ابتكار الأعمال الملهمة


# سياسة الاستخدام المقبول

**الإصدارة ١ .١**

**رقم السياسة:**

## ١. جدول المحتويات

## ٢. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة تقنية المعلومات والاتصالات في جامعة الإمام عبد الرحمن بن فيصل، وهي تعتبر سرية ولا يسمح بالاضطلاع عليها إلا للقراء للذين يحق لهم ذلك. كما لا يسمح بتوزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة تقنية المعلومات والاتصالات.

# ٣. الرقابة على الوثيقة

## ٣. معلومات عن الوثيقة

| العنوان | التصنيف | الإصدارة | الحالة |
|---|---|---|---|
| سياسة الاستخدام المقبول | سرية | ١. ٠ | معتمدة |

## ٣. ٢ تاريخ الإعداد والتّحديث

| الإصدارة | المؤلفون | تاريخ الاصدار | التغييرات |
|---|---|---|---|
| ١. ٠ | علاء عليوه | ١٨نوفمبر ٢٠١٤ | إعداد |
| ٢. ٠ | نبيل البحبوح | 30 نوفمبر ٢٠١٤ | تحديث |
| ٣. ٠ | أسامة العمري | 23 ديسمبر ٢٠١٤ | QA |
| ١. ٠ | نبيل البحبوح | 31 ديسمبر ٢٠١٤ | تحديث |
| ١. ١ | منيب أحمد - تقنية المعلومات والاتصالات بجامعة الامام عبد الرحمن بن فيصل | ٢١ أبريل ٢٠١٧ | تحديث |

## ٣. ٣ المراجعة والتحقّق والاعتماد

| الاسم | الصفة | التاريخ |
|---|---|---|
| لمياء عبد الله الجعفري | مديرة قسم الجودة | |
| د٠ خالد العيسى | عميد عمدة تقنية المعلومات | |
| | | |

٣. ٤ قائمة التوزيع

| رقم النسخة | المستلم | الموقع |
|---|---|---|
| | | |
| | | |

## ٤. نظرة عامة على السياسة

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها ومصطلحاتها وتعاريفها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها والامتثال لها، والتنازل، والأدوار والمسؤوليات، والمستندات ذات الصلة والملكيّة.

### ٤. ١ الغرض

الغرض الرئيسي من سياسة الاستخدام المقبول هو:
تحديد مجموعة القواعد التي تحكم الطرق التي يمكن استخدام الحاسب الآلي والشبكة والبريد الإلكتروني وخدمات الإنترنت من قبل المستخدمين. بالإضافة إلى التقليل إلى الحد الأدنى من المخاطر المحتملة مثل هجمات الفيروسات، والتنازل عن أنظمة وخدمات الشبكة، والمشاكل القانونية المترتبة على ذلك.

### ٤. ٢ النطاق

تنطبق بيانات السياسة المدرجة في هذه الوثيقة على جميع منسوبي جامعة الإمام عبد الرحمن بن فيصل في جميع مستوياتهم حيث تشمل:

- جميع الموظفين الذين يعملون في جامعة الإمام عبد الرحمن بن فيصل بدوام كامل أو بدوام جزئي أو بصفة مؤقتة سواء كان وظفتهم الجامعة أو يعملون لصالحها أو بالنيابة عنها.
- الطلاب الذين يدرسون في الجامعة.
- المقاولون والاستشاريون الذين يعملون لصالح الجامعة أو نيابة عنها.
- جميع الأفراد والجماعات الأخرى الذين مُنحوا إمكانية الوصول إلى أنظمة تقنية المعلومات والاتصالات في الجامعة.

تغطي هذه السياسة جميع أصول المعلومات المحددة في وثيقة نطاق تقييم المخاطر وسيتم استخدامها كأساس لإدارة أمن المعلومات.

