سياسة الالتزام

	عمادة التعاملات الإلكترونية والاتصالات **إدارة البوابة الالكترونية**	رقم الوثيقة	رقم الإصدار	اعتماد ادارة التطوير والجودة	اعتماد العميد
			1		
	سياسات وإجراءات إدارة المخاطر وأمن المعلومات				

1- هدف الوثيقة:

تهدف هذه السياسة إلى توفير متطلبات الالتزام لموظفي جامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات)لتجنب أي انتهاك لسياسات أمن المعلومات، والقوانين، والأنظمة، والالتزامات التعاقدية، أو أية متطلبات أمنية.
ويتعيّن تحديد كافة الضوابط الضرورية لضمان التزام كافة الموظفين، والمقاولين، والاستشاريين بسياسات أمن المعلومات الموضوعة من قبل جامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات)، وبالقوانين، والتشريعات أو الالتزامات التعاقدية، وبأية متطلبات أمنيّة.

2- مجال التطبيق:

تنطبق هذه السياسة على جامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات)، وعلى كافة الأطراف الأخرى بما في ذلك الشركاء، أو الجهات التابعة لها، وعلى نظم معالجة البيانات ونظم ضبط العمليات التي تحتوي على، أو تستخدم معلومات و/أو تسهيلات تعود ملكيتها لجامعة الملك سعود(عمادة التعاملات الإلكترونية والاتصالات.)
تسري هذه السياسة على كافة الموظفين /المستخدمين الذين يعملون بصورة مباشرة أو غيرة مباشرة لدى جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)أو الجهات التابعة لها أو أية جهة تقوم بتنفيذ عمل نيابة عنها يتضمن استخدام الأصول

3- تطبيق الالتزام بالسياسة :

يعتبر التقيُّد بهذه الوثيقة إلزامي، وعلى مدراء عمادة التعاملات الإلكترونية والاتصالات بجامعة الملك سعود، متابعة مدى الالتزام بها ضمن إداراتهم .ويكون الالتزام ببيان السياسة العامة خاضعا للمراجعة الدورية من قبل إدارة المخاطر وأمن المعلومات، ويسفر أي انتهاك لهذه السياسة عن قيام اللجنة التوجيهية لنظام إدارة أمن المعلومات باتخاذ إجراءات تأديبية.
يتلاءم مستوى الإجراءات التأديبية المطبقة مع مستوى المخالفة الذي تتوصل إليه التحقيقات .وتتضمن هذه الإجراءات التأديبية، عقوبات قد تنطوي على إنهاء خدمة الموظف، أو أية عقوبات أخرى وفقا لتقديرات إدارة عمادة التعاملات الإلكترونية والاتصالات وإدارة الموارد البشرية.

4- معايير الاستثناء من السياسة:

تسلط هذا السياسة الضوء على متطلبات أمن المعلومات .وفيما لو دعت الحاجة للحصول على استثناء من هذه السياسة، يمكن تقديم طلب رسمي إلى اللجنة التوجيهية لنظام إدارة أمن المعلومات، مع توضيح مسوغات الاستثناء، والمزايا التي قد تنجم عن منحه.
يبلغ الحد الأقصى للاستثناء من السياسة مدة عام واحد، وفيما لو اقتضى الأمر، يمكن أن إعادة النظر بالاستثناء واعتماده مرة أخرى لثلاث فترات متعاقبة كحد أقصى .على أن لا يتجاوز الاستثناء من السياسة مدة 3 فترات متعاقبة.

5- السياسات ذات العلاقة :

- كافة سياسات أمن المعلومات.

6- مالك الوثيقة :

- مدير نظام إدارة أمن المعلومات.

7- إدارة السياسة:

تقتضي التطورات التقنيّة والتغييرات على متطلبات العمل، إجراء مراجعات دورية للسياسات .ومن هذا المنطلق، فإن هذه السياسة قد تخضع للتعديل بهدف تطبيق التغييرات التي تمت، أو وضع متطلبات جديدة أو محسنة.
يجب إبلاغ مسئول أمن المعلومات فورا، بأي قصور يتم اكتشافه في هذه السياسة .علما بأن إجراء التغييرات على هذه الوثيقة يتطلب موافقة اللجنة التوجيهية لنظام إدارة المخاطر وأمن المعلومات. ينبغي الاحتفاظ بسجل حديث للتغييرات، وان يتم تحديثه فور حدوث أي تغيير.

