سياسة التحكم في الوصول

الإصدارة١,١

رقم السياسة:

1. جدول المحتويات

٢. ١. جدول المحتويات ٢
٣. 7. معلومات ذات ملكية فكرية ٤
٤. 8. الرقابة على الوثيقة ٥
8.1. معلومات عن هذه السياسة ٥
8.2. تاريخ الإعداد والتحديث ٥
8.3. المراجعة والتحقق والاعتماد ٥
8.4. قائمة التوزيع ٦
٥. 9. نظرة عامة على السياسة ٧
9.1. الغرض ٧
9.2. النطاق ٧
9.3. المصطلحات والتعريفات ٨
9.4. التغيير والمراجعة والتحديث ٩
9.5. النفاذ والامتثال ٩
9.6. الاستثناءات ١٠
9.7. الأدوار والمسؤوليات (مصفوفة راسي) ١١
9.8. الوثائق ذات الصلة ١٢
9.9. الملكية ١٣
٦. 10. بيانات السياسية ١٤
10.1. سياسة التحكم في الوصول ١٥
10.2. الوصول إلى الشبكات وخدمات الشبكة ١٦
10.3. تسجيل المستخدم وإلغاء التسجيل ١٩
10.4. توفير وصول للمستخدم ٢٠
10.5. إدارة حقوق الوصول المتميزة ٢١
10.6. إدارة التوثيق السري لمعلومات المستخدمين ٢٢
10.7. مراجعة حقوق وصول المستخدم ٢٤
10.8. إلغاء حقوق الوصول أو تعديلها ٢٤
10.9. استخدام معلومات التوثيق السرية ٢٥
10.10. تقييد الوصول إلى المعلومات ٢٦
10.11. إجراءات تسجيل الدخول الآمنة ٢٧
10.12. نظام إدارة كلمة المرور ٢٨
10.13. استخدام البرامج المميزة في المرفق ٢٨
10.14. التحكم في الوصول إلى رمز مصدر البرنامج ٢٩

7. معلومات ذات ملكية فكرية

8. الرقابة على الوثيقة

٨,١. معلومات عن هذه السياسة

عنوان	تصنيف	الإصدارة	الحالة
سياسة التحكم في الوصول	سرية	0.1	التحقق من صحة

٨,٢. تاريخ الإعداد والتحديث

الإصدارة	المؤلف/المؤلفون	تاريخ الاصدار	التغييرات
0.1	علاء عليوه	17نوفمبر 2014	إعداد
0.2	نبيل البحبوح	27نوفمبر 2014	تحديث
0.3	أسامة العمري	23ديسمبر 2014	QA
1.0	نبيل البحبوح	31 ديسمبر 2014	تحديث
1.1	منيب احمد	21 أبريل 2017	تحديث

٨,٣. المراجعة والتحقق والاعتماد

الاسم	العنوان	التاريخ
لمياء عبدالله الجعفري	مدير الجودة	
الدكتور خالد العيسى	عميد تقنية المعلومات والاتصالات	

٨,٤. قائمة التوزيع

عدد النسخ	المستفيد	الموقع

9. نظرة عامة على السياسة

يتناول هذا الجزء من الوثيقة بالتفصيل الغرض من سياسة التحكم في الوصول ونطاقها ومصطلحاتها والتعريفات المتعلقة بها، وتغييرها ، ومراجعتها وتحديثها ، وإنفاذها والامتثال لها، والتنازل عنها، وأدوار ومسؤوليات الأشخاص المرتبطين بها ، والمستندات لها صلة بهذه السياسة وملكيتها.

٩,١. الغرض

الغرض الرئيسي من سياسة التحكم في الوصول هو:

الحد من الوصول إلى المعلومات و المرافق التي تعالج فيها هذه المعلومات، وضمان وصول المستخدم المصرح به إلى الأنظمة والخدمات ومنع غيره من الوصول إليها ، وجعل المستخدمين مساءلين عن حفظ المعلومات الخاصة بهم ، ومنع الوصول غير المصرح به إلى الأنظمة والتطبيقات..

٩,٢. النطاق

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع مصادر جامعة الإمام عبد الرحمن بن فيصل بكل مستويات حساسيتها؛ بما ذلك:

- جميع الموظفين العاملين بدوام كامل وبدوام جزئي والمؤقتين الذين يعملون في جامعة الإمام عبد الرحمن بن فيصل أو يعملون لصالحها أو نيابة عنها.
- الطلاب الذين يدرسون في جامعة الإمام عبد الرحمن بن فيصل.
- المقاولون والاستشاريون الذين يعملون لصالح جامعة الإمام عبد الرحمن بن فيصل أو نيابة عنها.
- جميع الأفراد والجماعات الأخرى التي منحت إمكانية الوصول إلى نظم المعلومات والاتصالات في الجامعة.

