جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة حماية البيانات الشخصية

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-13.CS.A. V2.0

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

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 حماية البيانات الشخصية	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/02	إنشاء
V1.1	د. سامر بني عواد	2022/01/24	مراجعة وتحديث
V2.0	بهاء نوافله	2024/01/05	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 البيانات الشخصية أمر ضروري لنجاح أعمال الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني على تمكين التدابير والضوابط للحد من مخاطر الكشف عن البيانات الشخصية وتسريبها والوصول غير المصرح به إليها وتعديلها والعبث بها. وتحدد هذه الوثيقة سياسة حماية البيانات الشخصية داخل الجامعة وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

5. الهدف

تهدف هذه السياسة إلى تحديد المتطلبات اللازمة للمحافظة على خصوصية البيانات الشخصية وسريتها والمحافظة على حقوق الأفراد عند التعامل مع البيانات الشخصية في الجامعة وفقاً لنظام حماية البيانات الشخصية ولسياسة حماية البيانات الشخصية الصادرة عن مكتب إدارة البيانات الوطنية.

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.

يستثنى من نطاق تطبيق هذه السياسة، جمع البيانات الشخصية من غير صاحبها مباشرة – دون علمه – أو معالجتها لغير الغرض الذي جمعت من أجله أو الإفصاح عنها دون موافقته أو نقلها خارج المملكة في الأحوال التالية:

- إذا كان جمع البيانات الشخصية أو معالجتها مطلوباً لتحقيق متطلبات نظامية وفقاً للأنظمة واللوائح والسياسات المعمول بها في المملكة أو لاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيه.
- إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

7. السياسة

1.7 متطلبات السياسة العامة

1.1.7 بناءً على استراتيجية وخطة إدارة البيانات وحوكمتها وحماية البيانات الشخصية، يجب وضع خطة لحماية البيانات الشخصية تلبي متطلبات حماية البيانات الشخصية التشغيلية والاستراتيجية وفقاً لسياسة حماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية، وعلى الخطة أن تشمل على خارطة طريق بالنشاطات والأهداف المرحلية لتحقيق والحفاظ على الامتثال الكامل لسياسة حماية البيانات الشخصية الصادرة عن مكتب إدارة البيانات الوطنية، وعلى الموارد والميزانية المطلوبة لتحقيق الامتثال الكامل لسياسة حماية البيانات الشخصية.

2.1.7 يجب تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته الضمنية أو الصريحة فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.

3.1.7 يجب أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.

4.1.7 يجب أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والاحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة، وإتلافها بطريقه آمنة تمنع التسرب أو الفقدان أو الاختلاس أو إساءة الاستخدام أو الوصول غير المصرح به نظاماً.

5.1.7 يجب أن تتضمن ضوابط الخصوصية وآلياتها الوسائل التقنية الملائمة والتي يجب تقييمها من قبل الجامعة.

6.1.7 يجب حماية البيانات الشخصية خلال مرحلة الحصول عليها ونقلها ومعالجتها والتخلص منها.

7.1.7 يجب أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية

8.1.7 يجب على الجامعة تحديد وتوثيق والموافقة على تخزين البيانات الشخصية وفقاً للأغراض التي جمعت لها والتي ستستخدم لها، وفي حال الحاجة لجمع البيانات فان يجب توضيح الأسباب التالية:

- الحاجة لجمع البيانات الشخصية وتصنيفها.

- احتياجات العمل والغرض من جمع كل فئة من البيانات الشخصية.
- مدة الاحتفاظ بالبيانات الشخصية.
- تفاصيل المستلمين الذين تم كشف البيانات الشخصية لهم أو سيتم الكشف عنها لهم.
- تفاصيل مصدر البيانات الشخصية إذا لم يتم جمع البيانات الشخصية من صاحب البيانات الشخصية مباشرةً.

9.1.7 يجب أن يتم الاحتفاظ بالبيانات بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

10.1.7 يجب عدم استخدام البيانات الشخصية لأغراض التدريب أو البحوث.

11.1.7 يجب مراجعة البيانات الشخصية بشكل دائم وحذفها حسب حاجة العمل أو انتهاء فترة الاحتفاظ بها.

