سياسة إدارة أمن الشبكات والاتصالات

الأصدر ١,٠

تفاصيل الوثيقة

العنصر	الوصف		
عنوان الوثيقة	سياسة إدارة أمن الشبكات والاتصالات		
التصنيف الأمني	داخلي		
الحالة	تحت المراجعة	تاريخ المراجعة القادمة	٢٠٢١-٠١-٢٠
موقع التخزين	سيتم تحديده		
تاريخ الإصدار	٢٠٢٠-٠١-٢٠		
الاسم المرجعي	IU-POL-AU-001		
مالك الوثيقة	قسم امن المعلومات		

تحرير الوثيقة

رقم الإصدار	التاريخ	مبررات التحديث	ملخص التحديث
الأول	٢٠٢٠-٠١-٢٠	الإصدار الأول من الوثيقة	
الثاني			

المراجعة والاعتماد

	توقيع / اسم	المنصب الوظيفي	الإصدار	التاريخ
إعداد	فريق ابتكار	مستشار الأمن	الأول	٢٠٢٠-٠١-٢٠
رؤجع بواسطة				
اعتمدها				

يعتمد
عميد تقنية المعلومات
د. سامي بن سعد البوق

المحتويات

١. الهدف

الغرض من هذه السياسة هو مساعدة الجامعة الإسلامية على وضع مبادئ توجيهية لبناء الأمن في البنية التحتية لشبكتها.

٢. النطاق

تنطبق هذه السياسة على جميع مستخدمي أصول المعلومات، بما في ذلك الموظفون المؤقتون والدائمون، وموظفو وكالات التوظيف المؤقتة، والاستشاريون، المقاولون، والأطراف الثالثة والموردون، الجهات الخارجية التي تستخدم المعلومات و / أو المرافق التي تملكها الجامعة الإسلامية، بغض النظر عن الموقع الجغرافي.

تشمل هذه السياسة جميع الأنظمة والأصول المعلوماتية بالجامعة الإسلامية، سواء أكانت تُدار من قبل العمادة أو من قبل طرف ثالث

٣. إدارة السياسات

ستستلزم التطورات التقنية والتغييرات في متطلبات الأعمال إجراء تعديلات دورية للسياسات. لذلك، قد يتم تحديث هذه السياسة لتعكس التغييرات أو تحديد متطلبات جديدة أو محسنة. وترسل على الفور أوجه القصور في هذه السياسة إلى إدارة أمن المعلومات. تتطلب تغييرات السياسة موافقة عميد تقنية المعلومات. يجب أن تبقى سجلات التغيير حديثة وسيتم تحديثها بمجرد إجراء أي تغيير.

٤. الأدواروالمسؤوليات

- راعي هذه السياسة هو عميد تقنية المعلومات.
- قسم أمن المعلومات مسؤول عن صيانة ودقة السياسة.
- المديرون المباشرون مسؤولون عن تنفيذ هذه السياسة داخل إداراتهم.
- قسم أمن المعلومات لديه سلطة التحقق من الالتزام لهذه السياسة من قبل جميع موظفي عمادة تقنية المعلومات وكذلك المقاولين والاستشاريين والأطراف الثالثة وسلسلة التوريد التابعة لطرف ثالث وأي موظفين مؤقتين لديهم إمكانية الوصول إلى أصول المعلومات
- يجب توجيه أي أسئلة بخصوص هذه السياسة إلى قسم أمن المعلومات.

استناداً إلى الهيكل التنظيمي لعمادة تقنية المعلومات، فيما يلي قائمة بالأدواروالمسؤوليات المرتبطة بها تجاه هذه السياسة.

عميد تقنية المعلومات في الجامعة الإسلامية

- فرض سياسات الأمان داخل بيئة عمادة تقنية المعلومات لحماية أصول ونظم المعلومات الهامة.
- التأكد من أن السياسات متوافقة مع المتطلبات القانونية والتعاقدية لعمادة تقنية المعلومات.
- الموافقة على أنظمة المعلومات المستخدمة لمعالجة المعلومات الحساسة أو تخزينها أو طباعتها .
- الموافقة على السياسات الجديدة أو التعديلات على السياسات المطبقة.

