ابتكار الأعمال الملهمة


# سياسة الامتثال

الإصدارة ١,١

**رقم السياسة:**

## ١. جدول المحتويات


١. جدول المحتويات ..... ٢
2. معلومات ذات ملكية فكرية ..... ٣
3. الرقابة على الوثيقة ..... Error! Bookmark not defined.
3.1. معلومات عن الوثيقة ..... ٤
3.2. الإعداد والتحديث ..... Error! Bookmark not defined.
3.3. المراجعة والتحقق والاعتماد ..... ٤
3.4. قائمة التوزيع ..... ٤
4. نظرة عامة على السياسة ..... ٥
4.1. الغرض ..... ٥
4.2. النطاق ..... ٥
4.3. المصطلحات والتعاريف ..... ٥
4.4. التغيير والمراجعة والتحديث ..... ٦
4.5. الإنفاذ / الامتثال ..... ٧
4.6. الاستثناءات ..... Error! Bookmark not defined.
4.7. الأدوار والمسؤوليات (مصفوفة راكي) ..... ٧
4.8. الوثائق ذات الصلة ..... ١٠
4.9. الملكية ..... ١١
5. البيانات السياسية ..... ١١
5.1. تحديد التشريعات المعمول بها والمتطلبات التعاقدية ..... ١١
5.2. حقوق الملكية الفكرية ..... ١٢
5.3. حماية السجلات ..... ١٣
5.4. خصوصية وحماية معلومات التعريف الشخصية ..... ١٣
5.5. تنظيم ضوابط التشفير ..... ١٤
5.6. المراجعة المستقلة لأمن المعلومات ..... ١٤
5.7. الامتثال للسياسات والمعايير الأمنية ..... ١٤
5.8. مراجعة الامتثال الفني ..... ١٥

## 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

### معلومات عن الوثيقة

| العنوان | تصنيف | الإصدار | الحالة |
|---|---|---|---|
| سياسة الامتثال | سري | 1.0 | التحقق من صحة |

### الإعداد والتحديث

| الإصدارة | إعداد/ تحديث | تاريخ الاصدار | التغييرات |
|---|---|---|---|
| 0.1 | علاء عليوه | 18نوفمبر 2014 | إعداد |
| 0.2 | نبيل البحبوح | 1ديسمبر 2014 | تحديث |
| 0.3 | أسامة العمري | ٢٣ ديسمبر 2014 | QA |
| 1.1 | نبيل البحبوح | 24أبريل 2017 | تحديث |

### مراجعة والتحقق والموافقة

| الاسم | العنوان | التاريخ |
|---|---|---|
| لمياء عبد الله الجعفري | مدير الجودة | |
| الدكتورخالد العيسى | عميد تقنية المعلومات والاتصالات | |
| | | |

### قائمة التوزيع

| عدد ال نسخ | المستفيدين | موقعك |
|---|---|---|
| | | |
| | | |

# ٤. نظرة عامة على السياسة

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

### الهدف

الغرض الرئيسي من سياسة الامتثال هو:

تجنب انتهاك الالتزامات القانونية أو القانونية أو التنظيمية أو التعاقدية المتعلقة بأمن المعلومات وأي متطلبات أمنية.

### 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.

### المصطلحات والتعاريف

يقدم الجدول ١ تعريفات للمصطلحات الشائعة المستخدمة في هذا المستند.

| مصطلح | تعريف |
|---|---|
| **المسا ءلة** | **مبدأ أمني يشير إلى وجوب تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.** |
| **الأصول** | **معلومات لها قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام** |

| | |
|---|---|
| | **المعلومات.** |
| **توفر** | **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 والمبادئ التوجيهية التي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو إدارية أو قانونية.** |
| **الإرشاد** | **وصف لما يجب القيام به وكيفية تحقيق الأهداف المحددة في السياسات.** |
| **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.** |
| **الملكية الفكرية** | **فئة الممتلكات المعنوية (غير المادية) التي تتألف في المقام الأول من الحقوق المتعلقة بالمواد المحمية بحقوق النشر والعلامات التجارية وبراءات الاختراع والتصميم الصناعي.** |
| **صاحب** | **أي شخص أو مجموعة من الأشخاص الذين تم تحديدهم من قِبل الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. وقد يتغير الصاحب أثناء دورة حياة الأصل.** |
| **السياسة** | **خطة عمل لتوجيه القرارات والإجراءات. تتضمن عملية السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.** |
| **الخصوصية** | **حق الفرد في أن يكون آمنًا من الإفصاح غير المصرح به لمعلومات عن نفسه مضمنة في المستندات.** |
| **خطر** | **مجموعة العواقب التي تنجم عن حدث من الأحداث (بما في ذلك التغييرات في الظروف) واحتمال حدوثها.** |
| **المورّد** | **الطرف الذي يوفر المعدات أو الخدمات.** |
| **النظام** | **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 ١: المصطلحات والتعاريف**

## التغيير والمراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر صاحبها إجراء مراجعة سابقة 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.