8- بيان السياسة:

8.1. الالتزام بالمتطلبات القانونية

8.1.1. تحديد التشريعات السارية

- تقوم جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) بتحديد وتحليل المتطلبات التشريعية والتنظيمية والقانونية والتعاقدية السارية، واتخاذ التدابير الملائمة للالتزام بها، بحيث يتم معالجة المجالات التالية:
  - ❖ المعايير والإرشادات الخاصة بتقنية المعلومات.
  - ❖ المتطلبات الحكومية و/أو الخارجية ذات الصلة (القوانين، والتشريعات، والإرشادات، والنظم، والمعايير) والتي تتعلق بمراجعة العلاقات الخارجية والمتطلبات الداخلية.
  - ❖ قوانين العمل وخصوصاً ما يتطرق منها لمتطلبات السلامة والصحة في مجال تقنية المعلومات.
  - ❖ حقوق الملكية الفكرية / قوانين حقوق تأليف ونشر البرامج.
  - ❖ متطلبات أمن نظم المعلومات وخصوصاً تلك المتعلقة باستخدام البيانات المشفرة وبث البيانات.
  - ❖ تقارير التدقيق التي يعدها المدققون الخارجيون، ومزودي خدمات الطرف الثالث والهيئات الحكومية.

- يتعين على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) التأكد من التزام تصميم، وتشغيل، وإدارة، واستخدام الأصول والتسهيلات ذات الصلة بكافة المتطلبات القانونية والتنظيمية أو المتطلبات التعاقدية ذات الصلة بأمن المعلومات.

8.1.2. حقوق المُلكية الفكرية

- تُقر جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) وتحترم حقوق الملكية الفكرية (والتي تتضمن حقوق الطبع والتأليف والنشر الخاصة بالبرامج والوثائق، وحقوق التصميم، والعلامات التجارية، وبراءات الاختراعات، ورخص الرموز البرمجية) المرتبطة بنظم المعلومات لديها.

- يتعيّن كافة وحدات العمل تطبيق إجراءات ملائمة لضمان الالتزام بالمتطلبات التشريعية والتنظيمية والتعاقدية المتعلقة باستخدام المواد التي قد تكون خاضعة لحقوق الملكية الفكرية، وحول استخدام منتجات البرامج التي هي محل ملكية

حصرية.

- يتعيّن على كافة وحدات العمل تطبيق إجراءات ملائمة لضمان الالتزام بالتحديدات القانونية على استخدام المواد التي قد تكون خاضعة لحقوق الملكية الفكرية، وحول استخدام منتجات البرامج التي هي محل ملكية حصرية، مثل حقوق التأليف والنشر، حقوق التصميم والعلامات التجارية.

يتعين على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) الالتزام بالمتطلبات التالية:

- أن يكون شراء وإصدار كافة البرامج المستخدمة في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) وفقاً لاتفاقيات الترخيص.

- لا يجوز لأي شخص أو كيان في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) الاشتراك في عمليات نسخ غير مصرح بها للبرامج.

- يتعين على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) الاحتفاظ بما يدل على توفر الرخص أو ملكية كتيبات التشغيل والاستخدام.

- متطلبات التراخيص والتي تُقيد استخدام المنتجات، والبرامج، والتصاميم، والمواد الأخرى التي تحتاج إليها جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

- على كافة الموظفين الذين يستخدمون الأصول المعلوماتية التابعة لجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) التقيّد بقوانين وقيود التأليف والنشر التي تحددها الجهة المصنعة للبرمجيات.

- تمتنع جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) عن نسخ المواد التي تخص طرف ثالث، أو تحويلها إلى صيغة أخرى، أو استخلاصها من التسجيلات التجارية (الأفلام، والتسجيلات الصوتية) ما لم يكن ذلك مصرحاً به بموجب سياسة حقوق التأليف والنشر.