12.1.7 على الجامعة أن يجري تقييماً مبدئياً لحماية البيانات الشخصية لتقييم بيئة حماية البيانات الشخصية القائمة. وينبغي للتقييم أن يشمل الآتي كحدٍ أدنى:

- تحديد أنواع البيانات الشخصية.
- موقع وطريقة تخزين البيانات الشخصية.
- المعالجة والاستخدامات الحالية للبيانات الشخصية.
- تحديات حماية البيانات الشخصية أمام الالتزام لسياسة حماية البيانات الشخصية الصادرة من مكتب إدارة البيانات الوطنية.

13.1.7 يجب استضافة البيانات حسب تنظيمات الهيئة الوطنية للأمن السيبراني لتكون داخل المملكة العربية السعودية إما في خوادم الجهة أو مقدمي الخدمات السحابية والاستضافة الوطنيين.

14.1.7 يجب على الجامعة تخزين ومعالجة البيانات الشخصية داخل المملكة العربية السعودية فقط وفرض ذلك على الأطراف الخارجية بتضمينه في بنود العقود أو الوثائق ذات العلاقة، وعندما يحتاج الجامعة إلى مشاركة البيانات الشخصية مع جهة آخرى خارج المملكة، فانه يجب الحصول على موافقة مكتب إدارة البيانات الوطنية.

15.1.7 على الجامعة أن يجري تدقيقاً داخلياً لمراقبة الامتثال لقواعد حماية البيانات الشخصية وتوثّق نتائجه في تقرير يُرفع إلى مسؤول حماية البيانات في الجامعة. وفي حالات عدم الامتثال، على الجهة أن تتخذ إجراءات تصحيحية مع إشعار الجهة التنظيمية ومكتب إدارة البيانات الوطنية وتوثيقها في تقرير نتائج التدقيق.

16.1.7 في حال قام الجامعة بإسناد مهام معالجة البيانات لطرف خارجي فيجب التحقق من امتثال الطرف الخارجي أو أي تعاقدات لاحقة قد يقوم بها الطرف الخارجي لمتطلبات الجامعة في حماية البيانات الشخصية.

17.1.7 على الجامعة أن يوثّق في سجل مجمّع سجلات تدقيق الامتثال لفترة زمنية معقولة لا تقل عن 24 شهرًا، وأن تتيحه عند الطلب إلى مكتب إدارة البيانات الوطنية وفقاً لسياسة حماية البيانات الشخصية الصادرة عن مكتب إدارة البيانات الوطنية ويجب أن يحتوي كحدٍ أدنى على سجل بكل عملية جمع أو معالجة لأي بيانات شخصية.

18.1.7 يجب متابعة أي تغييرات أو تحديثات فيما يتعلق بالأنظمة والقوانين واللوائح المعمول بها لتعكسها على سياسة حماية البيانات الشخصية.

2.7 حماية البيانات الشخصية

1.2.7 يجب التأكد من القدرة على استعادة توافر البيانات الشخصية والوصول إليها في الوقت المناسب في حالة وقوع حادث مادي أو تقني.

2.2.7 يجب استخدام تقنيات إخفاء وتعتيم البيانات لحماية البيانات الشخصية.

3.2.7 يجب على الجامعة اختبار وتقييم فعالية الإجراءات الفنية والتنظيمية لضمان أمن معالجة البيانات الشخصية.

4.2.7 يجب إجراء تقييماً سنوياً لمخاطر تشغيل واستخدام أنظمة المعلومات التي تحتوي معلومات شخصية، ويشمل ذلك جمع ومعالجة البيانات الشخصية وتخزينها ونقلها في كل نظام، سواءً كان ذلك يتم يدوياً أو آلياً، ويجب أن تخضع نتائج تقييم المخاطر لما يلي كحدٍ أدنى:

- التوثيق
- تحليل التأثير واحتمالات الوقوع
- التقييم على أساس الالتزامات التنظيمية وأهمية حلها

5.2.7 يجب أن تكون البيانات الشخصية كافية وذات صلة ومحدودة بما هو ضروري للأغراض التي تتم معالجتها من أجلها.

6.2.7 يجب أن تكون البيانات الشخصية دقيقة ومناسبة ومحدّثة، ويجب اتخاذ التدابير المناسبة لضمان محو أو تصحيح البيانات الشخصية غير الدقيقة المتعلقة بالأغراض دون تأخير.

7.2.7 إذا تم الحصول على البيانات الشخصية من مصادر أخرى غير صاحب البيانات الشخصية، فيجب إبلاغ صاحب البيانات الشخصية، كما يجب على الجامعة إرسال إشعار خصوصية إليه/إليها أيضاً.

