



# سياسة الاستخدام المقبول

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

## 1- هدف الوثيقة:

حاجة عناوين هذي السياسة لإدارة عمادة التعاملات الإلكترونية والاتصالات بفرض مسؤوليات معينة على مستخدمي الموارد المعلومات لضمان شرعيتها والسرية والتوفر. الامتثال لهذه السياسة اساسيا لتهيئة بيئة تقضي الى ممارسات الامن السليمة.

## 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 غير مباشرة لدى جامعة الملك سعود (عمادة التعاملات الإلكترونية والاتصالات)، أو الجهات التابعة لها أو أية جهة تقوم بتنفيذ عمل نيابة عنها يتضمن استخدام الأصول المعلوماتية التابعة لها.

## 3- تطبيق الالتزام بالسياسة:


يعتبر التقيد بهذه الوثيقة إلزامي، وعلى عمادة التعاملات الإلكترونية والاتصالات بجامعة الملك سعود، متابعة مدى الالتزام بها ضمن إدارتهم. 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 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 ألا يتجاوز الاستثناء من السياسة مدة 3 فترات متعاقبة.

## 5- السياسات ذات العلاقة :

- سياسة أمن المعلومات.
- سياسة الالتزام.
- سياسة إدارة الأصول.
- سياسة إدارة حوادث أمن المعلومات.

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

## 6- مالك الوثيقة :

●مسئول أمن المعلومات.

## 7- إدارة السياسة:

تقتضي التطورات التكنولوجية 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 فوراً، بأي قصور يتم اكتشافه في هذه السياسة. علماً بأن إجراء التغييرات على هذه الوثيقة يتطلب موافقة اللجنة التوجيهية لنظام إدارة المخاطر وأمن المعلومات. ينبغي الاحتفاظ بسجل حديث للتغييرات، وأن يتم تحديثه فور حدوث أي تغيير.

## 8- بيان السياسة:

### 8.1. استخدام نظم المعلومات


- 8.1.1. المستخدمين المصرح لهم لديهم موارد المعلومات في عمادة التعاملات الإلكترونية والاتصالات للأغراض الرسمية التي اذن بها. استخدام نظم المعلومات والموارد في عمادة التعاملات الإلكترونية والاتصالات لاستخدام شخصي أو بنيابة عن طرف ثالث) أي أفراد الأسرة، سياسية أو دينية أو خيرية أو خيرية الخ) ممنوع منعاً باتاً.
- 8.1.2. ممنوع منعاً باتاً مشاركة أو توزيع المعلومات الخاصة بعمادة التعاملات الإلكترونية والاتصالات إلا إذا أخذت الموافقة على ذلك.

### 8.2. ادخال النسخ غير المرخصة من البرامج أو الأجهزة

- 8.2.1. يحذر من النسخ غير المرخصة من برامج واهزته الى موارد المعلومات في عمادة التعاملات الإلكترونية والاتصالات ونسخ من هذه المواد.
- 8.2.2. يجب منع تخزين ومعالجة النسخ غير المرخصة من قبل الموظفين في عمادة التعاملات الإلكترونية والاتصالات.

### 8.3. ادخال التطبيقات المجانية

- 8.3.1. ادخال البرامج المجانية من أي مكان تم تحميلها من الانترنت أو بأي وسيلة لنظم المعلومات عمادة التعاملات الإلكترونية والاتصالات يجب ان تخضع لعملية تقييم رسمي والحصول على موافقة مسبقة لتركيبه.
- 8.3.2. يجب تقييم البرامج والتطبيقات المجانية واختبارها من قبل مركز معلومات قبل تثبيتها على موارد المعلومات في عمادة التعاملات الإلكترونية والاتصالات.

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

#### 8.4 ادخال المواد غير الاخلاقية والالعاب

- 8.4.1 يجب منع ادخال اى مواد غير اخلاقية في بيئة نظم المعلومات عمادة التعاملات الإلكترونية والاتصالات وفي اضافته الى ذلك اى تخزين او نقل من مواد غير اخلاقية والالعاب على نظم المعلومات في عمادة التعاملات الإلكترونية والاتصالات من قبل الموظفين او المتعاقدين تمنع منعاً باتاً.
- 8.4.2 لا يسمح للألعاب ويجب تكون بعيدا عن كل الانظمة.