تغطي هذه السياسة جميع أصول المعلومات المحددة في وثيقة نطاق تقييم المخاطر وسيتم استخدامها كأساس لإدارة أمن المعلومات.

٩,٣. المصطلحات والتعريفات

يقدم الجدول ٢ تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى أنه يمكن تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي لها قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفّر	الحالة التي يكون فيها الأصل أو الخدمة قابلة للوصول إليها واستخدامها عند الطلب من قِبل جهة معتمدة.
السرية	عدم اتاحة وصول الأفراد غير مصرح لهم لأصل من الأصول
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 يوضح ما يجب عمله وكيفية تحقيق الأهداف المحددة في السياسات.
الحاجة إلى المعرفة	لا يُمنح المستخدم سوى الوصول إلى المعلومات التي يحتاجها لأداء مهامه (المهام / الأدوار المختلفة تعني اختلاف الحاجة إلى المعرفة وبالتالي توصيفات وصول مختلفة).
الحاجة الى الاستخدام	لا يُمنح المستخدم سوى الوصول إلى مرافق تقنية المعلومات التي يحتاجها لأداء مهمته / الوظيفة / الدور (مثل المعدات والتطبيقات والإجراءات والغرف).
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوافرها. بالإضافة إلى ذلك، يمكن أيضًا استخدام خصائص أخرى مثل الأصالة والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على وتأكيد دقة وتناسق الأصول طوال دورة حياتها بأكملها.

المالك	أي شخص أو مجموعة من الأشخاص حددتهم الإدارة ليكونوا مسؤولين عن الحفاظ على سرية الأصول وتوافرها وسلامتها. قد يتغير المالك 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.
التوفير (توفير الوصول)	عملية إعطاء أو إلغاء حقوق الوصول للمستخدمين إلى المعلومات والأنظمة والخدمات.
الخطر	مزيج من عواقب الحدث (بما في ذلك التغييرات في الظروف) واحتمال حدوثها.
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 والتعريفات

٩,٤. التغيير والمراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا تجرى تغييرات في هذه السياسة إلا من قبل ضابط أمن المعلومات على تعتمد هذه التغييرات من قبل الإدارة. يجب أن يظل سجل التغيير محدثًا ويتم تحديثه بمجرد إجراء أي تغيير.

٩,٥. النفاذ والامتثال

يعد الامتثال لهذه السياسة أمراً إلزاميًا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات. ويجب على جميع وحدات الجامعة (من عمادات، وإدارات، وكليات ، وأقسام ، ومراكز) ضمان مراقبة الامتثال المستمر لهذه السياسة في نطاق وحداتهم.

وفي حالة تجاهل أو انتهاك توجيهات أمن المعلومات، يمكن أن تتضرر بيئة الجامعة (فعلى سبيل المثال، تفقد الجامعة الثقة فيها و تفقد سمعتها أو يتعطل فيها ، أو تحدث فيها مخالفات قانونية). وفي هذه الحالة يكون الأشخاص المخطئون مسؤولين عما حدث مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات القانونية.

يجب ضمان خضوع الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية لمعاملة صحيحة وعادلة (مثل الإجراءات التأديبية). ويجب إبلاغ إدارة الموارد البشرية لمعالجة المخالفات المتعلقة بهذه السياسة، والتعامل مع ما يحدث لها من انتهاكات.

٩,٦. الاستثناءات

يجب أن ينظر أمن المعلومات في الاستثناءات المتعلقة بهذه السياسة على أساس فردي. وللموافقة على استثناء متعلق بها، يجب أن يرفق مع طلب الاستثناء ظروف العمل التي اقتضت التقدم به مشفوعة بالمبررات المنطقية لذلك. ويتعيّن أن يوافق ضابط أمن المعلومات على الاستثناءات من شرط الامتثال للسياسة وأن تعتمد عمادة تقنية المعلومات والاتصالات هذه الموافقة. ويجب أن يشمل كل طلب تنازل المبررات والمزايا المنسوبة إلى الاستثناء.

تبلغ فترة الاستثناء من السياسة أربعة أشهر كحد أقصى، ويجب إعادة تقييمها واعتمادها – إذا اقتضى الأمر - لمدة أقصاها ثلاثة فترات متتالية. ولن يتم تقديم أي استثناء لأكثر من ثلاث فترات متتالية.