8.2.7 يجب تنفيذ ضوابط أمنية مناسبة لحماية البيانات الشخصية التسرب أو التلف أو الفقدان أو الاختلاس أو إساءة الاستخدام أو التعديل أو الوصول غير المصرح به – وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

9.2.7 يجب أن يتم استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات أمن المعلومات في الجامعة لضمان حماية البيانات الشخصية ومنها ما يلي:

10.2.7 منح صلاحيات الوصول إلى البيانات وفقاً لمهام العاملين بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤوليات.

11.2.7 تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفر إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).

12.2.7 توقيع العاملين الذين يباشرون عمليات معالجة البيانات على تعهد للمحافظة على البيانات وعدم الإفصاح عنها إلا وفقاً لسياسات وإجراءات الجامعة والأنظمة والتشريعات ذات العلاقة

13.2.7 اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية وفقاً لطبيعة وحساسية البيانات وسياسة الوصول المعتمدة من قبل الجامعة.

3.7 حقوق أصحاب البيانات الشخصية

1.3.7 يجب على الجامعة إشعار صاحب البيانات بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية والغرض من ذلك، وألا تعالج بياناته بصورة تتنافى مع الغرض من جمعها والذي من أجله قدم موافقته الضمنية أو الصريحة.

2.3.7 يحق لصاحب البيانات الرجوع عن موافقته في معالجة بياناته الشخصية في أي وقت مالم يكن هناك أغراض مشروعة تتطلب عكس ذلك

3.3.7 يحق لصاحب البيانات الوصول إلى بياناته الشخصية وذلك للاطلاع عليها وطلب تصحيحها أو إتمامها أو تحديثها وطلب إتلاف ما انتهت الحاجة إليه منها والحصول على نسخة منها بصورة واضحة.

4.3.7 يجب أن يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.

4.7 مبدأ الخصوصية في التصميم

1.4.7 يجب أن يتبنى الجامعة مبدأ الخصوصية في التصميم وتضمن تلبية متطلبات الخصوصية على الأنظمة والبرامج الحالية أو الجديدة والتي تجمع البيانات الشخصية أو تعالجها.

2.4.7 يجب على الجامعة أن يجري بانتظام تقييماً لتأثير الخصوصية على جميع الأنظمة التي تجمع البيانات الشخصية أو تعالجها. يشمل هذا التقييم ما يلي:

- تطبيق مبادئ حماية البيانات الشخصية.
- الوفاء بمسؤوليات وحدة التحكم.
- تطبيق ضوابط أمنية لحماية المعلومات الشخصية.
- التأكد من أن الأساس القانوني لمعالجة البيانات الشخصية
- ضمان جمع البيانات الشخصية أو استخدامها أو معالجتها أو تخزينها أو مشاركتها وفقاً للأغراض المصرح بها والتي تم تحديدها في إشعار الخصوصية
- اعتماد مبدأ الخصوصية في التصميم لجميع الأنظمة والعمليات الجديدة أو المتغيرة.

3.4.7 يجب على الجامعة تطبيق تقنيات مناسبة لإخفاء الهوية للبيانات والتشفير لحماية البيانات الشخصية.

4.4.7 يجب على الجامعة استيفاء متطلبات التوثيق التالية وإتاحة إمكانية الوصول إليها من خلال مواضيع البيانات فيما يتعلق بأنشطة المعالجة على البيانات الشخصية:

- أهداف معالجة البيانات الشخصية.
- أنشطة المعالجة التي أجريت على البيانات الشخصية.
- معالجة فئات البيانات الشخصية.
- اتفاقيات وآليات نقل البيانات الشخصية من وإلى المنظمات الأخرى بعد الحصول على موافقة أو طلب صاحب البيانات الشخصية.
- جداول الاحتفاظ بالمعلومات الشخصية.
- الضوابط الأمنية الموجودة لحماية المعلومات الشخصية.

5.7 نقل المعلومات الشخصية

1.5.7 يجب أن يستند أي نقل للبيانات الشخصية إلى موافقة أو طلب صاحب المعلومات الشخصية.

2.5.7 قبل نقل البيانات الشخصية خارج الجامعة، يجب تنفيذ تحليل تأثير الخصوصية.

