مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة الأمن المادي والبيئي			
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 تحديد القواعد الأساسية لمنع الدخول غير المصرح به والتداخل مع مرافق وأنظمة أمن معلومات الجامعة وكذلك الحماية والحفاظ على أمن المعلومات والموظفين من التعرض إلى التهديدات المادية المختلفة، والتي من شأنها التأثير سلبياً على خدمات أنظمة المعلومات أو توقفها عن 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 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، وغيرها.

٥. **السياسات** :

- **ضوابط الأمن المادي القائمة على المخاطر**

- يجب أن تتأكد الجامعة من أن جميع منشآتها المادية تتمتع بعوامل الأمان بما يتوافق مع مخاطر أنظمة المعلومات في تلك المنشآت.
- يتم تحديد جميع منشآت الجامعة المادية ويتم تصنيفها أمنيا حسب معايير أمن المعلومات لدى الجامعة.
- يتم تخطيط الأمن المادي والبيئي للمنشآت المادية للجامعة مع الأخذ بعين الاعتبار درجة تصنيف أمن المعلومات والمعايير المتعلقة بالنوع المحدد من البنية التحتية المادية لدى الجامعة.
- تُعنى الإدارات ذات الصلة والإدارة العامة لتقنية المعلومات بمسؤولية التنسيق فيما بينها للتأكد من تصميم وتنفيذ ومراقبة الضوابط المادية والبيئية في الجامعة و القائمة على المخاطر.

- **المنطقة الآمنة**

- يجب أن تقوم الجامعة بتطوير مخطط الأمن المادي لمرافقها كما يجب توزيع المخطط المادي الخاص بالجامعة على مناطق بحيث يكون لكل منطقة مستوى أعلى من القيود التي تحكم متطلبات التصريح بالدخول. ويمكن تصنيف المناطق المحيطية كالتالي:
  - المنطقة العامة ومنطقة الاستقبال: (قيود محدودة وتخضع هذه المنطقة للمراقبة العامة).
  - منطقة المكاتب (دخول محدود، يتم تسجيل الدخول و مرافقة الزوار الذين يدخلون إلى هذه المنطقة. كما تخضع المنطقة للمراقبة العامة).
  - منطقة الدخول الآمنة (دخول محدود، يتم تسجيل الدخول و مرافقة دخول الزوار. تخضع المنطقة للإشراف).
  - منطقة الدخول المقيد – التي تقتصر على دخول الأشخاص المصرح لهم فقط. (الدخول يخضع لقيود عالية. يتم تسجيل الدخول. يجب حصول الموظفين والزوار الذين يدخلون إلى هذه المنطقة على تصريح محدد بالدخول. تخضع المنطقة للمراقبة).
- يجب التأكد مما يلي:
  - أن مرافق معالجة المعلومات لا تقع في منطقة غير مستقرة من ناحية البيئة.
  - عدم وقوع مرافق معالجة المعلومات على مقربة من أي مرافق مجاورة خطرة (مثل المختبرات الكيمائية وخلافه).
  - يتم تخزين المعدات المزمع استخدامها في الحالات الطارئة ووسائط النسخ الإحتياطية على مسافة آمنة بعيداً عن الموقع الرئيسي لتفادي التعرض لنفس الكارثة التي قد تلم بالموقع الرئيسي.

