# جامعة الإمام عبد الرحمن بن فيصل
# IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

## سياسة ملفات تعريف الارتباط

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-12.CS.A. V2.0

## 1. جدول المحتويات

## 2. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة الاتصالات وتقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة الاتصالات وتقنية المعلومات.

## 3. الرقابة على الوثيقة

### 1.3 معلومات عن الوثيقة

| العنوان | التصنيف | الإصدار | الحالة |
|---|---|---|---|
| سياسة ملفات تعريف الارتباط | مقيد | V2.0 | فعال |

### 2.3 تاريخ الإعداد والتّحديث

| الإصدار | المؤلفون | تاريخ الاصدار | التغييرات |
|---|---|---|---|
| V1.0 | د. بشار الذيب | 2021/02/29 | إنشاء |
| V1.1 | د. سامر بني عواد | 2022/01/24 | مراجعة وتحديث |
| V2.0 | بهاء نوافله | 2023/12/23 | مراجعة وتحديث |
| | | | |
| | | | |

### 3.3 المراجعة والتدقيق

| تاريخ المراجعة القادمة |
|---|
| 2025/01/01 |

### 4.3 قائمة التوزيع

| الرقم | المستفيد |
|---|---|
| 1 | جميع أقسام عمادة الاتصالات وتقنية المعلومات |
| 2 | الشؤون القانونية |
| 3 | الموقع الإلكتروني |
| 4 | |

### 5.3 الاعتماد

| الاسم | الوظيفة | رقم القرار | التاريخ |
|---|---|---|---|
| د. نهاد بنت عبد الله العمير | نائب الرئيس للتطوير والشراكة المجتمعية | 61945 | 2024/03/06 |

## 4. المقدمة

حماية الأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني بتحديد ضوابط أمن جميع المعلومات والبيانات، حيث تعتبر البيانات الشخصية عنصر مهم من البيانات التي يجب حمايتها في الجامعة والجهات المحتضنة لديه. ولذلك وجب وضع مقاييس وضوابط لحماية البيانات التي تم الاحتفاظ بها وتخزينها والخاصة بالمستخدمين في المواقع الإلكترونية التابعة للجامعة بهدف الحد من مخاطر الإفصاح أو التسريب أو الوصول الغير المصرح به أو العبث والتزوير.

تُدرج هذه السياسة في إطار سياسة الجامعة وتحت الصلاحيات الممنوحة من صاحب الصلاحية ابتداءً من تاريخ اعتمادها.

## 5. الهدف

تحدد توجهات هذه السياسة الممارسات التي تتم في الجامعة فيما يتعلق بمعالجة واستخدام ملفات تعريف الارتباط على خدمات الجامعة.

## 6. قابلية التطبيق ونطاق العمل

تنطبق أحكام هذه السياسة على جميع العاملين أو المكلفين الذين يعملون في الجامعة سواء بعقود دائمة أو مؤقتة وبشكل مباشر أو غير مباشر بما في ذلك الموردين والمقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أو المؤقت إلى بيانات الجامعة مهما كان مصدرها أو شكلها أو طبيعتها وإلى أنظمة وأجهزة وقواعد بيانات الجامعة.

## 7. السياسة

### 1.7 متطلبات السياسة العامة

1.1.7 يجب مراجعة وحماية خاصية ملفات تعريف الارتباط التعريف المخزنة على موقع الجامعة الإلكتروني بانتظام وأن يتم حذفها حسب الحاجة للعاملين والمستفيدين.

2.1.7 يجب تخزين خاصية ملفات تعريف الارتباط للعاملين بالجامعة والمستفيدين ومعالجتها أو نقلها بطريقة دقيقة وآمنة وفقاً لمتطلبات العمل.

3.1.7 في حال الضرورة ووجود سبب مشروع وفقاً للقوانين والأنظمة ذات العلاقة، يجب الحصول على موافقة صريحة من صاحب البيانات الخاضعة لجمع ملفات تعريف الارتباط ومعالجة بياناتها.

4.1.7 يجب أن تتم الإشارة الى استخدام خاصية ملفات تعريف الارتباط للخدمات الموجودة على مواقع الجامعة الإلكترونية؛ وذلك بإعلام المستخدمين بنوع البيانات التي يتم جمعها وماهي الجهات التي يتم مشاركة وتخزين ومعالجة تلك البيانات معها. كما يجب إعطائهم حق إغلاق خاصية ملفات تعريف الارتباط.

5.1.7 يجب أن تتاح إمكانية مسح البيانات التي يتم تخزينها من خلال خاصية ملفات تعريف الارتباط والبيانات الأخرى المرتبطة بها حسب الإمكان.

6.1.7 يجب أن يقوم الجامعة بتطبيق تقنيات إخفاء الهوية والتشفير لحماية البيانات الشخصية المخزّنة في ملفات تعريف الارتباط.

7.1.7 يجب أن يكون العاملين لدى الجامعة على علم بمحتوى هذه السياسة ومعرفة أدوارهم في حماية بيانات التعريف الشخصية للعاملين والمستفيدين لدى الجامعة.