## 4. ٣ مصطلحات وتعريفات

الجدول رقم (١) يوفر تعريفات ومصطلحات عامة مستخدمة في هذه الوثيقة

| المصطلح | التعريف |
|---|---|
| المساءلة | مبدأ أمني يشير إلى وجوب تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم. |
| أصل | معلومات ذات قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات. |
| توفّر | حالة حصول جهة مصرح لها على أصل من الأصول أو خدمة من الخدمات والقدرة على استخدامها عند الطلب. |
| السرية | عدم إتاحة أصل من الأصول أو خدمة من الخدمات لأفراد أو كيانات أو عمليات غير مصرح بها. |
| الرقابة | وسيلة لإدارة المخاطر، بما في ذلك السياسات والإجراءات والإرشادات التي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو إدارية أو قانونية. |
| الإرشاد | وصف لمتطلبات تحقيق الأهداف المحددة في السياسات وطريقة القيام بهذه المتطلبات. |
| أمن المعلومات | الحفاظ على سرية المعلومات وسلامتها وتوافرها. ويشمل أمن المعلومات استخدام خصائص أخرى تتعلق بها مثل الأصالة والمساءلة وعدم التنصل والموثوقية. |
| السلامة | الحفاظ على الأصول وضمان دقتها وتناسقها طوال دورة حياتها بأكملها. |
| البرامج الضارة | برنامج مصمم لتعطيل تشغيل الحاسب الآلي أو جمع معلومات حساسة أو الوصول إلى أنظمة الحاسب الآلي الخاصة (على سبيل المثال، فيروس أو حصان طروادة). |
| سياسة | خطة عمل لتوجيه القرارات والإجراءات. و تتضمن عملية السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، واختيار البديل الملائم من بينها على أساس التأثير الذي سيحدثه. |
| خطر | مزيج من عواقب الحدث (بما في ذلك التغيّرات في الظروف) واحتمال حدوثها. |
| نظام | جهاز أو نظام مترابط أو أنظمة فرعية من المعدات تُستخدم في الحصول على البيانات أو تخزينها أو معالجتها أو إدارتها أو التحكم فيها أو عرضها أو تبديلها أو تبادلها أو نقلها أو استقبالها، بما في ذلك برامج الحاسب الآلي والبرامج الثابتة والأجهزة. |

**الجدول رقم (١): المصطلحات والتغييرات**

٤. ٤ تغيير السياسة ومراجعتها وتحديثها

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة مبكّرة ضرورية لضمان استمرار السياسة الحالية. والشخص الوحيد المسموح له بإجراء تغييرات في هذه السياسة هو ضابط أمن المعلومات ويجب أن تعتمد الإدارة هذه التغييرات. كما يجب أن يظل سجل التغييرات محدثًا بحيث يتم تحديثه بمجرد إجراء أي تغيير.

٤. ٤ النفاذ والامتثال

يجب الالتزام بهذه السياسة وعلى المسؤول عن أمن المعلومات التأكّد من ذلك بصورة دورية. كما يجب على جميع وحدات الجامعة (من عمادات وإدارات وكليات وأقسام ومراكز) ضمان مراقبة الامتثال المستمر لهذه السياسة في نطاقها.

وفي حالة تجاهل توجيهات أمن المعلومات أو مخالفة هذه التوجيهات، فإنّ بيئة الجامعة قد يلحق بها الضرر (على سبيل المثال، قد يحدث فقدان للثقة في الجامعة أو تفقد الجامعة سمعتها أو قد يتعطّل العمل فيها كما قد تحدث مخالفات قانونية)، وسيكون الأشخاص المخطئون في هذه الحالة مسؤولين عن هذا الضرر مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية ضدهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب أن يعامل الأشخاص الذين يشتبه في انتهاكهم للأوامر الأمنية بطريقة صحيحة وعادلة (مثلاً اتخاذ إجراءات تأديبية). ولمعالجة انتهاكات هذه السياسة، يجب إبلاغ إدارة (الجامعة) وإدارة الموارد البشرية والدخول في المعالجة.