- **التحكم في الوصول المادي**

- يسمح لموظفي وموردي ومقاولي الجامعة بالدخول إلى المرافق المادية لدى الجامعة بما في ذلك مرافق معالجة المعلومات، و ذلك فقط بناءً على التعريف بأنفسهم والتحقق من هويتهم وفقاً لإجراءات منح صلاحية الدخول المادي.
- يتم اعتماد الوصول إلى المناطق الآمنة والمقيدة من قبل المسؤول عن النشاط/تقنية المعلومات. ويكون الدخول إلى المناطق التي تتمتع بتصنيف أمني مرتفع مثل غرف الخوادم محصوراً على الأشخاص الذين لديهم مسؤولية مباشرة عن تشغيل وصيانة غرفة الخوادم.
- يجب أن يُطلب من موظفي وموردي ومقاولي الجامعة والزوار الآخرين أن يضعوا شارة تعريفية فريدة أثناء تواجدهم في مرافق الجامعة بشكل دائم.
- ينبغي أن يوقع كل زائر على سجل الزوار الذي يتم الاحتفاظ به لزوار الجامعة. يجب أن يتم توثيق اسم الزائر وشركته والغرض من الزيارة ووقت الدخول ووقت المغادرة والتاريخ في ذلك السجل.
- يمنع منعاً باتاً مشاركة الموظفين بعضهم باستخدام بطاقة الدخول إلى لمنشآت العمل.
- يجب عدم وضع أدلة الهاتف والوثائق السرية المستخدمة في تحديد مواقع مرافق المعالجة الحساسة في مكان يسهل الوصول إليها من قبل الموظفين الداخليين والخارجيين الذي ليست لديهم الصلاحيات الأمنية المطلوبة.
- يجب مرافقة جميع الزوار أثناء تجوالهم في المناطق الآمنة من قبل موظفي الجامعة.

- **التفتيش الأمني للمواد الداخلة إلى والخارجة من الجامعة**

- يتعين القيام بتفتيش المواد الداخلة إلى والخارجة من الجامعة قبل نقلها من مناطق الدخول العامة إلى نقطة استخدامها. ويجب أن يتم التصريح رسمياً بجميع طلبات النقل من قبل المسؤول عن المعلومات وتسجيلها من قبل موظفي الأمن المادي.
- ينبغي أن تتم صيانة وإصلاح معدات الجامعة من قبل موظفي صيانة مصرح لهم ومؤهلين للقيام بذلك.
- ينبغي أن تتأكد إدارتا الأمن المادي والشئون الإدارية من أنه يتم فحص أجهزة ومعدات البنية التحتية للأمن المادي والبيئي بشكل منتظم.
- يتعين على الجامعة القيام بجدولة وتنفيذ وتوثيق ومراجعة سجلات الصيانة الوقائية والمنتظمة (بما في ذلك الإصلاحات) لعناصر نظام المعلومات.
- يتعين على الجامعة التفويض بالمراقبة والتحكم بأي أنشطة صيانة وأنشطة تشخيصية يتم تنفيذها محلياً أو عن بعد. كما أن عليها مراقبة كافة عمليات الصيانة المحلية/ و التي تتم عن بعد والأنشطة التشخيصية، وعلى موظفي الجامعة المعنيين مراجعة سجلات الصيانة للأنشطة البعيدة.

- **الحماية ضد الحرائق**

- يجب أن تضطلع الإدارات الإدارية بالمسؤولية عن الاستجابة لحوادث الحريق الطارئة وإجراء تمارين للتعامل مع الحريق.
- ينبغي إجراء تمارين التعامل مع الحريق بشكل ربع سنوي (ويفضل أن تكون بصفة شهرية). كما ينبغي مراقبة تلك التمارين، وتزويد جميع المشاركين بإفادات تتعلق بمساهمتهم وأدائهم.
- تقوم إدارتا الأمن المادي والشئون الإدارية بتحديد المواقع الحرجة التي سيتم تجهيزها بطفايات حريق يدوية. وعليه فإنه يتعين وضع بطاقات واضحة على تلك المناطق والتبليغ عن موقعها بشكل دوري لجميع الموظفين أثناء التدريب التوعوي واستخدام النشرات الموجزة.
- كجزء من تدابير الأمن المادي المطلوبة أثناء الإخلاء بسبب الحريق، يتم تجهيز أبواب مخارج الحريق لتفتح من الداخل فقط. كما ينبغي إعداد إنذارات الحريق لتنطلق فوراً عند فتح مخرج الطوارئ.

- **مراقبة الأمن المادي والبيئي**

- يجب أن تتأكد الجامعة من مراقبة ضوابط الأمن المادي والبيئي لديها بما يتوافق مع مستويات تصنيف المخاطر لبيئة الأمن المادي ذات العلاقة.
- يجب أن تقوم الإدارت الإدارية بتطوير خطة مراقبة الأمن المادي والبيئي المبنية على المخاطر، والتي تحدد ضوابط الأمن المادي والبيئي الواجب مراقبتها والمسؤوليات التي سيتم تحديدها بهذا الصدد.