جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة الاستخدام المقبول للأصول

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-27.CS.A. V2.0

جامعة الإمام عبد الرحمن 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 الاستخدام المقبول للأصول	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/16	إنشاء
V1.1	د. سامر بني عواد	2022/02/05	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/27	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 المعلومات والأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني بتطوير وإنشاء وتنظيم العمليات الأمنية المطلوبة لحماية الأصول المعلوماتية والتقنية وتحدد هذه الوثيقة سياسة استخدام الأصول المقبولة في الجامعة والمتطلبات الأمنية بناءً على أفضل الممارسات العالمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

5. الهدف

الغرض من هذه السياسة هو تحديد الاستخدام المقبول للأصول مثل المعدات والبرمجيات والشبكات والمعلومات وأنظمة الاتصالات المشغّلة من قبل الجامعة وتوعية جميع العاملين والمتعاقدين ومن له صلاحية الوصول إلى أنظمة الجامعة بمسؤولياتهم وواجباتهم فيما يتعلق باستخدام أصول وخدمات نظم المعلومات. القصد من هذه السياسة هو حماية المعلومات والأصول الكامنة في البنية الأساسية لتقنية المعلومات والوثائق الأخرى من خلال التحكم باستخدام نظم المعلومات والمعلومات على مستوى مقبول يتناسب مع متطلبات العمل والأمن في 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 التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات في الجامعة بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

2.1.7 يجب على جميع العاملين والمتعاقدين والأطراف الخارجية عدم محاولة الوصول إلى البيانات والوثائق الإلكترونية والبريد الالكتروني والبرامج الكامنة في نظم تقنية المعلومات في الجامعة أو أي أصول ورقية من غير تصريح.

3.1.7 يجب أن يعي جميع العاملين أن أي بيانات مخزنة في أنظمة الجامعة هي مملوكة للجامعة وعلى ذلك فإن أي عملية نقل لهذه المعلومات يترتب عليها تحقيق واتخاذ الاجراءات اللازمة لذلك.

4.1.7 يجب على جميع العاملين عدم الإفصاح عن أي معلومات متعلقة بالمنظمة أو العمل للأشخاص غير المصرح لهم بذلك خارجياً أو داخلياً.

5.1.7 يجب على مديري الأنظمة والأشخاص المصرح لهم عدم الإفصاح عن أي تفاصيل متعلقة بالأنظمة والشبكات بما في ذلك الوصول إلى أو الاتصال عن بعد بموارد تقنية المعلومات في الجامعة إلى أي أشخاص غير مصرح لهم بذلك.

6.1.7 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

7.1.7 يجب على جميع العاملين استخدام نظم وأصول تقنية المعلومات المسندة إليهم بعناية وحرص وستكون سلامة هذه النظم والأصول مسؤوليتهم.

8.1.7 يجب على العاملين والمتعاقدين والأطراف الأخرى عدم نسخ المستندات محفوظة الحقوق أو البرمجيات والمعلومات المملوكة من قبل الجامعة.

9.1.7 يجب على جميع العاملين والمتعاقدين عدم تنصيب البرمجيات غير النظامية (مثل البرمجيات المجانية / المشتركة) بدون موافقة واعتماده من قبل عمادة الاتصالات وتقنية المعلومات.

10.1.7 على جميع العاملين عدم المشاركة في الأنشطة التي قد تؤثر سلباً على كفاءة وفعالية موارد تقنية المعلومات الخاصة بالمنظمة. بالإضافة إلى الامتناع عن القيام بأنشطة قد تؤدي إلى الغاء الصلاحيات.

11.1.7 يجب على العاملين اتخاذ الخطوات الكافية والمناسبة لضمان تفادي الدخول غير المصرح به إلى معلومات الجامعة (مثل: منع الكشف عن المعلومات).

12.1.7 يجب عدم استخدام موارد معلومات الجامعة لمنفعة شخصية، أو نشاط سياسي، أو إعلان لم يتقدم الجامعة بطلبه، أو لجمع تبرعات من غير تصريح مسبق، أو للحصول على عروض في أي نشاط محظور من قبل الجامعة أو قوانين ولوائح المملكة العربية السعودية.