3.5.7 يجب إرسال إشعار مناسب إلى صاحب المعلومات الشخصية بما في ذلك المستلمين الذين سيتم نقل البيانات الشخصية إليهم، بما في ذلك: التاريخ والطبيعة والغرض من كل إفشاء للسجل؛ واسم وعنوان المستلمين الذين تم الإفصاح لهم.

4.5.7 يجب التأكد من اجراءات حماية البيانات الشخصية في الطرف المستقبل؛ وهذا يتضمن الآتي:

- اسم المنظمة والتفاصيل ذات الصلة.
- أهداف معالجة البيانات الشخصية.
- فئات الأفراد ومعالجة البيانات الشخصية.
- فئات متلقي البيانات الشخصية.
- اتفاقات وآليات نقل البيانات الشخصية.

- جداول الاحتفاظ بالمعلومات الشخصية.
- الضوابط الفنية والتنظيمية ذات الصلة المعمول بها في الجامعة.

6.7 إشعار الخصوصية

1.6.7 يجب على الجامعة أن يحدد ويوثق ويوافق وينفذ المتطلبات لتقديم إشعار الخصوصية لصاحب البيانات الشخصية فيما يتعلق بما يلي:

2.6.7 أنشطته التي تؤثر على خصوصية البيانات الشخصية، بما في ذلك جمعها واستخدامها ومشاركتها والحفاظ عليها والتخلص منها.

3.6.7 كيفية استخدام الجامعة للبيانات الشخصية وعواقب ممارسة أو عدم ممارسة تلك الخيارات.

4.6.7 الحق في الوصول وتعديل البيانات الشخصية أو تصحيحها إذا لزم الأمر.

5.6.7 نوع البيانات الشخصية التي يجمعها الجامعة والغرض الذي تجمع من أجله تلك المعلومات.

6.6.7 طرق استخدام الجامعة للبيانات الشخصية.

7.6.7 إذا كان الجامعة يشارك البيانات الشخصية مع كيانات خارجية، وفئات تلك الكيانات، وأغراض هذه المشاركة.

8.6.7 كيف يمكن للأفراد الوصول أو الحصول على البيانات الشخصية.

9.6.7 كيفية حماية البيانات الشخصية.

10.6.7 الفترة التي سيتم تخزين البيانات الشخصية لها.

11.6.7 أحقية الطلب من المتحكم الوصول إلى البيانات الشخصية وتصحيحها أو محوها أو تقييد المعالجة المتعلقة بصاحب البيانات الشخصية وكذلك الاعتراض على معالجتها والحق في نقل البيانات.

12.6.7 أحقية سحب الموافقة في أي وقت.

13.6.7 أحقية تقديم شكوى أو أسئلة أو مخاوف إلى الجامعة، وتقديم شكوى إلى السلطة الإشرافية.

14.6.7 سواء كان توفير البيانات الشخصية مطلوبًا قانونيًا أو شرطاً ضرورياً لإبرام عقد، وكان صاحب البيانات الشخصية ملزماً بتقديم البيانات الشخصية وتم إشعاره بالعواقب المحتملة لعدم تقديم هذه البيانات.

15.6.7 التغييرات في الممارسات أو السياسات التي تؤثر على البيانات الشخصية أو التغييرات في أنشطتها التي تؤثر على الخصوصية، قبل أو في أقرب وقت ممكن بعد التغيير.

16.6.7 يجب على الجامعة إبلاغ صاحب البيانات الشخصية قبل رفع قيود المعالجة إذا كانت المعالجة مقيدة بواسطة صاحب البيانات. كما يجب معالجة البيانات الشخصية باستثناء التخزين بموافقة صاحب البيانات فقط.

17.6.7 يجب على الجامعة الإبلاغ عن أي تصحيح أو محو للبيانات الشخصية أو تقييد المعالجة لكل مستلم تم الكشف عن بياناته الشخصية، وأن يقوم المراقب بإبلاغ صاحب البيانات الشخصية لمن تمت مشاركة بياناته معهم إذا طلب هو ذلك.

7.7 انتهاك الخصوصية

1.7.7 يجب أن يقوم الجامعة بتطوير وتوثيق والموافقة على خطة الاستجابة لحوادث الخصوصية وتنفيذها عند الحاجة.

2.7.7 على الجامعة أن يقوم بإعداد وتوثيق الاجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والجامعة حسب التسلسل الإداري بناء على قياس شدة الأثر.