8.1.7 يجب أن يعتمد الجامعة على مقاييس تقنية وتنظيمية مناسبة للتأكد من أن البيانات التي يتم تخزينها في ملفات تعريف الارتباط لا يتم تخزينها لغير الضرورة. وينطبق هذا على كمية البيانات الشخصية التي يتم جمعها ومدى معالجتها ومدة تخزينها ومن يمكنه الوصول إليها على وجه الخصوص، كما يجب على الجامعة ضمان عدم إتاحة البيانات الشخصية بشكل افتراضي لعدد غير محدد من الأشخاص دون اتخاذ أي إجراء فيما يتعلق بخصوصية البيانات.

## 8. الأدوار والمسؤوليات

**يجب على إدارة الأمن السيبراني:**

1.1.8 على مدير الأمن السيبراني اعتماد السياسة من صاحب الصلاحية والعمل على تنفيذها.

2.1.8 على مدير الأمن السيبراني اعتماد المعايير والإجراءات والتوجيهات لضمان الالتزام الضروري بمتطلبات أمن عمليات الجامعة.

3.1.8 على مدير الأمن السيبراني ضمان التوافق بين هذه السياسة وأعمال الجامعة.

4.1.8 على مدير الأمن السيبراني حل أي تعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة حيثما أمكن.

6.1.8 على إدارة الأمن السيبراني تعميم سياسة الالتزام بالأمن السيبراني وحوكمة البيانات على جميع إدارات وموظفي ومستخدمي الجامعة المصرح لهم أو الذين سيصرح لهم الوصول إلى الأصول التقنية والمعلوماتية.

7.1.8 على إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

8.1.8 على إدارة الأمن السيبراني مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

**يجب على عمادة الاتصالات وتقنية المعلومات:**

9.1.8 الالتزام بهذه السياسة، وتنفيذ الضوابط المذكورة في هذه السياسة وكذلك الإبلاغ عن أي حادث أمني لإدارة الأمن السيبراني.

**يجب على الإدارة العليا ومدراء الإدارات ورؤساء الوحدات والمستشارين ما يلي:**

10.1.8 التأكد من مشاركة هذه السياسة لجميع العاملين داخل الجامعة أو الملف.

11.1.8 إبلاغ إدارة الأمن السيبراني عن أي تجاوزات أو عدم التزام بهذه السياسة.

**يجب على العاملين في الجامعة الالتزام بأحكام هذه السياسة والإبلاغ عن أي حادث أمني أو عدم التزام بأي أحكام واردة في هذه السياسة الى مدير الأمن السيبراني.**

## 9. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

## 10. تغييرات السياسة

يجب مراجعة السياسة سنويًا على الأقل أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الجامعة.

## 11. الالتزام

يجب على جميع العاملين في الجامعة والأطراف (الخارجية/المتعاقد معهم) الالتزام بأحكام هذه السياسة، ويجب على مدير الأمن السيبراني في الجامعة ضمان المراقبة المستمرة للالتزام، ورفع التقارير اللازمة بهذا الشأن لصاحب الصلاحية بشكل دوري.

يجب اتخاذ الإجراءات اللازمة لضمان الالتزام بأحكام هذه السياسة، وذلك من خلال قيام إدارة الأمن السيبراني أو الإدارات ذات العلاقة بمراجعة دورية، واتخاذ إجراءات تصحيحية من قبل صاحب الصلاحية في الجامعة وفقاً للتوصيات المقدمة من قبل مدير الأمن السيبراني حيال أي انتهاك لأي من أحكام هذه السياسة، على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يسفر عنه التحقيق بهذا الخصوص، وتتضمن الإجراءات التأديبية على سبيل المثال لا الحصر الآتي:

- سحب صلاحية الوصول إلى البيانات وأصول تقنية المعلومات وأنظمة الجامعة المتصلة بها.
- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما يراه الجامعة من إجراءات مناسبة.

يستوجب عدم الالتزام بأي من أحكام هذه السياسة -دون الحصول على استثناء مسبق من إدارة الأمن السيبراني - اتخاذ الإجراءات المناسبة وفقًا للسياسات واللوائح المعمول بها في الجامعة، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية مع أي أشخاص أو جهات متعاقد معهم.

## 12. السياسات والمعايير والإجراءات ذات العلاقة

- ❖ DICT.I.06-01.CS.A. V2.0- السياسة العامة للأمن السيبراني وحوكمة البيانات
- ❖ DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- ❖ DICT.I.06-03.CS.A. V2.0- سياسة حماية البيانات
- ❖ DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- ❖ DICT.I.06-13.CS.A. V2.0- سياسة حماية البيانات الشخصية
- ❖ DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- ❖ DICT.I.06-33.CS.A. V2.0- سياسة التحكم في الوصول
- ❖ DICT.I.06-53.CS.A.V2.0- معايير الحماية من فقدان البيانات

- DICT.I.06-56.CS.A.V2.0- معايير أمن البيانات
- DICT.I.06-58.CS.A.V2.0- معايير أمن قواعد البيانات
- DICT.I.06-61.CS.A.V2.0- معايير حماية البيانات
- DICT.I.06-71.CS.A.V2.0- معايير التشفير

## 13. المراجع

| اسم القسم | الضوابط الأساسية للأمن السيبراني | ضوابط الأمن السيبراني للأنظمة الحساسة | ضوابط الأمن السيبراني عن بعد للعمل | ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات | ضوابط الأمن السيبراني للحوسبة السحابية | الآيزو 27001:2013 | المعهد الوطني للمعايير والتقنية |
|---|---|---|---|---|---|---|---|
| متطلبات السياسة العامة | 1-15-2 | - | - | - | - | - | - |

----------نهاية الوثيقة----------