13.1.7 لا يسمح لجميع العاملين والمتعاقدين الخارجيين ربط أجهزتهم الشخصية/المتنقلة بشبكة الجامعة.

14.1.7 يجب حماية جميع النسخ الورقية للمستندات التي تحتوي على معلومات مصنفة بشكل يتناسب مع ضوابط تصنيف المعلومات وفقاً لسياسة تصنيف البيانات.

15.1.7 يسمح باستخدام الوصول إلى شبكة الإنترنت لأغراض العمل فقط. كما يمنع استخدام الوصول إلى شبكة الإنترنت الخاصة بالجامعة لمنافع شخصية أو للترفيه في شبكات التواصل الاجتماعي أو على مواقع الإنترنت والمرئيات (مثل: يوتيوب، فيسبوك، توتير أو أي مواقع أخرى).

16.1.7 يجب عدم نشر أي معلومات مصنفة خاصة بالجامعة على شبكات التواصل الاجتماعي (مثل: واتساب، فيسبوك، توتير، لينكد أن وما إلى ذلك).

17.1.7 يجب عدم استخدام أنظمة الجامعة وشبكته ومقره للدخول إلى المواقع غير المتعلقة بالعمل مثل حسابات البريد الإلكتروني العامة، وبوابات الإنترنت، والمواقع التي تتضمن مواد غير قانونية.

18.1.7 أي وصول إلى الإنترنت داخل الجامعة يجب أن يتم من خلال وسيط/جدران حماية الإنترنت ولا يجب تجاوزه من قبل المستخدمين.

19.1.7 يجب على العاملين عدم تحميل، أو تثبيت، أو تنفيذ أي برامج، أو خدمات حماية (مثل: الشبكات الخاصة الافتراضية، وكاسر كلمات المرور، وحزمة التنصت، وبرامج ماسحات المنافذ، وما إلى ذلك) التي قد تكشف أو تعرض مواطن الضعف في الموارد التقنية إلى الاستغلال ما لم يتم الموافقة على ذلك من قبل إدارة الأمن السيبراني.

20.1.7 يجب فحص أي برنامج آلياً من أجل الكشف عن الفيروسات والبرمجيات الخبيثة بعد الحصول على إذن بتحميله وقبل تنزيله على الجهاز.

21.1.7 يجب أن يتاح الوصول إلى الإنترنت من خلال متصفح إنترنت آمن وملائم.

22.1.7 يمنع نقل المعلومات السرية من خلال الإنترنت عبر الوسائل غير المصرح بها بدون موافقة من مدير الأمن السيبراني لتأمين الضوابط الأمنية اللازمة.

23.1.7 يجب على الجامعة مراقبة أنظمته والبنية التحتية للشبكة للكشف عن الأنشطة الخبيثة أو التسريب العرضي للمعلومات المصنفة.

24.1.7 لا يسمح باستخدام موارد الجامعة للأغراض الشخصية بما في ذلك تخزين البيانات الشخصية. كما أن الجامعة لا يضمن خصوصية المعلومات الشخصية المخزنة على أي من أصوله المستخدمة خصيصاً لأغراض العمل.

25.1.7 يمنع مشاركة بيانات حساب المستخدم (كلمة المرور) مع الآخرين ويتحمل المستخدم كامل المسؤولية وقد يؤدي ذلك إلى اتخاذ الإجراءات التأديبية.

26.1.7 يجب استخدام الحاسب المحمول أو الجامعي وأي أنظمة معلومات أخرى تابعة للجامعة بطريقة تحافظ على سريتها وتحمي المعلومات المخزنة فيها.

27.1.7 لا يسمح للمستخدمين بتعطيل أي خدمة أو جهاز حماية أو برامج الحماية من الفيروسات الموجودة على أي من موارد تقنية المعلومات في الجامعة.