3.7.7 إذا حدث انتهاك على لخصوصية البيانات الشخصية، فيجب على الجامعة اتباع خطة الاستجابة وإجراءات الاستجابة كما يجب إبلاغ إدارة الأمن السيبراني.

4.7.7 يجب على الجامعة أن يقوم بتطوير وتوثيق وتنفيذ والموافقة على الإجراء الخاص بإبلاغ أصحاب البيانات الشخصية عن انتهاك خصوصية البيانات الشخصية دون تأخير.

5.7.7 على الجامعة أن يخطر السلطة التنظيمية في حال تسريب البيانات الشخصية، في الإطار الزمني المقرر في سياسة حماية البيانات الشخصية الصادرة عن مكتب إدارة البيانات الوطنية؛ علمًا بأن الإطار الزمني المحدد للإبلاغ هو 72 ساعة.

6.7.7 على الجامعة أن يوثق عملية إدارة التعامل مع تسريب البيانات من أجل الإدارة الفورية ومعالجة انتهاكات حماية البيانات الشخصية ولتحديد وظائف ومسؤوليات فريق العمل المعني، وعلى عملية إدارة التعامل مع التسريب أن تشمل ما يلي كحد أدنى:

- إجراء مراجعة للحادثة
- صياغة استجابة فورية للحادثة
- تنفيذ الإجراء الإصلاحي الدائم
- إجراء اختبارات على الإجراءات التصحيحية للتحقق من كفاءة حلول حماية البيانات الشخصية

8.7 التوعية والتدريب

1.8.7 يجب أن يقوم الجامعة بتطوير برنامج تدريب وتوعية شامل، وتوثيقه والموافقة عليه وتنفيذه وتحديثه بانتظام بهدف التأكد من معرفة العاملين بمسؤوليات وإجراءات الخصوصية، مثل إدارة التدريب على الخصوصية الأساسي؛ والتدريب على الخصوصية المستهدفة القائمة على أدوار العاملين الذين يتحملون مسؤولية البيانات الشخصية أو الأنشطة التي تتضمن البيانات الشخصية.

2.8.7 يجب أن يشمل برنامج التدريب على التالي كحدٍ أدنى:

- أهمية حماية البيانات الشخصية وتأثيراتها وعواقبها على الجهة و/أو صاحب البيانات.
- تعريف البيانات الشخصية.
- حقوق صاحب البيانات.
- مسؤوليات الجهة وصاحب البيانات.
- الإشعارات: متى يجب إشعار الجهة أو صاحب البيانات، وكيفية التعامل مع طلبات جمع البيانات الشخصية ومعالجتها ومشاركتها.

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 والتوجهات 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 مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

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

يجب على مديردائرة الشؤون القانونية:

8.1.8 تحديد القوانين والتنظيمات التي تنطبق على الجامعة.

9.1.8 تنفيذ الجزئية الخاصة بالشؤون القانونية فيما يتعلق بخصوصية البيانات.

10.1.8 تحديد متطلبات الخصوصية في العقود وتعهد المحافظة على السرية بالاتفاق مع عمادة الموارد البشرية.

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

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

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

يتحمل مستخدمي أصول الجامعة المعلوماتية والتقنية مسؤولية الالتزام بهذه السياسة بالإضافة إلى الإبلاغ عن أي حادثة أمنية أوعدم الالتزام بهذه السياسة إلى إدارة 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 في حال حدوث تغييرات كبيرة في السياسات أو الإجراءات التنظيمية للجامعة أو المتطلبات التشريعية والتنظيمية ذات العلاقة 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.V.2.0- السياسة العامة للأمن السيبراني وحوكمة البيانات
- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- DICT.I.06-04.CS.A. V2.0- سياسة إدارة الأصول
- DICT.I.06-03.CS.A. V2.0- سياسة حماية البيانات
- 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.06-83.CS.A.V2.0- معايير أجهزة نقل البيانات في اتجاه واحد
- DICT.I.06-62.CS.A.V2.0- معايير إدارة الأصول
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.04-35.CS.A.V2.0- إجراءات إدارة النسخ الاحتياطي

13. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية	النظام الأوروبي العام لحماية البيانات
حماية البيانات والمعلومات	3-7-2	-	-	-	-	A.18.1.4	Appendix J	Article 5 to 46

----------نهاية الوثيقة----------