ابتكار الأعمال الملهمة

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

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

سياسة الوصول عبر الشبكة الافتراضية الخاصة

الإصدار: 2.0

رمز السياسة: DICT-QAP021

October 2020

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

جدول المحتويات

معلومات ذات ملكية فكرية 3
الرقابة على الوثيقة 4
معلومات عن الوثيقة 4
الإعداد والتحديث 4
قائمة التوزيع 4
الإعتماد 4
نظرة عامة على السياسة 5
الغرض 5
النطاق 5
تعريف المصطلحات 6
التغيير والمراجعة والتحديث 6
الإنفاذ / الامتثال 7
الاستثناءات 7
الوثائق ذات الصلة 7
الملكية 8
بيانات السياسة 9

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

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.

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة الوصول الخاصة الافتراضية	عام	2.0	معتمدة

الإعداد والتحديث

الإصدار	الإعداد	تاريخ الاصدار	التغييرات
1.0	جميل س. بإجامي	27 أغسطس 2015	إعداد
1.1	منيب أحمد	24 أبريل 2017	تحديث
1.2	لمياء عبد الله الجعفري	6 يونيو 2020	تحديث
2.0	د. سامر بني عواد	13 سبتمبر 2020	تحديث

قائمة التوزيع

الرقم	المستفيد
1	إدارة الشؤون القانونية
2	الموقع الالكتروني للجامعة
3	قسم ضمان الجودة بالعمادة
4	قسم إدارة الأنظمة بالعمادة
5	قسم إدارة الشبكات بالعمادة

الإعتماد

الاسم	الوظيفة	التاريخ	التوقيع
د. خالد عدنان العيسى	عميد الاتصالات وتقنية المعلومات	8th October 2020	

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

نظرة عامة على السياسة

الغرض من هذه السياسة هو توفير إرشادات للوصول عن بعد عبر حزمة برتوكول الانترنت الأمنية (IPsec) أو لتوصيل الشبكة الافتراضية الخاصة (VPN) بشبكة جامعة الإمام عبد الرحمن بن فيصل.

الغرض

يتيح اتصال الشبكة الافتراضية الخاصة بجامعة الإمام عبد الرحمن بن فيصل للمستخدمين الاتصال مباشرة بشبكة الجامعة عبر الإنترنت. وللسماح بهذا الاتصال، يجب معالجة مشكلات الاتصال الآمن ومشكلات الأداء والتعامل وفق معايير استخدام النطاق الترددي. لذا فالغرض الرئيسي من الامتثال لهذه السياسة هو:

تجنب حدوث انتهاكات للالتزامات النظامية أو القانونية أو اللائحية أو التعاقدية المتعلقة بأمن المعلومات وتجنب انتهاك أي متطلبات أمنية.

النطاق

تنطبق بيانات السياسة المكتوبة في هذا المستند على جميع مستخدمي الشبكة الافتراضية الخاصة في جامعة الإمام عبد الرحمن بن فيصل على جميع مستويات الحساسية بما في ذلك:

- إدارة الشبكة الافتراضية الخاصة
- الإداريون
- العاملون
- المقاولون العاملون 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 الذين تم منحهم إمكانية الوصول إلى شبكة تقنية المعلومات والاتصالات الخاصة بجامعة الإمام عبد الرحمن بن فيصل من خلال الدخول بالشبكة الافتراضية الخاصة.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

تعريف المصطلحات

يقدم الجدول 1 تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى ضرورة القدرة على تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي تعتبر ذات قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفر	الحالة التي يكون فيها الأصل أو الخدمة قابلة لأن تصلها جهة مصرّح لها بذلك وقابلة لأن تستخدمها أيضاً.
السرية	عدم توفير الأصل أو الخدمة أو عدم كشف أيّ منهما لأفراد غير مصرح لهم أو جهات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر تشمل السياسات والإجراءات والإرشادات التي قد تكون ذات طبيعة إدارية عليا أو تقنية أو إدارية أو قانونية.
الإرشاد	وصف يوضح ما يجب عمله لتحقيق الأهداف المحددة في السياسات والطريقة التي تحقق بها تلك الأهداف.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفّرها. وهو يشمل وسائل أخرى مثل التحقّق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول والتأكّد من دقتها وتناسقها طوال دورة حياتها بأكملها.
البرمجيات الضارة (الخبيثة)	برمجيات مصممة لتعطيل تشغيل الحاسب الآلي أو لجمع معلومات حساسة أو الوصول إلى أنظمة الحاسب الآلي الخاصة (على سبيل المثال، فيروس أو حصان طروادة).
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. وتشمل السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.
الخطر	مزيج من عواقب الحدث واحتمالات حدوثها (بما في ذلك التغيرات في الظروف).
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 1: تعريف المصطلحات