**النفاذ / الامتثال**

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.

**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 لعمل استثناءات من هذه السياسة هي أربعة أشهر، ويجب إعادة تقييم الاستثناءات وإعادة اعتمادها لثلاث فترات متتالية إذا لزم الأمر. ويمنع الاستثناء من أيّ سياسة لأكثر من ثلاث فترات متتالية.

**الأدوار والمسؤوليات (مصفوفة راكي)**

يوضح الجدول ٣ مصفوفة راكي[١] (RACI) التي تحدد من هو المسؤول ومن الذي ستتم استشارته بشأن كل مهمة يجب القيام بها ومن سيبلّغ بها.

هناك بعض الأدوار التي تقوم بها الأطراف ذات الصلة بهذه السياسة وهي على التوالي كما يلي: الإدارة، مدير عمليات تقنية المعلومات والاتصالات، عمادة تقنية المعلومات والاتصالات، موظف أمن المعلومات، الإدارة القانونية، الوحدة الإدارية بإدارة الموارد البشرية ، المراجع الداخلي و الخارجي ، الصاحب و المستخدم (الموظف والمتعاقد).

| الأدوار / المسؤوليات | الإدارة | مدير التشغيل | تقنية المعلومات والاتصالات | ضابط أمن المعلومات | الإدارة القانونية | الوحدة الإدارية | المراجع | المستخدم |
|---|---|---|---|---|---|---|---|---|
| إجراء التحقق من الامتثال ومراجعته للتحقق من الامتثال لسياسات أمن معلومات جامعة الإمام عبد الرحمن بن فيصل. | I | | R,C | R,A | | | | |
| مساعدة فريق التدقيق الخارجي المستقل في إجراء عمليات تدقيق لأمن المعلومات في أنظمة الجامعة بشكل دوري. | I | | R,C | R,A | | | | |
| تطبيق الضوابط المناسبة لحماية سرية وسلامة وصحة المعلومات الحساسة. | I | | R,A | C | | | | |
| إجراء تدقيق داخلي لأنظمة الجامعة المهمة جداً باستخدام أدوات التدقيق المناسبة. | I | | R,A | R,C | | | | |
| التأكد من أن سياسات أمن المعلومات متوافقة مع المتطلبات القانونية والتعاقدية الخاصة بالجامعة. | I | | R | C | R | | | I |
| تقديم المشورة القانونية المتخصصة اللازمة للإدارات الأخرى لتقديم الخدمات بطريقة متوافقة تمامًا مع القوانين واللوائح الحالية. | I | | R | C | R | | | |
| توزيع وثائق أمن المعلومات بحيث يكون لدى من يحتاجون إلى هذه المستندات نسخ أو يمكنهم تحديد موقع المستندات بسهولة عبر موقع إنترانت. | I | | C | R,A | | R,C | | I |

| الأدوار / المسؤوليات | الإدارة | مدير التشغيل | تقنية المعلومات والاتصالات | ضابط أمن المعلومات | الإدارة القانونية | الوحدة الإدارية | المراجع | المستخدم |
|---|---|---|---|---|---|---|---|---|
| الالتزام بسياسات وإرشادات أمن المعلومات والإجراءات المتعلقة بحماية المعلومات. | | | C | C | | C | | R,A,I |
| الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة تقنية المعلومات والاتصالات. | I | | A,C | C | | | | R |
| قبول المساءلة عن جميع الأنشطة المرتبطة بامتيازات الوصول إلى الاستخدام. | I | | A,C | C | | | | R |
| استخدام المعلومات فقط للغرض الذي تقصده الجامعة | I | | A,C | C | | | | R |
| إدارة جميع أنشطة تدقيق أمن المعلومات. | | | | | | | | |
| تطوير خطة التدقيق السنوية. | | C, I | I | C, I | | | R,A | |
| إبلاغ مدير عمليات تقنية المعلومات والاتصالات بنتائج التدقيق. | | C, I | I | C, I | | | R,A | |
| ضمان الامتثال لممارسات وسياسات وإجراءات أمن المعلومات. | | C, I | I | C, I | | | R,A | |
| مراقبة الامتثال لسياسات وإجراءات وإرشادات ومعايير أمن المعلومات إلى جانب المعايير الخارجية المختارة. | | C, I | I | C, I | | | R,A | |