٤. ٦ الاستثناءات

يجب أن ينظر أمن المعلومات في الاستثناءات على أساس فردي. ولاعتماد أيّ استثناء يجب إرفاق قضية عمل مع طلب الاستثناء تحدد فيها الأسباب المنطقية للطلب. يجب أن يوافق المسؤول عن أمن المعلومات على الاستثناءات من شروط الامتثال لهذه السياسة وأن تعتمد عمادة تقنية المعلومات

والاتصالات هذه الموافقة. ويجب أن يتضمّن كل طلب استثناء مبررات الطلب والفوائد المنسوبة إلى الاستثناء.

أقصى فترة للتنازل عن السياسة هي أربعة أشهر، ويجب إعادة تقييمها وإعادة اعتمادها لثلاث فترات متتالية إذا لزم الأمر. ويمنع التنازل عن أي سياسة لأكثر من ثلاث فترات متتالية.

### ٧.٤ الأدوار والمسؤوليات (مصفوفة راكي (RACI))

يوضح الجدول (٢) مصفوفة راكي **(RACI)** [1] التي تحدد من هو المسؤول أو المساءل أو من الذي سيتشار أو سيبلّغ بكل مهمة يجب القيام بها.

هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: عميد تقنية المعلومات والاتصالات، عمادة تقنية المعلومات والاتصالات، موظف أمن المعلومات والمستخدم (الموظف والعقد).

| الدور / المسؤولية | عميد تقنية المعلومات والاتصالات | تقنية المعلومات والاتصالات | المسؤول عن أمن المعلومات | المستخدم |
|---|---|---|---|---|
| الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات. | I | C | C | R,A |
| الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة تقنية المعلومات والاتصالات. | I | C | C | R,A |
| استخدام المعلومات فقط للغرض الذي تقصده جامعة الإمام عبد الرحمن بن فيصل. | | C | C | R,A |
| قبول المساءلة عن جميع الأنشطة المرتبطة بامتيازات وصول المستخدم. | | C | C | R,A |
| توزيع وثائق أمن المعلومات بحيث يكون لدى من يحتاجون إلى هذه المستندات نسخ أو يمكنهم تحديد موقع المستندات بسهولة عبر موقع شبكة انترنت داخلية. | I | C | R,A | I |

**الجدول (٢) الأدوار والمسؤوليات المحددة بناء على مصفوفة راسي *(RACI)***

[1] تصف مصفوفة راكي (RACI) الخاصة بتحديد المسؤوليات الأدوار المختلفة التي يشارك بها أعضاء الفريق في إنجاز مهام العمل. وهي مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات عند تنفيذ عمليات تعدد فيها الوظائف أو الإدارات. يرمز الحرف (R) إلى الموظف الذي ينفذ مهمة من المهام، أما الحرف (A)فيرمز للشخص المسؤول (أو جهة الاعتماد) حيث يوقع هذا الشخص أو يعتمد المهمة المناطة إلى الموظف (R) أما الحرف (C) فيرمز إلى المستشار الذي يقدم رأياً حول ما هو مراد تنفيذه، ويرمز الحرف (I) إلى الشخص الذي يكون على علم ودراية بالمهمة وهو الذي تصله أحدث المعلومات عن سير المهمة.

### ٤. ٨ الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات
- سياسة أمن الموارد البشرية
- سياسة إدارة الأصول
- سياسة التحكم في الوصول
- سياسة إدارة حوادث أمن المعلومات
- سياسة الامتثال

### ٤. 9 الملكية

هذه الوثيقة مملوكة لعمادة تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل، وهي التي تحافظ عليها.

# ٥. عناصر السياسة

تقدم النقاط الفرعية التالية عناصر السياسة في ستة جوانب رئيسة هي:

- سرية المعلومات
- استخدام الحاسب الآلي
- استخدام البريد الإلكتروني
- استخدام الإنترنت
- استخدام كلمة المرور
- استخدام الشبكات والأنظمة

## ٥. ١سرية المعلومات

١. يلتزم المستخدمون التزاما صارما بسياسات أمن معلومات الجامعة ويبلغون عمادة تقنية المعلومات والاتصالات عن أي خرق أمني أو حوادث أو انتهاكات أمنية.