- على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) تبني سياسة موثقة تحدد الأسلوب الملائم للتخلص من البرمجيات أو تحويلها إلى الغير.

- تعنون كافة الوثائق الخاصة بجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) والخاضعة لحقوق الملكية الفكرية بالتصنيف الأمني "سري".

8.1.3. حماية سجلات الجامعة

- يجب وضع مجموعة موثقة من الإجراءات لتحديد مبادئ تصنيف سجلات المعلومات، بالإضافة إلى ضوابط الحماية المناسبة لهذه السجلات لحمايتها من الضياع أو التلف أو التزوير.

- ينبغي تصنيف السجلات في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) حسب نوع السجلات (سجلات محاسبية، وسجلات قواعد بيانات، وسجلات التعديلات، وإجراءات التشغيل)، بحيث يتضمن منها تفاصيل مدة الاحتفاظ بالسجلات ونوع وسائط التخزين (ورقية، أو مغنطيسية، أو ضوئية وغيرها).

- يجب العمل على حماية سجلات جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) من الضياع، والتلف، والتزوير بناءً على أهمية السجلات، وينبغي تخزينها بطريقة تتلاءم مع وسائط التخزين التي تحوي هذه السجلات.

- يراعى في نظام تخزين السجلات وتداولها أن يتم تحديد السجلات وفترات الاحتفاظ بها بوضوح تام، وأن يسمح النظام بإتلاف السجلات بصورة ملائمة بعد مرور المدة المحددة إذا لم تعد جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) بحاجة إليها.

8.1.4. حماية البيانات وخصوصية المعلومات الشخصية

- يتعين تطوير سياسة لحماية البيانات والخصوصية وتطبيقها لتحديد المتطلبات في القوانين، والنظم، والمتطلبات التعاقدية ذات الصلة بجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

- يُحدد هيكل للإدارة والضبط لضمان الالتزام بهذه السياسة، والقوانين، والنظم الأخرى ذات الصلة بحماية البيانات وفقا لمتطلبات جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

- يُحظر على أي موظف من موظفي جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) اطلاع أية جهة أخرى، أو شركة، أو وحدة من وحدات العمل أو أية جهة حكومية ترتبط بالجامعة، على أية معلومات سرية أو تعود ملكيتها حصرياً لجامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) أو تخص المواطنين، دون الحصول على تصريح بذلك.

- يُحظر نقل أو إطلاع الغير على المعلومات الشخصية في الحالات التي يمكن الاستعاضة فيها باستخدام بيانات إحصائية.

8.1.5. الحيلولة دون إساءة استخدام تسهيلات معالجة المعلومات

- ينبغي تحديد الاستخدام المناسب لتسهيلات معالجة المعلومات من خلال إجراء رسمي. وتتولى الإدارة الموافقة على استخدام تسهيلات معالجة المعلومات.

- يتعين على كافة الموظفين أن يكونوا على دراية بنطاق الدخول المسموح، وبعملية المراقبة التي تجري بهدف كشف الاستخدام غير المصرح به. وينبغي ثني المستخدمين عن استخدام تسهيلات معالجة المعلومات لأغراض غير مصرح بها.

- يتعين عند تسجيل الدخول، عرض تحذير/ رسالة التزام قانوني على شاشة الحاسوب تشير إلى أن النظام الذي يتم الدخول إليه هو نظام خاص، وبأنه لا يسمح بالدخول غير المصرح به.

- على كافة المستخدمين الإقرار بأن إساءة استخدام تسهيلات معالجة المعلومات من قبلهم قد يؤدي إلى انتهاك السرية على صعيد التزامات جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، وبأنهم خاضعون لسياسات جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).

8.2. الالتزام بالسياسات والمعايير الأمنيّة والالتزام الفني

8.2.1. الالتزام بسياسات ومعايير أمن المعلومات

- على جميع المستخدمين (الموظفين، والمقاولين، والاستشاريين) استيعاب مسئولياتهم والإقرار بها من حيث الالتزام بالسياسات والإجراءات الأمنيّة في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات).
- يتعين على رؤساء الإدارات/ المدراء العمل بانتظام على مراجعة التزام معالجة المعلومات داخل ضمن نطاق مسئولياتهم بالسياسات الأمنيّة المناسبة، والمعايير، وأية متطلبات أمنية أخرى.
- تدون نتائج المراجعة والإجراءات التصحيحية التي يقوم بها المدراء ويتم الاحتفاظ بهذه السجلات.