28.1.7 يجب عدم نسخ أو نقل أي معلومات صنفت على أنها مقيدة أو سرية بأي طريقة ومنها على سبيل المثال لا الحصر، الأقراص المدمجة والمحمولة، ومرفقات البريد الإلكتروني وما إلى ذلك، إلا وفقاً للضوابط التي تحددها إدارة الأمن السيبراني.

29.1.7 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

30.1.7 لا يسمح باستخدام الوسائط المحمولة لتخزين أو نقل بيانات أو معلومات الجامعة إلا لحاجة العمل بعد أخذ تصريح مسبق من إدارة الأمن السيبراني موضحاً فيه سبب الاستخدام، ومع مراعاة استخدام وسائط تخزين محمولة مشفرة ومحمية.

31.1.7 تحتفظ إدارة الأمن السيبراني بحق مراقبة ومراجعة حسابات الأشخاص، والشبكات، والأنظمة، والبنية التحتية بشكل دوري وذلك لتحديد الامتثال لهذه السياسة.

32.1.7 يمنع على أي من المستخدمين المشاركة في أنشطة غير قانونية مثل الوصول إلى أصول غير مصرح بها، والاختراق، وتعرض أجهزة الحاسوب إلى ملوثات أو فيروسات أو ارتكاب أي عمل قد يعطل استخدام الأصول.

33.1.7 يجب إبلاغ عمادة الاتصالات وتقنية المعلومات على الفور عن أي ضرر بالمعدات المملوكة من قبل الجامعة أو في حال ضياعها أو سرقتها.

34.1.7 يجب على جميع العاملين عدم السماح للأشخاص غير المصرح لهم بالدخول إلى المناطق المقيدة في الجامعة.

35.1.7 يمنع التقاط الصور أو تصوير مقاطع الفيديو في داخل الجامعة.

36.1.7 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

37.1.7 يجب ارتداء البطاقة التعريفية في جميع مرافق الجامعة.

38.1.7 يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها وفي حال الاشتباه بوجود أخطار سيبرانية.

2.7 حماية أجهزة المستخدمين

1.2.7 يجب على جميع المستخدمين التأكد من تسجيل خروجهم من أنظمة المعلومات قبل مغادرة الجامعة في نهاية ساعات العمل. كما يجب قفل النظام خلال فترة الاستراحة القصيرة المخصصة لهم وذلك قبل مغادرة محطة العمل الخاصة بهم.

2.2.7 على جميع المستخدمين عدم ترك أي معلومات سرية على مكاتبهم بحيث يمكن قراءتها أو نسخها أو التلاعب بها دون علمهم. يجب تأمين هذه المعلومات وتخزينها في خزانات الحفظ أو إتلافها بشكل آمن، مثل استخدام آلة تمزيق الورق.

3.2.7 يجب على جميع المستخدمين التأكد من حماية شاشة التوقف بكلمة مرور. كما يجب على عمادة الاتصالات وتقنية المعلومات تعيين شاشة توقف محمية بكلمة مرور بحيث تفعل بعد مرور 5 دقائق على عدم استخدام الجهاز.

4.2.7 يجب على المستخدمين التأكد من تثبيت شاشات حماية لدعم الخصوصية لكافة المستخدمين في الجامعة.

5.2.7 يجب على جميع المستخدمين عدم تثبيت معدات جديدة على أجهزة الحاسب المحمولة أو الجامعية إلا بإذن من عمادة الاتصالات وتقنية المعلومات.

6.2.7 يجب على جميع المستخدمين التأكد من عدم وجود برمجيات مقرصنة/غير قانونية مثبتة على أجهزة الحاسب المحمول أو الجامعي. كما يسمح فقط بتثبيت البرمجيات الموافق عليها والمصرح بها.

7.2.7 يسمح للمستخدمين باستخدام المعدات المصرح بها والمملوكة من قبل الجامعة فقط.

8.2.7 لا يسمح باستخدام برمجيات الألعاب على أي من أنظمة الجامعة ولا يسمح بتثبيتها أو نقلها في شبكة الجامعة.

9.2.7 يجب التحكم بجميع الصلاحيات العالية (Admin Privileges) بطريقة آمنة على جميع أجهزة الجامعة ولا يجب تعيينها للاستخدام من قبل أي مستخدم عادي في الجامعة.