٩,٧. الأدوار والمسؤوليات (مصفوفة راسي)

يوضح الجدول (٢) مصفوفة راكي (RACI) [١]التي تحدد من هو الشخص المسؤول ومن هو الشخص المساءل وماهي الجهة التي ينبغي استشارتها أو إبلاغها بكل مهمة هناك حاجة للقيام بها. هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: عمادة تكنولوجيا المعلومات والاتصالات، موظف أمن المعلومات ، إدارة الموارد البشرية / الوحدة الإدارية (الموارد البشرية أو الشخص المساءل) ، المالك والمستخدم (الموظفون ، أعضاء هيئة التدريس ، الطلاب ، المقاولون ، الاستشاريون والثالث حفلات).

الأدوار / المسؤوليات	تقنية المعلومات	المسؤول عن أمن المعلومات	الموارد البشرية أو الجهة المساءلة	مدير الإدارة	المالك	المستعمل
تحديد حقوق الوصول المطلوبة لمستخدمي الأصول.	R, C	C		C	R,A	I
الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات.	C	C	C			R,A ,I
الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة تكنولوجيا المعلومات والاتصالات	A, C	C			I	R

[١] تصف مصفوفة راكي (RACI) - الخاصة بتحديد المسؤوليات - الأدوار 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.

الأدوار / المسؤوليات	تقنية المعلومات	المسؤول عن أمن المعلومات	الموارد البشرية أو الجهة المساعدة	مدير الإدارة	المالك	المستعمل
التأكد من أن الموظف المستقيل أو المنتهية مدة عمله قد أعاد جميع أصول الجامعة التي معه قبل إكمال عملية إخلاء الطرف	C	C	R, A	I		
إلغاء حقوق الوصول (المنطقية والمادية) للأصول عند إنهاء خدمة الموظف أو تغييره.	R, A	C	C			
ضمان حماية نظم المعلومات / البنية التحتية، وفقا للآليات التكنولوجية المحددة من قبل فريق تصميم النظام / التطبيق	R, A	R, C				
التحقيق في انتهاكات الضوابط الأمنية، وتطبيق ضوابط تعويض إضافية عند الضرورة.	R, A	R, C			I	
تطبيق الضوابط المناسبة لحماية الأصول.	R, A	C			I	
مراجعة حقوق وصول المستخدم والامتيازات بشكل منتظم.	R, A	C	C		R,C	
الموافقة على استمارة تسجيل وصول المستخدم	C	C		R,A	C	I

الجدول ٢: الأدوار والمسؤوليات المخصصة بناءً على مصفوفة *RACI*

٩,٨. الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات
- سياسة الأمن
- سياسة الأمن المادي والبيئي

- سياسة أمن العمليات
- سياسة أمن الاتصالات
- سياسة الامتثال
- سياسة إدارة المخاطر
- تغيير إجراءات الإدارة
- إجراءات التحكم في الوصول المادي والمنطقي
- إجراءات أمن الموارد البشرية

٩,٩. الملكية

هذه الوثيقة مملوكة لعمادة تقنية المعلومات والاتصالات بجامعة الإمام عبدالرحمن بن فيصل و هي التي تحافظ عليها.

10. بيانات السياسية

تقدم الأجزاء الفرعية التالية بيانات السياسة في أربعة عشر جانبًا رئيسيًا هي:

- سياسة التحكم في الوصول
- الوصول إلى الشبكات والشبكات
- تسجيل المستخدم وإلغاء تسجيله
- توفير وصول المستخدم
- إدارة حقوق الوصول المتميزة
- إدارة معلومات التوثيق السرية للمستخدمين
- مراجعة حقوق وصول المستخدم
- إزالة تعديل حقوق الوصول
- استخدام معلومات المصادقة السرية
- تقييد الوصول إلى المعلومات
- إجراءات تسجيل الدخول الآمنة
- نظام إدارة كلمة المرور
- استخدام برامج الأدوات المساعدة المميزة
- التحكم في الوصول إلى رمز مصدر البرنامج

١٠,١. سياسة التحكم في الوصول

١. يجب التحكم في الوصول إلى المعلومات بناءً على متطلبات العمل ومقتضيات لأمن وقواعد الوصول المحددة لكل نظام من أنظمة جامعة الإمام عبد الرحمن بن فيصل. وتشمل هذه القواعد ما يلي:

i. ضوابط الوصول المنطقي والمادي.

ii. متطلبات الأمان لتطبيقات أعمال الجامعة

iii. أحد متطلبات الأعمال المحددة للمستخدم للوصول إلى المعلومات أو العمليات التجارية (مبادئ "الحاجة إلى المعرفة" و "الحاجة إلى الاستخدام").

iv. . يرفض أي وصول ما لم يتم اعتماده وفقًا لأحكام هذه السياسة

v. التغييرات في إذن المستخدم سواء تم تنفيذها تلقائيًا أو بواسطة مسؤول.

vi. الالتزام القانوني و / أو التعاقدي بتقييد وحماية الوصول إلى أنظمة الجامعة

٢. لا يتم إتاحة وصول المتعاقدين أو موظفي الأطراف الثالثة إلى أصول معلومات الأعمال الخاصة بـجامعة الإمام عبد الرحمن بن فيصل إلا بناءً على اتفاقية تعاقدية. تشمل هذه الاتفاقية على سبيل المثال لا الحصر:

I. شروط وأحكام الوصول المقدمة.

II. . المسؤوليات الأمنية للمقاولين أو موظفي طرف ثالث.

III. موافقة المتعاقدين أو موظفي الطرف الثالث على الالتزام بسياسات أمن المعلومات الخاصة بـ جامعة الإمام عبد الرحمن بن فيصل.