#### 8.5 ادخال البرامج المدمرة

- 8.5.1 يمنع ادخال البرامج المدمرة (مثل الفايروس والتروجان و Worms و Rootkit و back door) من اجل احداث اضرار متعمده تتداخل مع الاخرين والوصول غير المصرح به او تعوق انتاج العمل في أنظمة المعلومات عمادة التعاملات الإلكترونية والاتصالات.
- 8.5.2 يمنع استخدام ادوات تحليل / sniffing الشبكة دون اذن مسبق من مسؤول أمن المعلومات.

#### 8.6 استخدام الانترنت

- 8.6.1 استخدام خدمات الانترنت في الانشطة الرسمية ،ولايمكن استخدام شبكة عمادة التعاملات الإلكترونية والاتصالات المحدوده لاغراض اخرى ليس لها علاقه بالعمل.
- 8.6.2 طلب الموظف للانترنت يجب أن يكون موضح فيه أسباب استخدامه للانترنت ، ويجب ارفاق موافقة من رئيس قسم المعلومات وموظف امن المعلومات.
- 8.6.3 أي معلومة حساسة ترسل عبر الانترنت (مثلاً البريد الإلكتروني في الإنترنت) يجب تشفيرها.
- 8.6.4 يجب على الموظفين عدم الافصاح عن أي معلومة عبر الاتصال بالانترنت وعلاوة على ذلك لا يسمح للموظفين وضع أي معلومات على جهاز حاسب آلي له اتصال مباشر بالانترنت.

#### 8.7 استخدام موارد معلومات للتخزين والمعالجة وتنزيل أو نقل البيانات

- 8.7.1 يمنع منعاً باتاً استخدام أنظمة المعلومات في عمادة التعاملات الإلكترونية والاتصالات لتخزين ومعالجة والتنزيلات، أو نقل البيانات يمكن تفسر على أنها(سياسية او دينية أو عنصرية أو عرقية وغيرها) أو في انتهاك الآداب العامة والعادات والتقاليد في المملكة.
- 8.7.2 تحميل، وإعادة توزيع وطباعة مواد حقوق الطبع والنشر، وثائق، أو غيرها من مواد حقوق الطبع والنشر لأنظمة المعلومات الخاصة عمادة التعاملات الإلكترونية والاتصالات ممنوعه منعاً باتاً.
- 8.7.3 استقبال وطباعة وإرسال أو نشر البيانات الشخصية وأسرار عمادة التعاملات الإلكترونية والاتصالات او غيرها من المعلومات السرية واتفاقات الملكية ممنوعه منعاً باتاً.

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

## 8.8 إستخدامات البريد الإلكتروني

- 8.8.1 أي عملية ارسال خارج شبكة عمادة التعاملات الإلكترونية والاتصالات يجب أن تتم عبر رسمي نظام البريد. و يمنع استخدام الحسابات الشخصية (مثل الهوتميل و الجي ميل والياهو) لمراسلات عمادة التعاملات الإلكترونية والاتصالات.
- 8.8.2 يمنع استخدام الاتصالات المتضمنة لمعلومات حساسة عبر البريد الإلكتروني الخارجي الموجود في الإنترنت إلا إذا كان هناك إذن تم الحصول عليه من مسؤول أمن المعلومات مدير الإدارات ويجب أن تكون مشفرة في كلا الحالتين.
- 8.8.3 للحفاظ على امن نظام البريد الالكتروني في عمادة التعاملات الإلكترونية والاتصالات ،من المهم التحكم في الوصول للنظام، والموظفين يجب عليهم عدم إعطاء معلومات الدخول وكلمة المرور الشخصيتين للأشخاص الغير مصرح لهم.
- 8.8.4 اي استخدام للبريد الالكتروني من الشبكة من السهولة تتبعها إلى عمادة التعاملات الإلكترونية والاتصالات. على الأفراد عمل هذه الانشطة مع الأخذ بالاعتبار بسمعة عمادة التعاملات الإلكترونية والاتصالات. يجب على الموظفين الحرص نفسه عند صياغة البريد الالكتروني لأنها تعتبر في نفس مستوى أهمية أي خطاب يحمل اسم عمادة التعاملات الإلكترونية والاتصالات.
- 8.8.5 البريد الالكتروني الغير مرتبط بالعمل المحتوي على ملفات مرفقة مثل الصور وملفات الوسائط التي تستهلك موارد النظام، لا يمكن ارسالها عبر انظمة البريد الالكتروني الخاصة عمادة التعاملات الإلكترونية والاتصالات.
- 8.8.6 يجب على المستخدمين عدم ارسال الرسائل غير المرغوب فيها بالبريد "المعروف باسم سبام"
- 8.8.7 يجب على المستخدمين عدم نشر او توزيع القوائم البريدية الداخلية لغير الموظفين.
- 8.8.8 يجب عدم فتح اي مرفقات غير موثوق فيها. جميع المرفقات البريد الالكتروني، بغض النظر عن مصدرها او المحتوى، يجب تفحص المرفقات قبل ان يتم فتحها او تخزينها على أي نظام في عمادة التعاملات الإلكترونية والاتصالات. ويجب على الموظفين تفحص الفيروسات في جميع المواد التي يتم نقلها على اي نظام الى مستخدمين عبر البريد الالكتروني قبل ارسالها.
- 8.8.9 يجب أن لا تستخدم مرافق عمادة التعاملات الإلكترونية والاتصالات من قبل الموظفين والمتعاقدين لمناقشة الأمور الغير متعلقة بالعمل في لوحة المناقشات وجلسات الدردشة وغيرها على شبكة الانترنت.
- 8.8.10 على الموظفين التأكد من الرسائل التي تنشر على القوائم البريدية، المجموعات الاخبارية العامة والمواقع ذات الصلة لا تكشف عن أي تفاصيل سير عمادة التعاملات الإلكترونية والاتصالات بأقسامها ومواقع الضعف المحتملة في البنية التحتية لأمن المعلومات، مثل عناوين الأجهزة وأسماء الخوادم وأنواع الخوادم أو أرقام إصدار البرامج.