**الجدول ٣: الأدوار والمسؤوليات بناءً على مصفوفة راكي ( *RACI*)**

(I) تصف مصفوفة راكي (RACI) الخاصة بتحديد المسؤوليات والأدوار المختلفة التي يشارك بها أعضاء الفريق في إنجاز مهام العمل. وهي مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات عند تنفيذ عمليات تتعدد 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.

**الوثائق ذات الصلة**

فيما يلي جميع السياسات والإجراءات ذات الصلة لهذه السياسة:

- سياسة أمن المعلومات
- سياسة تنظيم أمن المعلومات
- سياسة أمن الموارد البشرية
- سياسة إدارة الأصول
- سياسة التحكم في الوصول
- سياسة التشفير
- سياسة الأمن المادي والبيئي
- سياسة أمن العمليات
- سياسة أمن الاتصالات
- سياسة اقتناء النظام وتطويره وصيانته
- سياسة علاقات المورّدين
- سياسة إدارة حوادث أمن المعلومات
- سياسة جوانب أمن المعلومات لاستمرارية العمل
- سياسة إدارة المخاطر
- سياسة الاستخدام المقبول
- إجراءات تصنيف الأصول
- إجراءات إدارة التغيير
- إجراءات إدارة التصحيح
- إجراءات إدارة المخاطر
- إجراءات التعامل مع حوادث أمن المعلومات

- إجراءات التحكم في الوصول المادي والمنطقي
- إجراءات أمن الموارد البشرية
- النسخ الاحتياطي واستعادة الإجراء
- إجراءات الحول على نظام وتطويره وصيانته.

**الملكية**

هذه الوثيقة مملوكة عمادة تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل و هي التي تحافظ عليها.

**بيانات السياسة**

تقدم الأقسام الفرعية التالية بيانات السياسة في ثمانية جوانب رئيسة **هي:**

- تحديد التشريعات المعمول بها والمتطلبات التعاقدية
- حقوق الملكية الفكرية
- حماية السجلات
- خصوصية وحماية معلومات التعريف الشخصية
- لائحة ضوابط التشفير
- المراجعة المستقلة لأمن المعلومات
- الامتثال للسياسات والمعايير الأمنية
- مراجعة الامتثال الفني

**تحديد التشريعات المعمول بها والمتطلبات التعاقدية**

١. يجب على عمادة تقنية المعلومات والاتصالات بالتعاون مع الوحدة الإدارية أو إدارة الموارد البشرية تحديد وتحليل جميع المتطلبات القانونية والتنظيمية والقانونية والتعاقدية المطبقة ، واتخاذ التدابير المناسبة للامتثال لها. ويجب تغطية المجالات التالية:

المعايير والمبادئ التوجيهية ذات الصلة المتعلقة بأنظمة جامعة.

المتطلبات الحكومية و (أو) الخارجية ذات الصلة (مثل القوانين والتشريعات والتوجيهات واللوائح والمعايير) المتعلقة بالعلاقات الخارجية ومراجعات المتطلبات الخارجية.

قوانين العمل، وخاصة معالجة متطلبات السلامة والصحة المتعلقة ب تقنية المعلومات.

حقوق الملكية الفكرية / قوانين حقوق النشر للبرنامج.

متطلبات أمن الأنظمة، خاصة فيما يتعلق باستخدام بيانات التشفير ونقل البيانات.

تقارير التدقيق من المراجعين الخارجيين ومقدمي الخدمات الخارجيين والوكالات الحكومية.

2. يجب إجراء تصميم وتشغيل وإدارة واستخدام الأنظمة والمرافق ذات الصلة وفقًا لمتطلبات الأمن القانونية أو التنظيمية أو التعاقدية المعمول بها.