مرجع # [ISO / IEC 27001: A.9.1.1]

١٠,٢. الوصول إلى الشبكات وخدمات الشبكة

١. يجب أن يكون الوصول إلى الشبكات وخدمات الشبكة مصرحاً به ومراقبًا استنادًا إلى متطلبات العمل ومتطلبات الأمن وقواعد التحكم في الوصول المحددة لكل شبكة. تشمل هذه القواعد ما يلي:

i. متطلبات الأمان للشبكة أو خدمات الشبكة

ii. متطلب عمل محدد يقتضي وصول المستخدم إلى الشبكة (مثل استخدام في بي إن {VPN } أو الشبكة اللاسلكية) أو خدمات الشبكة (مبدأ "الحاجة إلى الوصول ").

iii. تصنيف أمان المستخدم وتصنيف أمان الشبكة.

iv. متطلبات التصريح للمستخدم بالوصول إلى خدمات الشبكة المختلفة.

v. مراقبة وإدارة استخدام خدمات الشبكة.

vi. آليات الترخيص لتحديد من يُسمح له بالوصول إلى الشبكات وخدمات الشبكة.

٢. يجب ألا تكون جميع أجهزة الحاسب الآلي متصلة بشبكة الجامعة ولا يُسمح لها بالوصول الكامل إلى جميع موارد الشبكة والإنترنت ما لم تكن متوافقة مع متطلبات التحكم في الوصول إلى الشبكة المذكورة أدناه:

i. سياسات أمن نظام التشغيل.

ii. تحديث تعريفات مكافحة الفيروسات

iii. قواعد الأمن المتعلقة بحائط النيران.

٣. يجب توفير الوصول إلى شبكة الجامعة السلكية واللاسلكية للموظفين والطلاب والضيوف وفقًا لمتطلبات الأمان التالية:

المجموعة	متطلبات الأمن	
	شبكة سلكية	شبكة لاسلكية

الموظفون	• التأكد من وجود نقطة نهاية لبرنامج سمانتك (Symantec) ونقاط مكافحة التجسس وتعريفات مكافحة الفيروسات للحصول على تحديث لا تزيد مدته عن ٥ أيام. • يجب أن تحصل الأجهزة المتوافقة مع السياسة على إمكانية الوصول الكامل إلى شبكة الجامعة استنادًا إلى العضوية في بورت في إل إي . Port VLA • يجب حرمان المستخدمين غير الملتزمين بالسياسة والأجهزة الموجودة في نطاق الجامعة ولكنها غير ملتزمة بالسياسة من الوصول إلى شبكة الجامعة (بما في ذلك الانترنت)	• إعادة توجيه الويب إلى وكيل سيسكو ويب إن إي سي (Cisco Web NAC) للتحقق من وجود تحديثات لمكافحة الفيروسات لا تزيد مدتها عن ٥ أيام. • يجب منح المستخدمين الممتثلين للسياسة حق الوصول إلى خدمات يو سي ((UC باستخدام أجهزتهم النقالة بعد التنميط. • يمنح المستخدمون الملتزمون بالسياسة وصولاً محدوداً للاتصال بالإنترنت فقط دون الوصول إلى مصادر الشبكة الداخلية. • يجب حرمان المستخدمين غير الملتزمين بالسياسة حرماناً تاماً من الوصول إلى مصادر الشبكة (بما في ذلك الوصول إلى الإنترنت).
الطلاب	• التأكد من وجود نقطة نهاية لبرنامج سمانتك (Symantec) ونقاط مكافحة التجسس وتعريفات مكافحة الفيروسات للحصول على تحديث لا	• إعادة توجيه الويب إلى وكيل شبكة سيسكو Cisco Web NAC,للتحقق من وجود تحديثات لمكافحة الفيروسات لا تزيد مدتها عن