8.2.2. التحقق من الالتزام الفني

- يتعين إخضاع كافة المجالات والأصول المعلوماتية في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) لعمليات تدقيق منتظمة لضمان الالتزام بسياسات ومعايير أمن المعلومات.
- يجب القيام بعملية تدقيق على الالتزام الفني كل 6 شهور لتقييم الالتزام بسياسات حماية المعلومات، وتحديد نقاط الضعف الأمنيّة في النظام.
- يجب إجراء اختبار اختراق وتقييم نقاط الضعف الأمنيّة كلما أمكن ذلك لتقييم فعالية الضوابط المطبقة.
- يجب أن لا يتم إجراء تدقيق الالتزام الفني إلا من قبل شخص مؤهل ومفوض، أو أن يتم التدقيق تحت إشراف مثل هذا الشخص

8.3. الاعتبارات الخاصة بتدقيق نظم المعلومات

8.3.1. ضوابط تدقيق نظم المعلومات

- ينبغي أن يتم تخطيط متطلبات التدقيق بما في ذلك التحقق من النظم العاملة بعناية، وتنفيذها على فترات دورية (على الأقل سنوياً) بعلم مالكي الأصول المعلوماتية لتقليص مخاطر تعطل إجراءات العمل.

- حينما تتطلب عملية التدقيق الدخول إلى النظام أو البيانات أو تتضمن استخدام أدوات برمجية وبرامج خدمية، فإنه ينبغي إجراء مثل هذا التدقيق بمعرفة وتعاون وموافقة مالكي الأصول المعلوماتية، والعمل على اتخاذ التدابير المناسبة لحماية نظام المعلومات والبيانات من التلف أو التعطّل نتيجة لأعمال التدقيق أو أدواته.

- القيام دورياً (على الأقل مرة كل سنة) بإجراء تدقيق أو أكثر لنظم المعلومات في جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) من قبل مؤسسة تدقيق مؤهلة ومستقلة.

8.3.2. حماية أدوات تدقيق نظام أمن المعلومات

- ينبغي الفصل فيما بين أدوات التدقيق، كالبرامج أو ملفات البيانات، ونظم التطوير أو النظم العاملة الحية، وعدم حفظها في مكتبة الأشرطة أو في المناطق المخصصة للمستخدمين ما لم يتم تزويدها بمستويات إضافية من الحماية.

- يخضع استخدام أدوات تدقيق النظم للتفويض وللقيود ولضوابط تكون وفقاً لإرشادات محددة لهذا الغرض. وتتضمن أدوات تدقيق النظام برامج المراقبة، البرامج والتسهيلات المستخدمة في استخلاص البيانات والتحكم بها، والتي قد تشكل أو لا تشكل جزء محورياً من مجموعة برامج نظم المعلومات.

- يتعين على جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات) اتخاذ التدابير اللازمة بهدف:
  - ❖ الحيلولة دون إمكانية إساءة استخدام أدوات التدقيق (على سبيل المثال القيام باستخلاص معلومات سرية دون الحصول على التفويض المناسب).
  - ❖ التأكد من إدامة دقة نظم المعلومات والبيانات المرتبطة بها.
  - ❖ تجنب الانقطاع المحتمل لنظم المعلومات نتيجة لاستخدام مثل هذه الأدوات.

- فيما لو كانت هنالك أية أطراف ثالثة مشاركة في التدقيق، فقد يكون هناك فرصة لإساءة استخدام أدوات التدقيق من قبل هذه الأطراف، والدخول إلى المعلومات من قبلها. حيث ينبغي تقييم هذه المخاطر والنظر في استخدام ضوابط للتحكم بالدخول المادي لمواجهة هذه المخاطر، وأية آثار تترتب عليها، كالقيام فوراً بتغيير كلمات المرور التي يتم كشفها للمدققين.