2. يلتزم المستخدمون التزاما تاما في جميع الأوقات باتفاقية عدم الإفصاح الصادرة عن الجامعة في التعامل مع المعلومات السرية المتعلقة بالمعلومات المملوكة لها وحمايتها عند إرسال هذه المعلومات أو حفظها إلكترونيًا.

3. لا يجوز للمستخدمين الإفصاح عن المعلومات المتعلقة بالمعلومات المملوكة للجامعة أو تقديمها لأي شخص (داخل الجامعة أو خارجها) و / أو أي طرف ثالث دون موافقة الإدارة المعنية و أخذ تفويض بذلك.

4. يجب على المستخدمين توخي كل العناية اللازمة لحماية أصول الجامعة. وتقع على عاتق كل مستخدم المسؤوليات التالية:

ا. منع الوصول غير المصرح به، بما في ذلك عرض مصادر المعلومات الخاضعة لمسؤوليته أو سيطرته (مثل المعلومات المتوفرة على أجهزة الحاسب الآلي المحمولة أو أجهزة الحاسب الآلي المكتبية أو محطات الوصول أو المطبوعات أو الوسائط الشريطية وما إلى ذلك).

ب. طباعة معلومات الجامعة السرية على طابعات توفّر عناصر التحكم في الوصول. ولا تطبع المعلومات السرية إلا في ظل رقابة.

ج. إخطار عمادة تقنية المعلومات والاتصالات بأي سلوك شبيه بالفيروس أو الأنشطة المشبوهة على أنظمتها.

5. يجب على المستخدمين عرض شارات التعريف الخاصة بهم (بطاقات الهوية) في جميع الأوقات في مقر الجامعة.

6. يجب على المستخدمين المساهمة والمشاركة بنشاط في مبادرات وأنشطة أمن المعلومات التي ترتبها الجامعة (مثل التدريب والتوعية في مجال الأمن).

7. يجب على المستخدمين قفل و / أو تأمين أي معلومات حساسة (سواء بتنسيقات إلكترونية أو مطبوعة) قبل مغادرة أجهزتهم ومكاتبهم (أي الخوادم ومحطات العمل وأجهزة الحاسب الآلي المحمولة).
8. يجب على للمستخدمين ألا يتركوا أي مستند حسّاس سواء كان وثيقة وردت بالفاكس أو مستنداً مكتوباً.

### ٤.٥ استخدام البريد الإلكتروني

١. يجب على المستخدمين استخدام خدمات البريد الإلكتروني فقط لأعمال الجامعة.

٢. يكون المستخدمون مسؤولون عن الاستخدام المناسب ونشر المعلومات من خلال خدمات البريد الإلكتروني التي تقدمها الجامعة.

٣. لا يجوز للمستخدمين الوصول إلى حسابات و / أو خدمة البريد الإلكتروني للمستخدمين الآخرين دون الحصول على إذن مناسب من عمادة تقنية المعلومات والاتصالات.

٤. لا يجوز للمستخدمين استخدام خدمات البريد الإلكتروني الداخلية والخارجية لإرسال المعلومات السرية المتعلقة بالأعمال في الجامعة دون موافقة مسبقة وإذن من إدارتهم.

٥. لا يجوز للمستخدمين استخدام خدمات البريد الإلكتروني للأنشطة غير القانونية، بما في ذلك إرسال أو تلقي مواد محمية بحقوق الطبع والنشر في انتهاك لقوانين حقوق النشر أو اتفاقيات الترخيص.

٦. لا يجوز للمستخدمين إرسال رسائل سلسلة أو بريد مزعج أو إعادة توجيه متعددة غير ضرورية مثل تحيات العطلات الجماعية.

٧. لا يجوز للمستخدمين تعميم و / أو إرسال تنبيهات الفيروسات الواردة عبر البريد الإلكتروني إلى أي شخص آخر غير عمادة تقنية المعلومات والاتصالات.

٨. لا يجوز للمستخدمين الاشتراك في أي مجموعة بريدية سواء كانت محلية أو دولية لأي سبب غير الأغراض التجارية.