## 8.9 المسؤوليات المطلوبة

- 8.9.1 أي مستخدم مسؤول عن إبلاغ ضابط امن المعلومات على الفور عن أي اشتباه في انتهاك الامن فيما يتعلق:
- الدخول غير مصرح به للوصول الى شبكة أو الاتصالات أو نظم الحاسب.
  - وجود واضح لفيروس في جهاز الكمبيوتر.
  - وجود أي مصدر للمعلومات المحظورة بموجب السياسة.
  - العبث في اي ملف قام المستخدم بإنشاء ضوابط للوصول عليه.
  - انتهاك لهذه السياسة او اي سياسة متعلقة بأمن المعلومات أو إجراء معين تمت من قبل مستخدم اخر أو موظف أو مقال او مزود خدمه.

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

8.9.2. كل مستخدم تقع عليه مسؤولية منع الدخول غير المصرح به ، بما في ذلك النظر في مصادر المعلومات التي في حوزته مثل (الكمبيوتر المحمول او المكتبي و المطبوعات او الوسائط مثل القرص المرن و الأشرطة).

8.9.3. اي موظف مسؤول عن توفير الدخول الأمن ضد الاقارب والاصدقاء والجيران والعملاء والزبائن والبائعين وغيرهم. في بعض الحالات التي يكون فيها هؤلاء الناس حصلوا على صلاحية الدخول يقوم المستخدم بالإشراف والمراقبة على الأفعال لفترة زمنية محددة.

### 8.10. الحق في استخدام نظام المراقبة

8.10.1. الانظمة وجميع المعلومات الموجودة في الأنظمة (تشمل ملفات الكمبيوتر والبريد الالكتروني ورسائل البريد الصوتي والوصول الى الانترنت وغيرها) هي ممتلكات خاصة عمادة التعاملات الإلكترونية والاتصالات. في أي وقت وبدون سابق إنذار يمكن مراقبة المعلومات و تفتيشها ومراجعتها واعتراضها من قبل عمادة التعاملات الإلكترونية والاتصالات لأي غرض من الاغراض المشروعه بما في ذلك :

- مراقبة الاداء.
- التأكد من الامتثال لسياسات عمادة التعاملات الإلكترونية والاتصالات.
- منع سوء استخدام الانظمة.
- اختبار مشاكل البرامج والاجهزة.
- الامتثال للطلبات القانونية والتنظيمية للحصول على معلومات.
- التحقيق والتحري في الكشف عن أعمال المنظمة والملكية السرية للمعلومات أو السلوك التي قد يكون غير قانونيا و مؤثر سلباً على عمادة التعاملات الإلكترونية والاتصالات.
- الوصول الى رسائل محذوفة من الانظمة.