التغيير والمراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا يجري تغييرات في هذه السياسة إلا ضابط أمن المعلومات على أن تعتمد الإدارة هذه التغييرات. ويجب أن يظل سجل التغيير محدثًا بحيث يخضع للتحديث بمجرد إجراء أي تغيير في السياسة.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الإنفاذ / الامتثال

يعد الالتزام بهذه السياسة أمراً إلزاميًا وعلى ضابط أمن المعلومات أن يراجعه بشكل دوري. ويجب على جميع وحدات جامعة الإمام عبد الرحمن بن فيصل (من عمادات، وإدارات، وكليات، وأقسام ومراكز) التأكد من الامتثال لها باستمرار.

في حالة تجاهل أو انتهاك توجيهات أمن المعلومات، قد تتضرر بيئة جامعة الإمام عبد الرحمن بن فيصل (على سبيل المثال، يحدث فقدان للثقة في الجامعة وسمعتها، أو تتعطل عملياتها أو تحدث بها انتهاكات قانونية)، ويكون الأشخاص الذين تجاهلوا هذه التوجيهات أو انتهكوها مسؤولين عما وقعوا فيه من فعل أو ترك مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب ضمان معاملة الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية بطريقة صحيحة وعادلة (مثل الإجراءات التأديبية). ويجب إبلاغ إدارة الموارد البشرية لمعالجة انتهاكات السياسة وعند التعامل مع هذه الانتهاكات.

الاستثناءات

يجب أن ينظر أمن المعلومات في الاستثناءات على أساس فردي. كما يجب أن يرفق مع طلب الاستثناء حالة العمل المنطقية التي استدعت تقديمه وطلب الموافقة عليه. والجهة المخوّل لها الموافقة على هذا الطلب هي ضابط أمن المعلومات على أن تعتمد هذه الموافقة عمادة الاتصالات وتقنية المعلومات. ويجب أن يشتمل كل طلب استثناء على المبررات والمزايا المنسوبة إلى الاستثناء من الامتثال للسياسة.

تبلغ فترة الاستثناء من الامتثال للسياسة أربعة أشهر كحد أقصى، ويجب إعادة تقييم هذه المدة واعتماد تمديدها- إذا لزم الأمر- لمدة أقصاها ثلاث فترات متتالية. ولا يجوز الاستثناء من هذه السياسة لأكثر من ثلاث فترات متتالية.

الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات
- سياسة أمن الموارد البشرية

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

- سياسة التحكم في الوصول
- سياسة الامتثال
- سياسة كلمة المرور

الملكية

هذه الوثيقة مملوكة لعمادة الاتصالات وتقنية المعلومات بجامعة الإمام عبد الرحمن بن فيصل وهي التي تحافظ عليها.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

بيانات السياسة

يجوز لأعضاء الجامعة المعتمدين والأطراف الخارجية المعتمدة (المقاولون، إلخ ...) الاستفادة من مزايا الشبكات الخاصة الافتراضية التي تعتبر خدمة "يديرها المستخدم". هذا يعني أن المستخدم مسؤول عن اختيار مزود خدمة الإنترنت (ISP)، وتنسيق التثبيت، وتثبيت أي برمجية مطلوبة ودفع الرسوم المرتبطة بذلك.