***REF:[ISO/IEC 27001: A.18.1.1]***

**حقوق الملكية الفكرية**

١. على عمادة تقنية المعلومات والاتصالات أن تعترف بحقوق الملكية الفكرية المرتبطة بأنظمتها وتحترمها (وهي تشمل حقوق المؤلف المتعلقة بالبرامج الإلكترونية أو المستندات ، وحقوق التصميم ، والعلامات التجارية ، وبراءات الاختراع وتراخيص شفرة المصدر).

٢. يجب تنفيذ الإجراءات المناسبة لضمان الامتثال للمتطلبات التشريعية والتنظيمية والتعاقدية بشأن استخدام المواد التي قد تكون لها حقوق ملكية فكرية وبشأن استخدام منتجات البرمجيات مسجلة الملكية مثل حقوق النشر وحقوق التصميم والعلامات التجارية.

٣. يجب أن تلتزم عمادة تقنية المعلومات والاتصالات بالمتطلبات التالية:

i. شراء وإصدار جميع البرمجيات المستخدمة وفقًا لاتفاقيات الترخيص..

ii. عدم إشراك شخص أو جهة في أي نسخ غير مصرح به البرمجيات..

iii. الحفاظ على الأدلة والبراهين التي تؤكد ملكية التراخيص أو الأدلة الإرشادية..

iv. تحديد جميع متطلبات الترخيص التي تحد من استخدام المنتجات والبرامج والتصميمات وغيرها من المواد المكتسبة..

v. يجب على جميع العاملين الذين يستخدمون نظم المعلومات التقيد الصارم بقوانين حقوق النشر والقيود المفصلة من قبل بائع البرنامج الإلكتروني.

vi. عدم دبلجة مواد الجهات الخارجية، أو تحويلها إلى تنسيق آخر أو استخراجها من التسجيلات التجارية (مثل الفيديو والصوت) بخلاف ما تسمح به سياسة حقوق الطبع والنشر.

**vii.** وضع سياسة موثقة تحدد الطريقة المناسبة للتخلص من البرمجيات أو نقلها..

***REF: [ISO/IEC 27001: A.18.1.2]***

**حماية السجلات**

١. يجب وضع مجموعة من الإجراءات الموثقة لتحديد طرق تصنيف السجلات، بالإضافة للضوابط المناسبة لحمايتها من الضياع والتدمير والتزوير.

٢. ينبغي أن تنظر عمادة تقنية المعلومات والاتصالات فيما يلي لضمان الحماية الصحيحة للسجلات:

أ- حماية السجلات بناءً على علاقة السجل بالموضوع وبناء على أهميته.

ب- تخزين السجلات بطريقة تلائم الوسائط المسجلة عليها.

ج - تصنيف السجلات إلى أنواع مختلفة (مثل سجلات الموظفين وسجلات الأنظمة وسجلات قواعد البيانات وسجلات التدقيق والإجراءات التشغيلية)، مع تقديم تفاصيل عن فترات الاستبقاء ونوع وسائط التخزين (مثل الورق والوسائط المغناطيسية والبصرية).

***REF: [ISO/IEC 27001: A.18.1.3]***

**خصوصية وحماية معلومات التعريف الشخصية**

١. ينبغي أن تقوم عمادة تقنية المعلومات والاتصالات بإعداد وتنفيذ سياسة لحماية البيانات والخصوصية تحدد المتطلبات الواردة في القوانين واللوائح ذات الصلة والمتطلبات التعاقدية الخاصة بجامعة الإمام عبد الرحمن بن فيصل.

٢. لا يجوز لأي موظف في جامعة الإمام عبد الرحمن بن فيصل تبادل معلومات سرية أو مملوكة للجامعة أو بيانات تتعلق بالعاملين فيها، مع كيانات أو وكالات أو جهات خارجية أو وحدات عمل أخرى ما لم يمنح إذناً بتبادل هذه المعلومات واستناداً إلى متطلبات أعمال الجامعة.

***REF:[ISO/IEC 27001: A.18.1.4]***

**تنظيم ضوابط التشفير**

١. يجب استخدام جميع عناصر التحكم في التشفير (على سبيل المثال ، القيود المفروضة على استيراد أو تصدير أجهزة وبرامج الحاسب الآلي لأداء وظائف التشفير) وفقًا لجميع اللوائح والقوانين والاتفاقيات ذات الصلة عندما يقتضي الأمر ذلك.