	تزيد مدته عن ٥ أيام. • يجب أن تمنح الأجهزة المتوافقة وصولاً محدودًا إلى خوادم إس آي إس(SIS)واتصال الإنترنت فقط. • يجب منع أجهزة المستخدمين غير المتوافقة مع السياسة والمستخدمين غير الملتزمين بها من الوصول إلى مصادر الشبكة (بما في ذلك الوصول للإنترنت)	٥ أيام. • يمنح المستخدمون الملتزمون بالسياسة الوصول إلى الإنترنت وخوادم SIS الداخلية. • يجب منع المستخدمين غير الملتزمين بالسياسة من الوصول إلى مصادر الشبكة (بما في ذلك الوصول إلى الإنترنت)
ضيوف	يمنع الضيوف من الوصول إطلاقاً	• يجب على الضيف تسجيل الدخول لفتح SSID للوصول إلى الاتصال اللاسلكي. • فرض إعادة التوجيه إلى صفحة الويب لإرسال المعلومات المطلوبة. • يسمح بالتسجيل الذاتي من خلال تقديم الاسم الأول والاسم الأخير ورقم الجوال. • يجب أن يتلقى المستخدمون كلمة مرور صالحة لمرة واحدة (OTP) من خلال الرسائل القصيرة) أي ، تسجيل الدخول بأوراق اعتماد مرسلة

		عبر الرسائل القصيرة وتوجيهها إلى السجل النشط • يجب منح المستخدمين الملتزمين وصولاً محدوداً إلى الإنترنت فقط.

التسمية التوضيحية، والإشارة إلى أن هذا جاء من جامعة الإمام عبد الرحمن بن فيصل

٤. يجب أن ينظر الوصول إلى المجلدات المشتركة فيما يلي:

i. المصرح به فقط لموظفي معين.

ii. يستخدم فقط لغرض أعمال جامعة الإمام عبد الرحمن بن فيصل

iii. لا يُسمح بمشاركة أي مواد تجارية غير ذات صلة (مثل الصور ومقاطع الفيديو والملفات الصوتية وما إلى ذلك).

المرجع: [ISO / IEC 27001: A.9.1.2]

١٠,٣. تسجيل المستخدم وإلغاء التسجيل

١. تحدد عمادة تقنية المعلومات والاتصالات إجراءً رسميًا للتحكم في الوصول يتضمن خطوات واضحة فيما يتعلق بطلب حسابات المستخدمين وإنشائها وتعديلها وتعليقها وسحبها.

٢. يُسمح للمالك بمنح وصول المستخدم والتغييرات في حقوق وصول المستخدم الحالية وإزالة وصول المستخدم، مع مراعاة ما يلي:

i. الامتياز الأقل (مبدأ "الحاجة إلى المعرفة").

ii. الفصل بين الواجبات.

iii. مستوى الوصول المطلوب.

٣. يجب أن تتناول عملية إدارة معرفات المستخدم ما يلي:

i. يتم تعريف جميع موظفي جامعة الإمام عبد الرحمن بن فيصل بمعرف خاص بتحديد الهوية. يجب أن يتطلب معرف المستخدم عامل مصادقة واحدًا على الأقل (على سبيل المثال، كلمة المرور أو الرقم المميز أو الأجهزة البيومترية).

ii. يجب تسجيل جميع موظفي الجامعة من خلال إجراءات تسجيل المستخدم الرسمية المعتمدة من جامعة الإمام عبد الرحمن بن فيصل.

iii. لا يجوز السماح بمعرفات مستخدم مكررة أو مشتركة أو جماعية.

iv. يجب إزالة المستخدم المكرر أو تعطيله.

v. يجب أن يقتصر عدد هويات المستخدمين المميزين على الأفراد الذين يتمتعون بهذه الامتيازات لأغراض عمل مصرح بها.

vi. يجب أن يكون لكل مسؤول عن الأنظمة متعددة المستخدمين معرّفين اثنين على الأقل ليفصلوا وصولهم المميز عن وصولهم اليومي العادي

vii. يتم تحقيق التحكم المستمر في الوصول عبر أنواع مختلفة من أنظمة الجامعة من خلال دعم رموز هوية المستخدم القياسية، وبرامج الإنتاج وأسماء الملفات، وأسماء النظام.

[ISO/IEC 27001: A.9.2.1]

١٠,٤. توفير وصول للمستخدم

١. يجب تعريف وتوثيق جميع المستخدمين المصرح لهم الذين يصلون إلى أصول جامعة الإمام عبد الرحمن بن فيصل. يجب تتبع وتسجيل عملية التصريح بالوصول على النحو التالي:

a. تاريخ الترخيص.

b. تحديد الشخص الذي يعتمد الوصول.

c. وصف امتيازات الوصول الممنوحة.

d. ذكر السبب الذي بموجبه تم منح امتيازات الوصول.