3.7 الاستخدام المقبول للإنترنت والبرمجيات

1.3.7 يجب استخدام الإنترنت لأغراض العمل فقط.

2.3.7 يجب على المستخدم عدم تنزيل الوسائط غير المتعلقة بمجال العمل مثل:

- برمجيات الند بالند (Peer to Peer) وبرمجيات مشاركة الملفات عبر الإنترنت
- الأفلام، والألعاب، والموسيقى، والبرمجيات، والبرامج النصية، وما إلى ذلك.

3.3.7 يجب أن يحصل العاملين الفنيين أو المتعاقدين أو الأطراف الأخرى التي تقوم بحل المشاكل التقنية وتنفيذ العمليات على تصريح من قبل إدارة الأمن السيبراني قبل تثبيت واستخدام البرمجيات في أجهزة العمل مثل برامج المراسلة الفورية أو برامج التحكم بالوصول إلى البيانات.

4.3.7 على المستخدمين اشعار عمادة الاتصالات وتقنية المعلومات عند الاشتباه برسائل التحذيرات الأمنية التي قد تظهر خلال الاستخدام.

5.3.7 يمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

6.3.7 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

7.3.7 يمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول الجامعة دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

8.3.7 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات الجامعة وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية بما في ذلك على سبيل المثال لا الحصر، فحص المنافذ، واستقصاء المعلومات من الشبكة والخداع، والمسح الأمني، ومراقبة الشبكة دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

9.3.7 لا يسمح لمستخدمي الإنترنت بزيارة صفحات تتعلق بالاختراق، أو التصيد، أو شبكات الند للند، أو الوسيط، كما يجب تجنب الخدمات وأي مواقع خبيثة معروفة ومثل هذه المواقع يجب حجبها من قبل الجامعة.

4.7 الاستخدام المقبول للبريد الإلكتروني

1.4.7 نظام البريد الإلكتروني متاح بصفة أساسية للاستخدام المتعلق بالعمل فقط. يجب استخدام البريد الإلكتروني بمسؤولية وفقاً لسياسة أمن البريد الإلكتروني.

2.4.7 لا يسمح بتداول رسائل البريد الإلكتروني ذات المحتوى غير اللائق أو غير مقبول باستخدام البريد الإلكتروني الخاص بالجامعة سواء كان ذلك داخلياً أو لمستقبلين آخرين من خارج الجامعة.

3.4.7 يجب على جميع المستخدمين إبلاغ إدارة الأمن السيبراني عن أي رسائل بريد اقتحاميه أو خبيثة.

4.4.7 يجب أن تتم جميع المراسلات البريدية في نطاق الشبكة المغلقة والمصرح بها في الجامعة.

5.4.7 يحق للجامعة أن يطلع على أو يكشف عن أي تواصل بريدي بناءً على طلب محدد وبعد أخذ التصريح اللازم من صاحب الصلاحية بالجامعة وإدارة الأمن السيبراني ووفقاً للقرارات التنظيمية والتشريعية ذات العلاقة (مثل: قرار ضوابط استخدام الحاسبات الآلية وشبكات المعلومات في الجهات الحكومية، الصادر من مجلس الوزراء بالمملكة العربية السعودية رقم (555) وتاريخ 23/9/1440هـ).

6.4.7 لا يسمح باستخدام أنظمة الجامعة لإنتاج أو توزيع رسائل بريد إلكتروني متسلسلة.

7.4.7 يمنع تداول رسائل البريد الإلكتروني التحذيرية فيما يخص أخطار الأمن السيبراني إلا من الجهة المعنية فقط وهي إدارة الأمن السيبراني أو إرسال رسالة إنذار عاجل عن فيروس غير موجود.

8.4.7 على عمادة الاتصالات وتقنية المعلومات التأكد من أن جميع رسائل البريد الإلكتروني الواردة داخل أو خارج الجامعة تتضمن إخلاء مسؤولية الجامعة.