***REF: [ISO/IEC 27001: A.18.1.5]***

**المراجعة المستقلة لأمن المعلومات**

١. يجب على إدارة جامعة الإمام عبد الرحمن بن فيصل إنشاء وحدة مراجعة داخلية مستقلة لإدارة أمن المعلومات وتكليف أشخاص للقيام بمهامها (وهي سبيل المثال ، التدقيق الداخلي والخارجي ، والتحقق من الامتثال الفني).

٢. يجب إجراء مراجعة داخلية مستقلة بشكل دوري (مرة واحدة في السنة على الأقل):

أ. بعد مراجعة سياسة أمن المعلومات.

ب. عند إجراء تغييرات كبيرة على مصادر معلومات جامعة الإمام عبد الرحمن بن فيصل أو بنيتها التحتية التقنية.

ج. في حالة حدوث تغيير في متطلبات الجامعة أو السياق القانوني.

٣. ينبغي إجراء مراجعة داخلية مستقلة لأمن المعلومات للتحقق مما إذا كان الطريقة التي تسلكها عمادة تقنية المعلومات والاتصالات لإدارة وتنفيذ أمن المعلومات كافية وفعالة. (على سبيل المثال، تتبّع أهداف أمن المعلومات والسياسات والإجراءات والعمليات المتعلقة بأمن المعلومات)

***REF: [ISO/IEC 27001: A.18.2.1]***

**الامتثال للسياسات والمعايير الأمنية**

١. يجب على جميع العاملين بجامعة الإمام عبد الرحمن بن فيصل فهم سياسات وإجراءات أمن المعلومات الخاصة بالجامعة والإقرار المسؤولية تجاه الامتثال لها.

٢. يجب على رؤساء الأقسام والمسؤولين عن الوحدات الإدارية بالجامعة القيام بمراجعة منتظمة لمدى الامتثال لأمن الأنظمة في نطاق مسؤوليتهم عن السياسات والمعايير الأمنية الصحيحة وأي متطلبات أمنية أخرى. ويجب تسجيل نتائج المراجعات والإجراءات التصحيحية التي تنفّذ والحفاظ عليها.

***REF: [ISO/IEC 27001: A.18.2.2]***

**مراجعة الامتثال الفني**

١. يجب أن يتم التخطيط لمتطلبات وأنشطة التدقيق التي تغطي عمليات فحص الأنظمة التشغيلية بعناية وتنفيذها على فترات دورية (على الأقل سنويًا) مع معرفة أصحاب الأصول لتقليل مخاطر حدوث اضطرابات في العمليات التجارية.

٢. عندما تتطلب عمليات تدقيق النظام الوصول إلى النظام أو البيانات التي تتضمن استخدام أدوات البرنامج وأدواته المساعدة، يجب إجراء هذه التدقيقات بمعرفة أصحاب الأصول والتعاون معهم وموافقتهم، ويجب اتخاذ الاحتياطات ذات الصلة لحماية أنظمة وبيانات جامعة الإمام عبد الرحمن بن فيصل من التلف أو الاضطرابات نتيجة للتدقيق أو أدواته.

٣. يجب على ضابط أمن المعلومات بالتعاون مع عمادة تقنية المعلومات والاتصالات إجراء عمليات تدقيق داخلية وخارجية مستقلة لأنظمة العمادة في جامعة الإمام عبد الرحمن بن فيصل. يجب أن يكون الشخص (أو الأشخاص) الذين يقومون بالتدقيق مستقلين عن الأنشطة التي تم تدقيقها. ويجب توفير أي وصول مطلوب لأعضاء فريق التدقيق الخارجي عند إجراء التدقيق. وقد يشمل هذا الوصول على سبيل المثال لا الحصر ما يلي:

أ- الوصول إلى مستوى المستخدم و / أو مستوى النظام إلى أي جهاز حوسبة أو اتصالات.

ب- الوصول إلى المعلومات (على سبيل المثال، المعلومات الإلكترونية أو المطبوعة) التي قد يتم إنتاجها أو نقلها أو تخزينها على معدات أو مقار أقسام معنية.

ت- الوصول إلى مناطق العمل (على سبيل المثال، مركز البيانات).

ث- الوصول إلى التقارير أو الوثائق التي تم إنشاؤها أثناء التدقيق الداخلي.

ج- الوصول إلى رصد وتسجيل حركة المرور بشكل تفاعلي على الشبكات.

***REF: [ISO/IEC 27001: A.15.2.3]***

---------- نهاية الوثيقة ----------