٢. يجب أن تراعي عملية منح أو إلغاء حقوق الوصول للمستخدمين ما يلي:

a. الحصول على ترخيص مناسب من النظام أو مالك الخدمة

b. يتم الفصل بين الواجبات لضمان مستوى وصول مناسب.

c. لا يتم تنشيط حقوق الوصول حتى تكتمل عملية التصريح بالوصول.

d. يتم تحديث السجلات التي تبرز جميع حقوق وصول المستخدم مركزيًا.

e. تحديث حقوق وصول المستخدمين بناءً على أدوار ومسؤوليات موظفي جامعة الإمام عبد الرحمن بن فيصل

f. مراجعة حقوق وصول المستخدمين بشكل دوري

٣. تمنح عمادة تقنية المعلومات والاتصالات المستخدمين إمكانية الوصول إلى أنظمة الجامعة وخدماتها وفقًا لدور منسوب الجامعة العمل ووصفه الوظيفي (أي الوصول إلى الملفات الشخصية الصحيحة).

[ISO/IEC 27001: A.9.2.2]

١٠,٥. إدارة حقوق الوصول المتميزة

١. تتم إدارة منح حقوق الوصول إلى الامتيازات واستخدامها على النحو التالي:

i. تحديد حقوق الوصول المطلوبة لكل نظام أو عملية (مثل نظام التشغيل وقاعدة البيانات والتطبيق والشبكة).

ii. منح حقوق الوصول وفقاً لمبدأ الحاجة إلى الاستخدام ومبدأ الحدث تلو الحدث.

iii. تحديد متطلبات انتهاء صلاحية جميع حقوق الوصول.

iv. توفير حقوق الوصول وفقًا لقدرات تشكيل النظام

٢. لا يجوز للمستخدمين الوصول إلى حساب الإدارة أو امتيازاتها على أجهزتهم المحلية.

[ISO/IEC 27001: A.9.2.3]

١٠,٦. إدارة التوثيق السري لمعلومات المستخدمين

١. تتطلب جميع أنظمة جامعة الإمام عبد الرحمن بن فيصل تحديد الهوية والتوثيق من خلال طريقة مناسبة لمعلومات المصادقة السرية (مثل كلمات المرور ومعرفات الرموز المميزة أو البطاقات الذكية أو القياسات الحيوية).

٢. قبل السماح للمستخدم بالوصول إلى أي نظام أو تطبيق خاص بوحدة من وحدات الجامعة، يتم تنفيذ المصادقة على كلمة المرور وفق الخطوات التالية:

i. يجب ألا تقل كلمة المرور عن ثمانية أحرف كحد أدنى للمستخدمين العاديين و ١٢ حرفًا لمسؤولي تقنية المعلومات (على سبيل المثال، مسؤول النظام، مسؤول التطبيق، المشرف على قاعدة البيانات ومشرف الشبكة).

ii. يجب أن تكون كلمة المرور مكونة من ثلاثة عناصر على الأقل من العناصر الأربعة التالية:

- حرف أبجدي واحد صغير على الأقل (a-z)
- حرف أبجدي واحد كبير على الأقل (A-Z)
- رقم واحد على الأقل (٠-٩)
- حرف خاص واحد على الأقل (على سبيل المثال، @ # $٪ ^ & * () _ + | ~ - = \ `{}[]:";'<>? /)

iii. يجب ألا تحتوي كلمات المرور على هوية المستخدم.

iv. يجب ألا تحتوي كلمات المرور على أكثر من حرفين متطابقين في صف واحد ولا تتكون من جميع الأحرف الرقمية أو الهجائية.

v. لا يجوز السماح بكلمة مرور في شكل فراغ.

vi. يجب على المستخدمين تغيير كلمة المرور الخاصة بهم فور تسجيل الدخول لأول مرة إلى أي نظام (على سبيل المثال، يجب تكوينها لمطالبة المستخدم باختيار كلمة مرور أخرى قبل متابعة جلسة العمل الخاصة به).

vii. يجب قفل حساب المستخدم بعد ٣ دقائق من ثلاث محاولات فاشلة:

viii. يجب تطبيق تغيير كلمة المرور (بواسطة نظام التشغيل أو التطبيق) كل ٩٠ يومًا على الأقل. ولا يجوز إعادة استخدام نفس كلمة المرور

ix. يجب استخدام كلمة المرور الأولية مرة واحدة فقط (على سبيل المثال، يجب أن تكون صالحة فقط لأول تسجيل دخول للمستخدم المشترك) وتنتهي في ٢٣:٥٩:٥٩ من تاريخ إصدارها.

x. يجب تخزين كلمة المرور وإرسالها في صورة محمية (على سبيل المثال، مشفرة أو مجزأة)، إن أمكن.