9.4.7 يجب على جميع المستخدمين عدم فتح أي بريد إلكتروني مشبوه، أو رابط، أو ملف مرفق، أو أي بريد إلكتروني ليس من المتوقع استلامه حتى وإن كان من مصدر موثوق.

10.4.7 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة الجامعة أو أصولها.

11.4.7 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بالجامعة في أي موقع ليس له علاقة بالعمل.

12.4.7 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

5.7 الاتصالات القائمة والاجتماعات المرئية على شبكة الإنترنت

1.5.7 يجب أن يتأكد جميع المستخدمين من استخدام المعدات المصرح بها من الجامعة لإجراء اتصالاتهم القائمة على شبكة الإنترنت وعقد الاجتماعات المرئية.

2.5.7 يجب إجراء الاتصالات القائمة على شبكة الإنترنت ومؤتمرات الفيديو لأغراض العمل فقط.

3.5.7 يجب مراعاة الضوابط الأمنية لأمن الاجتماعات الحضورية والافتراضية.

6.7 استخدام كلمة المرور

1.6.7 يجب على جميع مستخدمي نظام المعلومات في الجامعة تحمل مسؤولية الاختيار والحفاظ على كلمة مرور آمنة بناءً على سياسة كلمة المرور في الجامعة.

2.6.7 لا يسمح لمستخدمي نظام المعلومات في الجامعة كتابة كلمة المرور الخاصة بهم في رسائل البريد الإلكتروني أو في المراسلات الإلكترونية.

3.6.7 لا يسمح باستخدام نظام المعلومات في الجامعة للأغراض التالية:

- الكشف عن كلمة المرور عبر الهاتف لأي شخص.
- الكشف عن كلمة المرور لأي شخص حتى وإن كان العميد أو فرد من العائلة أو زملاء العمل أو مدراءهم.
- الكشف عن كلمة المرور عبر الإنترنت
- كتابة كلمة المرور على ورق او هاتف

- كتابة كملة المرور أمام أي شخص آخر.

4.6.7 يتحمل مستخدمي نظام المعلومات في الجامعة مسؤولية أي نشاط متعلق بحقوق الوصول الخاصة بهم.

5.6.7 لا لا يسمح لمستخدمي نظام المعلومات في الجامعة بالحصول على أو امتلاك أي كلمة مرور أو مفاتيح فك الشفرات أو الوصول إلى آليات المراقبة والتي قد تؤدي إلى وصول غير مصرح به. المستخدمين معرضين للمساءلة في حال تم ارتكاب أي أنشطة من خلال حساباتهم.

6.6.7 يجب أن يقوم مستخدمي نظام المعلومات في الجامعة باختيار كلمات مرور مختلفة لحساباتهم في الجامعة عن باقي حساباتهم الشخصية مثل حسابات التواصل الاجتماعي وحسابات البريد الشخصية (مثل ياهو، جيميل، هوتميل وما إلى ذلك).

7.6.7 على المستخدم القيام بتغيير كلمة المرور فوراً بعد استلام كلمة المرور المؤقتة من قبل مسؤول النظام.

8. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني القيام بالآتي:

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 متعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة المقبولة لاستخدام الأصول 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.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- ❖ DICT.I.06-44.CS.A. V2.0- سياسة أمن البريد الإلكتروني
- ❖ DICT.I.06-15.CS.A. V2.0- سياسة كلمة المرور
- ❖ DICT.I.06-69.CS.A.V2.0- معايير كلمة المرور
- ❖ DICT.I.06-49.CS.A.V2.0- معايير إدارة هويات الدخول والصلاحيات
- ❖ DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول

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
السياسة المقبولة لاستخدام الأصول	3-1-2	-	-	-	-	A.7.1.3	AC-20, PL-4, PS-6
استخدام معلومات المصادقة السرية	2-2-3	-	-	-	-	A.9.3.1	IA-5(1), IA-5(4), IA-2
التبادل الإلكتروني للرسائل	2-4	-	-	-	-	A.10.8.4	AU-10, SC-7, SC-8, SC-44

----------نهاية الوثيقة----------