### ٥. ٦استخدام الانترنت

١. يجب على المستخدمين فقط استخدام الوصول إلى الإنترنت لأنشطة أعمال الجامعة.

٢. لا يجوز للمستخدمين استخدام خدمة الإنترنت في أنشطة غير قانونية، بما في ذلك إرسال أو استلام المواد المحمية بحقوق الطبع والنشر في انتهاك لقوانين حقوق النشر أو اتفاقيات الترخيص المعمول بها.

٣. يكون المستخدمون مسؤولين ومحاسبين عن الاستخدام المناسب للمعلومات ونشرها من خلال خدمات الإنترنت التي تقدمها الجامعة.

٤. لا يجوز للمستخدمين استخدام أنظمة الجامعة لتوزيع أي رموز أو معلومات ضارة أو مدمرة و / أو احتيالية، أو إدراج أو تمكين فيروسات الكمبيوتر أو رموز الفيروسات أو القيام بأي أنشطة قرصنة داخل أو خارج بيئة الجامعة.

٥. لا يجوز للمستخدمين استخدام خدمات المراسلة الفورية والشبكات الاجتماعية للدردشة مع المشتركين المحليين أو الدوليين عبر الإنترنت.

**٥. ٥ كلمة المرور**

١. يجب على المستخدمين عدم تبادل أو الكشف عن اسم المستخدم أو كلمة المرور لأي أحد.

٢. تقع على المستخدمين مسؤولية اختيار كلمات مرور آمنة والحفاظ عليها وفقاً لسياسة كلمة المرور بالجامعة.

**3**. يجب على المستخدمين ألا يجعلوا تسجيل الدخول التلقائي على الأنظمة خياراً ممكناً بحفظهم لكلمات المرور.

٥. ٦ استخدام الشبكة والانظمة

١. لا يجوز أن يدخل المشغلون برامج ضارة (مثل الفيروسات والديدان وأحصنة طروادة وقنابل البريد الإلكتروني وما إلى ذلك) في أنظمة الجامعة.

٢. لا يجوز للمستخدمين التعريف ببرامج مجانية أو برامج حاسب آلي في شبكة المؤسسة، سواء تم تنزيلها من الإنترنت أو تم الحصول عليها من خلال أي وسائط أخرى، دون إذن من عمادة تقنية المعلومات والاتصالات.

٣. لا يجوز للمستخدمين استخدام أنظمة الجامعة لتخزين بيانات يمكن تفسيرها على أنها منحازة (على سبيل المثال، سياسيًا أو دينيًا أو عرقيًا أو عرقيًا، إلخ) أو معالجتها أو تنزيلها أو نقلها.

٤. لا يجوز للمستخدمين إيقاف تشغيل حزمة برامج الكشف عن الفيروسات المعتمدة من الجامعة، أو استخدام أي حزمة برامج لمكافحة فيروسات أخرى دون موافقة كتابية من عمادة تقنية المعلومات والاتصالات.

٥. لا يجوز للمستخدمين إجراء مسح ضوئي أو مسح أمان لشبكة أو أنظمة الجامعة ما لم يكن ذلك مصرحًا به من قبل عمادة تقنية المعلومات والاتصالات ويتم إرسال إخطار مسبق إلى الموظفين المعنيين.

٦. لا يجوز للمستخدمين تنفيذ أي شكل من أشكال مراقبة الشبكة التي تعترض البيانات غير المخصصة لمضيف الموظف، ما لم يكن هذا النشاط جزءًا من العمل المصرح به للموظف أو جزءاً من الواجب المناط إليه.

٧. لا يجوز للمستخدمين التحايل على مصادقة المستخدم أو أمن أي مضيف أو شبكة أو حساب.

٨. لا يجوز للمستخدمين استخدام أي برنامج أو إرسال رسائل من أي نوع، بقصد التدخل في جلسة عمل مستخدم لجهاز طرفي أو تعطيله، عبر أي وسيلة ، محليَّةً كانت أو خارجيَّة.

---------- النهاية ----------