٣. يجب تغيير كلمات المرور على الفور إذا كان هناك أي شك في وجود مشكلة تتعلق بكلمة المرور؛ ويبلغ هذا على الفور إلى عمادة تقنية المعلومات والاتصالات

٤. يجب على عمادة تقنية المعلومات والاتصالات تغيير جميع أنظمة الجامعة وأسماء المستخدمين وكلمات المرور الافتراضية للبرنامج عند التثبيت.

٥. يجب على عمادة تقنية المعلومات منح المستخدم كلمة مرور جديدة بعد التحقق من هويته

المرجع: [ISO / IEC 27001: A.9.2.4]

١٠,٧. مراجعة حقوق وصول المستخدم

١. عند اكتشاف سوء استخدام حقوق الوصول المميزة، تقوم عمادة تقنية المعلومات والاتصالات بتقييد الامتيازات المتعلقة بحقوق الوصول.

٢. يجب مراجعة حقوق الوصول لجميع مستخدمي جامعة الإمام عبد الرحمن بن فيصل وفقًا لإجراءات التحكم في الوصول المادي والمحلي للمستخدم المعتمدة رسميًا.

٣. تقوم عمادة تقنية المعلومات والاتصالات بالتعاون مع مالك الأصول ومسؤول أمن المعلومات بما يلي:

أ- وضع خطة مراجعة لحقوق وصول المستخدم تشمل ما يلي:

- مراجعة أنظمة جامعة الإمام عبد الرحمن بن فيصل
- عدد مرات المراجعة.

ب- مراجعة امتيازات الوصول التالية:

- ملفات الوصول للأنظمة عالية المخاطر (أنظمة مهمة حرجة) كل ثلاثة أشهر
- ملفات الوصول لأنظمة المخاطر المتوسطة كل ستة أشهر
- ملفات الوصول لأنظمة المخاطر العادية على أساس سنوي

المرجع: [ISO / IEC 27001: A.9.2.5]

١٠,٨. إلغاء حقوق الوصول أو تعديلها

١. يقوم مدير الإدارة بالإبلاغ الفوري عن جميع التغييرات المهمة في واجبات الموظفين و / أو حالة التوظيف إلى إدارة الموارد البشرية والوحدة الإدارية المعنية وعمادة تقنية المعلومات والاتصالات

٢. عندما يغادر الموظف بشكل دائم جامعة الإمام عبد الرحمن بن فيصل

a. يجب إخطار المسؤولين عن النظام.

b. يجب إنهاء جميع امتيازات الوصول إلى جامعة الإمام عبد الرحمن بن فيصل على الفور.

c. يجب على عمادة تقنية المعلومات والاتصالات إزالة جميع الملفات الموجودة في دليل الموظف بعد شهر واحد من انتهاء خدمته، ما لم يتم الإخطار بعدم إزالتها.

[ISO/IEC 27001: A.9.2.6]

١٠,٩. استخدام معلومات التوثيق السرية

١. يكون المستخدمون مسؤولين عن أي نشاط يرتبط بحقوق الوصول الخاصة بهم.

٢. لا يجوز للمستخدمين التقاط أو الحصول على كلمات المرور أو مفاتيح فك التشفير أو أي طريقة مصادقة سرية أخرى قد تسمح بالوصول غير المصرح به.

٣. لا يجوز للمستخدمين القيام بما يلي:

أ- كشف كلمة المرور عبر الهاتف لأي شخص.

ب- كشف كلمة المرور في رسالة بريد إلكتروني.

ت- كشف أو وزع كلمة مرور للآخرين ولا يجوز كشف كلمة المرور حتى لمسؤولي تقنية المعلومات أو لرئيس المستخدم في العمل.

ث- التحدث عن كلمة المرور أمام الآخرين.

ج- التلميح بمكونات كلمة المرور:

- اسم العائلة والأصدقاء وزملاء العمل
- تاريخ الميلاد والعنوان ورقم الهاتف
- الأنماط: "aaabbb" و "١١١٢٢٢٢"

ح- كشف كلمة المرور على الاستبيانات أو نماذج الأمن.

خ- تبادل كلمة المرور مع أفراد الأسرة

د- الكشف عن كلمة مرور لزملاء العمل أثناء العطلة.

ذ- كتابة كلمة المرور على قطعة من الورق وتركها في مكان يستطيع المستخدمون غير المصرح لهم باكتشافها.

٤. تتأكّد عمادة تقنية المعلومات والاتصالات مما يلي:

أ- تشفير كلمات المرور دائمًا عند تخزينها أو وضعها في سجلات الوصول لأي نظام خاص بجامعة الإمام عبد الرحمن فيصل.

ب- لا يتم تخزين كلمات المرور في متصفحات الإنترنت (على سبيل المثال، ملفات تعريف الارتباط (cookie) الموجودة على أجهزة عمل المستخدم لم توضع لإكمال كلمة المرور وتسجيل الدخول تلقائيًا).

