يجب مراجعة الملاحظات التي تم اكتشافها جراء عملية تقييم المخاطر من حيث أثرها على الجامعة والطبيعة التقنية للخطر. و كما يجب تحديد الأشخاص المناسبين وإجراءات/مبادرات التخفيف المتعلقة بالعمليات أو التقنية، ومن ثم يجب رفع المرئيات إلى إدارة الجامعة واعتمادها وتطبيقها بشكل فاعل.
- قد تقبل جامعة الملك خالد أي مخاطر متبقية يتعذر تخفيفها بشكل فعال. وتكون الصلاحية النهائية لمجلس الجامعة بالتشاور مع الإدارات ذات العلاقة بشأن القرارات المتعلقة بقبول المخاطر المتبقية.