بالإضافة إلى ذلك لابد من مراعاة الأشياء التالية:

1. للحصول على إذن للوصول إلى شبكة الجامعة عبر الشبكة الافتراضية الخاصة، يجب أن يوافق مجلس إدارة عمادة الاتصالات وتقنية المعلومات على طلب التغيير الذي يجب أن يوضح فيه المبررات التي دعت إليه والبريد الإلكتروني وتفاصيل الاتصال بالمستخدمين، والموارد اللازمة للوصول (بما في ذلك عناوين بروتكول الانترنت ورقم المنفذ) ومدة الوصول المطلوبة.

2. تقع على عاتق المستخدمين ذوي امتيازات الشبكة الافتراضية الخاصة ضمان عدم السماح للمستخدمين غير المصرح لهم بالوصول إلى الشبكات الداخلية للجامعة.

3. يتم التحكم في استخدام الشبكة الافتراضية الخاصة إما بالتحقق من كلمة المرور لمرة واحدة واستخدام هذه الكلمة أداة تمييز أو باستخدام نظام مفتاح عام أو خاص بعبارة مرور قوية.

4. عند الاتصال النشط بشبكة الجامعة، ستجبر الشبكات الافتراضية الخاصة كل حركة المرور من الحاسب الشخصي وإليه على أن تسلك نفق الشبكة الافتراضية الخاصة مما يعني أن جميع حركات المرور الأخرى سيتم اسقاطها.

5. لا يُسمح بعمل أنفاق مزدوجة (تقسيم النفق) إذ إن المسموح به هو الاتصال بشبكة واحدة فقط ولا يستثنى من ذلك إلا الطلبات التي تقدم عبر مجلس عمادة الاتصالات وتقنية المعلومات ويعتمدها عميد العمادة.

6. تنشئ شبكة الجامعة وفرق الأمن بالجامعة بوابات للشبكة الافتراضية الخاصة وتقوم بإدارتها.

7. على جميع أجهزة الحاسب المتصلة بالشبكات الداخلية للجامعة عبر الشبكة الافتراضية الخاصة أو أي تقنية أخرى أن تستخدم أحدث البرمجيات لمكافحة الفيروسات؛ وهذا المطلب يشمل أجهزة الحاسب الشخصية.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

8. سيتم فصل مستخدمي الشبكة الافتراضية الخاصة تلقائيًا عن شبكة الجامعة بعد 15 دقيقة من التوقف عن النشاط. فإذا أراد المستخدم أن يستأنف نشاطه بعد ذلك عليه أن يتصل بالشبكة عبر إعادة تسجيل الدخول. ولا يسمح باستخدام فاحص الاتصال (Ping) أو العمليات الاصطناعية الأخرى للإبقاء على الاتصال بالشبكة.

9. لا تزيد مدة تشغيل مكثف الشبكة الافتراضية الخاصة على 72 ساعة أو الوقت الذي يحدده مجلس إدارة عمادة الاتصالات وتقنية المعلومات.

10. يجب على المستخدمين ضبط أجهزتهم لتتوافق مع سياسات شبكة الجامعة الافتراضية الخاصة وشبكتها العامة.

11. يتعين على المستخدمين تنزيل برمجية عميل الشبكة الافتراضية الخاصة من بوابة شبكة الجامعة الافتراضية الخاصة من أجل تنشيط حساباتهم في الشبكة الافتراضية الخاصة.

12. أي استثناء من هذه السياسة يجب أن يعتمده مجلس إدارة عمادة الاتصالات وتقنية المعلومات مقدما.

13. سيتم تقديم الدعم فقط لعملاء الشبكة الافتراضية الخاصة المعتمدين من قبل خدمات تقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل.

14. قد يتعرض المستخدمون الذين يكتشف انتهاكهم لسياسة الوصول عبر الشبكة الافتراضية الخاصة إلى فقدان امتيازات الخدمات وربما يخضعوا لإجراءات تأديبية.

15. على مجلس إدارة عمادة الاتصالات وتقنية المعلومات مراجعة هذه السياسة وتعديلها بشكل دوري.

16. للاستفسار عن أي شيء يتعلق باستخدام شبكة الجامعة الافتراضية الخاصة، يرجى الاتصال بمكتب الدعم الفني التابع لعمادة الاتصالات وتقنية المعلومات.

----------نهاية الوثيقة----------

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©