مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة إدارة حوادث أمن المعلومات			
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 التأكد من التبليغ عن جميع حوادث أمن المعلومات المتعلقة بأنظمة المعلومات لدى جامعة الملك خالد ومتابعتها والتحقيق فيها وحلها بالسرعة الواجبة وبصورة فعالة.

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

○ تعريف حوادث أمن المعلومات

- تعرف الجامعة حوادث أمن المعلومات على أنها أية أحداث غير متوقعة تؤثر على أنظمة معلومات الجامعة حسبما يلي:
  - الأحداث التي لا تشكل جزءاً من العمليات الاعتيادية لخدمات تقنية المعلومات، والتي تسبب، أو قد تسبب، تعطيل أو توقف أو هبوط في جودة تلك الخدمات.
  - الأحداث التي قد تنتهك سرية أو نزاهة/سلامة أو توفر المعلومات لدى الجامعة أو أنظمة المعلومات وتشمل الحوادث الأمنية المتعلقة بتقنية المعلومات، والحوادث المتعلقة بالأمن المادي وأمن الأشخاص.
  - الأحداث المتعلقة بأوضاع استثنائية أو أوضاع تستدعي تدخل الإدارة العليا، ومن شأنها أن تسبب أذى أو ضرر بالغ في الممتلكات.
  - الثغرات الأمنية (مَواطِن الضعف في أنظمة المعلومات، والتي قد تستغل في انتهاك سرية أو سلامة أو توفر النظام) وأخطاء البرامج (وهي أي خلل أو انحراف في سير التطبيقات البرمجية). كما تُعد أية مخالفة لسياسات وإجراءات أمن المعلومات لدى الجامعة من حوادث أمن المعلومات.

○ التبليغ عن حوادث أمن المعلومات

- يتوجب على جميع موظفي جامعة الملك خالد وموظفي الأطراف الثالثة المعنيين التبليغ عن حوادث أمن المعلومات إلى مكتب الدعم الفني عن طريق الإتصال بالرقم (٠١٧٢٤١٨٠٠٠) أو عن طريق موقع أمن المعلومات (infosec.kku.edu.sa) بالسرعة اللازمة.
- على الجامعة أن تقوم بتزويد المستخدمين/ العملاء عبر الإنترنت بآلية بسيطة وسهلة الوصول إليها لاستخدامها في التبليغ عن الأنشطة المشبوهة، أو المخاوف الأمنية، أو الشكاوى، أو الحوادث. كما وأن عليها الرد على ما يقدمه العملاء بالسرعة اللازمة. وفيما يلي بعض الضوابط الرئيسية التي يجب أن تضعها الجامعة:
  - يجب أن يتضمن الموقع الإلكتروني أو الشبكة الداخلية الخاصة بـالجامعة على وسيلة تمكن العملاء من تبليغها عن الحوادث الأمنية أو الأنشطة المشبوهة.
  - يجب أن يقدم الموقع الإلكتروني أو الشبكة الداخلية الخاصة بـالجامعة رقم هاتف ليتواصل من خلاله العملاء للتبليغ عن الحوادث أو الأنشطة المشبوهة.
- على مستخدمي/ عملاء الخدمات عبر الإنترنت/ الخدمات الإلكترونية للجامعة القيام بالتبليغ عن الأنشطة المشبوهة، أو المخاوف الأمنية، أو الحوادث الأمنية باستخدام وسيلة تبليغ حوادث أمن المعلومات على الموقع الإلكتروني للجامعة.

- **اعتبارات تتعلق بعملية إدارة الحوادث**

- يجب أن يضطلع مكتب الدعم الفني و/أو فريق الحوادث الأمنية حسبما ينطبق بمسئولية تلقي وتسجيل جميع حوادث أمن المعلومات المبلغ عنها، وتقييم مدى صحة هذه الحوادث، وتصنيفها بناءً على أولويتها وأثرها على العمل، ومن ثم معالجتها، أو التبليغ عن الحوادث التي تم التحقق منها إلى الشخص المناسب لمعالجتها.
- يجب أن يتوفر لدى الجامعة خطة موثقة للإستجابة لحوادث أمن المعلومات بحيث تغطي الأنواع المختلفة من حوادث أمن المعلومات. كما يجب فحص كل خطة من خطط الاستجابة لحوادث أمن المعلومات للتأكد من فاعليتها من خلال الوسائل المناسبة كاستخدام المحاكاة ومثال ذلك، خطة الاستجابة لحوادث هجمات الشفرات الخبيثة، الاستجابة لهجمات الاصطياد الإلكتروني، وغير ذلك.
- يجب إشراك الإدارة العليا لدى الجامعة في التحري عن أية حوادث أمن معلومات تتعلق بأنظمة المعلومات الحساسة والخدمات والعمليات والموظفين.
- يجب التبليغ عن كافة حوادث أمن المعلومات الرئيسية إلى هيئة الاتصالات وتقنية المعلومات – فريق الاستجابة لطوارئ الحاسوب- المملكة العربية السعودية. (وتشمل هذه الحوادث على سبيل المثال لا الحصر عمليات الغش الداخلية، الوصول غير المصرح به لأنظمة أو معلومات الجامعة، الإزعاج غير المرغوب فيه أو الهجمات الإغراقية، الاستخدام غير المصرح به لمعالجة أو تخزين البيانات). ويتوجب على الجامعة في هذه الحالات إشراك الإدارة القانونية لديها أثناء التنسيق مع فريق الاستجابة لطوارئ الحاسوب في المملكة لتجميع الأدلة والقرائن اللازمة لإجراء التحريات المناسبة.
- يجب على الإدارة العامة لتقنية المعلومات ان تقوم بمراقبة الحوادث المسجلة وإجراء مراجعات دورية للحوادث القائمة للتأكد من حلها بالسرعة الواجبة ووفقاً لاتفاقية مستوى الخدمات المحددة حسب الحالة.
- يجب على الإدارة العامة لتقنية المعلومات ان تتولى المحافظة على والاحتفاظ بتقارير حوادث أمن المعلومات بما في ذلك تقارير حل تلك الحوادث.
- يجب على الإدارة العامة لتقنية المعلومات ان تجري تقييماً لاحقاً للحادثة المتعلقة بأمن المعلومات، وتسارع باتخاذ الإجراءات الوقائية بناءً على الدروس المستفادة لتفادي أو الحد من وقوع أحداث مشابهة.

- **تجميع الأدلة**

- عندما تستدعي الإجراءات المتخذة بحق الشخص أو المنشأة المتورطين في حوادث أمن المعلومات اتخاذ إجراءات قانونية (سواء مدنية أو جنائية)، فإنه على الإدارة العامة لتقنية المعلومات أن تتأكد من تجميع الأدلة والقرائن المطلوبة، والحفاظ عليها بشكل آمن، وتقديمها عند الحاجة، مع طلب تدخل الإدارة القانونية للجامعة عند الحاجة لذلك.

- **تحليل التوجهات والتقارير التنفيذية**

- تقوم إدارة أمن المعلومات بشكل دوري بتحليل الحوادث المسجلة لتحديد التوجهات التي تظهر بهذا الصدد. ويتم رفع تقرير بتحليل التوجهات السائدة في حوادث أمن المعلومات إلى مشرف الإدارة العامة لتقنية المعلومات.