ت- تصميم الأنظمة واختبارها والتحكم فيها لمنع استرجاع كلمات المرور المخزنة واستخدامها بطريقة غير مصرح بها.

REF: [ISO/IEC 27001: A.9.3.1]

١٠،١٠. تقييد الوصول إلى المعلومات

١. تحدد الضوابط المناسبة للتحكم في وظائف أنظمة التطبيق على النحو التالي:

أ- وضع حد لمعلومات المخرجات.

ب- تقييد الوصول إلى المعلومات وفقاً لملف الوصول الذي يعرف بالمستخدم.

ت- تحديد امتيازات الوصول المناسبة المطلوبة (على سبيل المثال، القراءة والكتابة والحذف والتنفيذ).

ث- تطبيق عزل الوصول المنطقي والمادي فيما بين أنظمة الجامعة الهامة المختلفة.

[ISO/IEC 27001: A.9.4.1]

١٠,١١. إجراءات تسجيل الدخول الآمنة

١. يجب أن يستند تسجيل الدخول إلى أنظمة تشغيل الجامعة إلى إجراء تسجيل دخول آمن رسمي.

٢. يجب أن تعرض جميع الأنظمة رسالة تحذير إشعار عامة بأن الوصول إلى أنظمة جامعة الإمام عبد الرحمن بن فيصل يُمنح للمستخدمين المصرح لهم فقط.

٣. يجب أن توفر عملية تسجيل الدخول على أي نظام من الأنظمة عرضاً لمعلومات محددة عن النظام والغرض الذي تستخدم من أجله.

٤. عندما تكون هناك حاجة قوية إلى توثيق وتحديد الهوية، يجب تنفيذ أساليب توثيق بخلاف كلمات المرور (مثل، معرفات الرمز المميز أو البطاقات الذكية أو القياسات الحيوية)

٥. يجب أن تحدد جميع الأنظمة عدد محاولات تسجيل الدخول غير الناجحة المسموح بها؛ وأن يؤخذ في الحسبان ما يلي:

أ- تسجيل كل المحاولات الناجحة وغير الناجحة.

ب- فرض تأخير زمني قبل السماح بمزيد من محاولات تسجيل الدخول أو رفض أي محاولات أخرى دون إذن محدد.

ت- إرسال رسالة إنذار إلى وحدة تحكم النظام إذا تم الوصول إلى الحد الأقصى لعدد محاولات تسجيل الدخول.

٦. يجب على مسؤولي تقنية المعلومات والاتصالات (على سبيل المثال ، مسؤول النظام ، مسؤول التطبيق ، مشرف قاعدة البيانات ومشرف الشبكة) مراجعة جميع محاولات تسجيل الدخول غير الناجحة بشكل دوري

[ISO/IEC 27001: A.9.4.2]

١٠,١٢. نظام إدارة كلمة المرور

١. يجب على عمادة تقنية المعلومات والاتصالات اعتماد نظام تفاعلي لإدارة كلمات المرور من أجل:

أ- فرض جودة كلمات المرور.

ب- فرض تغييرات كلمة المرور العادية حسب الحاجة.

ت- الحفاظ على سجل يشمل كلمات المرور المستخدمة سابقا

ث- إخفاء كلمات المرور على الشاشة عند إدخالها.

ج- عزل ملفات كلمة المرور عن بيانات نظام التطبيق

ح- تشفير كلمة المرور عند تخزينها ونقلها

REF: [ISO/IEC 27001: A.9.4.3]

١٠,١٣. استخدام البرامج المميزة في المرفق

١. يجب منع المستخدمين من دخول جميع مرافق النظام إلا بإذن كتابي من عمادة تقنية المعلومات والاتصالات.

٢. على عمادة تقنية المعلومات والاتصالات تسجيل ومراجعة كل عمليات الوصول إلى مرافق النظام

٣. يجب تقييد الوصول إلى برامج النظام واستخدامها والتحكم فيها.

٤. يجب إزالة جميع خدمات وبرامج النظام غير الضرورية.

[ISO/IEC 27001: A.9.4.4]

١٠,١٤. التحكم في الوصول إلى رمز مصدر البرنامج

١. يجب توثيق الوصول إلى رموز مصدر البرامج والتكوينات والعناصر ذات الصلة (مثل التصميمات والمواصفات وخطط التحقق وخطط الاعتماد) وأن يقتصر ذلك على الموظفين المعتمدين.

٢. تتأكّد عمادة تقنية المعلومات والاتصالات من جمع كل رموز المصدر والتحكم فيها وصيانتها مركزيا.

REF: [ISO/IEC 27001: A.9.4.5]

---------- نهاية الوثيقة ----------