جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة المكتب النظيف والشاشة الخالية

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-26.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 المكتب النظيف والشاشة الخالية	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	2023/12/26	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 التقنية أو في أي من المستندات المطبوعة أو وسائط التخزين القابلة للإزالة، والحفاظ على مكاتب آمنه في جميع مرافق الجامعة للحد من أخطار الوصول غير المصرح به وفقدان المعلومات وإحداث الضرر بها أثناء ساعات العمل وخارجها.

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

5. الهدف

الهدف من هذه السياسة هو تزويد جميع العاملين في الجامعة بالوعي اللازم بشأن سياسة الجامعة النظيف والشاشة الخالية لحماية أصول الجامعة المعلوماتية والتقنية.

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 الجامعة النظيف

1.1.7 يجب على العاملين التأكد من تخزين المستندات والورق ووسائط الحاسب الآلي في خزائن مؤمنة مناسبة و/أو أي أشكال أخرى من الخزائن الآمنة أو ما يماثلها في حالة عدم استخدامها، خاصةً خارج ساعات العمل.

2.1.7 يجب أن تبقى جميع المكاتب نظيفة ومرتبة وخالية من أصول الجامعة التي تحتوي على بيانات شخصية أو معلومات مصنفة بتصنيف مقيّد فأعلى.

3.1.7 في حالة عدم توفر الخزانات القابلة للقفل وخزانات حفظ الملفات والأدراج والخزائن وما إلى ذلك، يتم تأمين أبواب المكاتب/الغرف إذا تركت دون رقابة.

4.1.7 يجب أن تكون معلومات العمل السرية والمقيدة مؤمنة في خزائن آمنة عند عدم الحاجة إليها.

5.1.7 يجب التخلص من البيانات الشخصية والسرية والمقيدة عند طباعتها، من الطابعات وآلات النسخ والماسحات الضوئية وأجهزة الفاكس فور الانتهاء من النشاط، وفي حالة لم تعد هذه المعلومات مطلوبة يجب تقطيعها بآلة تمزيق الورق.

6.1.7 يُمنع تثبيت المعلومات/الملاحظات السرية والهامة أو البيانات الشخصية أمام الجامعة أو على لوحة الإعلانات.

7.1.7 يجب المحافظة على سرية كلمات المرور وعدم كتابتها على الوسائط مثل الأوراق والملاحظات اللاصقة.

8.1.7 يجب على المستخدمين الذين يستخدمون طابعات وماسحات ضوئية وآلات تصوير وأجهزة فاكس/تيليكس وآلات تمزيق ورق مشتركة أو خاصة أن يضمنوا آليات الحماية الكافية لتجنب الوصول غير المصرح به.

9.1.7 يجب على جميع العاملين التأكد من خلو مساحة العمل/الجامعة من المواد المطبوعة/الوثائق في حالة عدم استخدامها.

10.1.7 يجب على العاملين الذين يستخدمون أنظمة الحاسب الآلي التأكد من أن المعلومات الموجودة على الشاشة غير متاحة للعرض بسهولة لعاملين آخرين، ويجب ألا يتم الاحتفاظ بها بطريقة تمكن المستخدمين غير المصرح لهم من القيام باختلاس النظر أو إلقاء نظرة سريعة على شاشة نظام الحاسب الآلي لشخص ما.

11.1.7 على جميع العاملين المسؤولين عن الاجتماعات أن يضمنوا عدم ترك أي بيانات شخصية أو معلومات سرية في الجامعة، سواءً على الطاولة أو اللوحات الورقية أو السبورات البيضاء، إلخ.

2.7 متطلبات الشاشة الخالية

1.2.7 يجب تثبيت شاشات حماية لدعم الخصوصية لكافة المستخدمين في الجامعة.

2.2.7 يجب أن تكون جميع أنظمة الحاسب الآلي محمية بكلمات المرور أو شاشات التوقف أو أدوات التحكم المماثلة عندما لا تكون قيد الاستخدام أو غير نشطة لمدة خمس (5) دقائق.

3.2.7 يجب على المستخدمين تأمين أنظمة الحاسب الآلي الخاصة بهم يدوياً عند عدم استخدامها أو عندما يغادرون مكان عملهم.

4.2.7 يجب ابقاء الجهاز مقفل حتى يعيد المستخدم اجراء الوصول باستخدام التعريف المحدد وإجراءات المصادقة.

5.2.7 يجب أن تكون جميع أجهزة المستخدمين الموجودة في الأماكن العامة مزودة بشاشات محمية بكلمات مرور يمكن تنشيطها بعد ساعات عدم النشاط أو استخدامها لإعادة تنشيط الشاشة.

8. الأدواروالمسؤوليات

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 متعارضات 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 التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

7.1.8 على إدارة الأمن السيبراني التأكد من استيفاء المتطلبات الأمنية الضرورية قبل تنفيذ الحلول/الأنظمة الجديدة في بيئة تقنية المعلومات.

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

9-1 المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

10. تغييرات السياسة

جب 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.06-27.CS.A. V2.0- سياسة الاستخدام المقبول للأصول
- ❖ DICT.I.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- ❖ DICT.I.06-67.CS.A.V2.0- معايير إدارة حوادث الأمن السيبراني

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
سياسة الجامعة النظيف والشاشة الخالية	-	-	-	-	-	A.11.2.9	AC-1, AC-11, MP-1, MP-2, MP-4

----------نهاية الوثيقة----------