مدير أمن المعلومات

- توزيع وثائق أمن المعلومات بحيث يكون لدى أولئك الذين يحتاجون إلى هذه الوثائق نسخ أو يمكنهم تحديد موقع الوثائق بسهولة عبر الموقع الداخلي.
- ضمان حماية نظم المعلومات/ البنية التحتية، وفقاً للآليات التكنولوجية التي يحددها فريق تصميم النظام
- تنفيذ الضوابط المناسبة لحماية سرية المعلومات الحساسة وسلامتها وتوفرها عند الحاجة .
- تحديد سياسات وإجراءات أمن المعلومات والحفاظ عليها.
- تنسيق الاستجابة للانتهاكات والاختراقات المتعلقة بالأنظمة
- التحقيق في اختراقات الضوابط الأمنية وتنفيذ ضوابط تعويض إضافية عند الضرورة.
- الإشراف والتنسيق مع قسم تقنية المعلومات للتأكد من أن التدابير الأمنية المنفذة تفي بمتطلبات السياسة الأمنية.

رؤساء الأقسام والإدارات

- رؤساء أقسام عمادة تقنية المعلومات مسؤولون عن تنفيذ ومراقبة هذه السياسة داخل إداراتهم

مستخدمي المعلومات

- الالتزام بالسياسات والإرشادات والإجراءات الأمنية المتعلقة بحماية البيانات الحساسة.
- الإبلاغ عن نقاط الضعف المتعلقة بسرية أو سلامة أو توفر البيانات الحساسة إلى إدارة تقنية المعلومات/ موظف أمن المعلومات.
- استخدام المعلومات للأغراض المقصودة والمحددة في عمادة تقنية المعلومات

٥. الالتزام

- الالتزام بهذه السياسة إلزامي، ويجب على رؤساء اقسام عمادة تقنية المعلومات ضمان مراقبة الالتزام المستمر.
- الالتزام ببنود هذه السياسة هو مسألة مراجعة دورية من قبل إدارة أمن المعلومات.
- أي مخالفة سوف تؤدي إلى اتخاذ إجراءات تأديبية من قبل عميد تقنية المعلومات.
- وتستند الإجراءات التأديبية إلى شدة الانتهاك الذي ستحدده التحقيقات.
- تتخذ إجراءات تأديبية مثل إنهاء الخدمة أو فقدان امتيازات الوصول إلى أصول المعلومات أو غيرها من العقوبات حسبما تراه الجامعة وإدارة شؤون الموظفين مناسبا.

٦. الاستثناءات

- تهدف هذه السياسة إلى معالجة متطلبات أمن المعلومات. وإذا لزم الأمر، يمكن تقديم الاستثناءات رسميا إلى إدارة أمن المعلومات، بما في ذلك التبرير والفوائد المنسوبة إلى الاستثناء، ويجب أن يوافق عليها مدير أمن المعلومات.
- ومدة الاستثناء من السياسة العامة هي سنة واحدة كحد أقصى، ويمكن إعادة تقييمها وإعادة الموافقة عليها، إذا لزم الأمر، لثلاث فترات متتالية كحد أقصى. ولا ينبغي منح أي سياسة استثناء لأكثر من ثلاث فترات متتالية.

٧. المراجع المعيارية

- ضوابط الأمن السيبراني الأساسية NCA_ECC-1:2018
- ISO 27001:2013 نظام إدارة أمن المعلومات

٨. بنود السياسة

إدارة أمن الشبكة

٨,١. يجب على قسم تقنية المعلومات تنفيذ التدابير والضوابط المناسبة لأمان الشبكة، من خلال(جدار الحماية ، نظام كشف التسلل ، إلخ)لحماية البنية التحتية للشبكة والنظام وللحفاظ على الأمن للأنظمة والتطبيقات التي تستخدم الشبكة ، بما في ذلك المعلومات أثناء النقل .

٨,٢. يجب تطبيق ضوابط تقنية كافية لحماية الأنظمة المتصلة، ولحماية سرية وسلامة المعلومات الهامة التي تمر عبر الشبكات العامة ليتم تأمينها من خلال التقنيات المناسبة.

٨,٣. يجب تحديد ميزات الأمان ومستويات الخدمة ومتطلبات الإدارة لجميع خدمات الشبكة وإدراجها في أي اتفاقية ، سواء تم توفير هذه الخدمات داخل الجامعة الإسلامية أو أثناء الاستعانة بمصادر خارجية.

٨,٤. يجب على جميع نقاط الوصول اللاسلكي أن توفر القدرة على مصادقة المستخدمين قبل السماح لهم بالوصول إلى شبكة الجامعة.

٨,٥. يجب تقييد الوصول إلى بيانات وموارد الشبكة اللاسلكية المحلية، ما لم يتم التصريح بذلك.

٨,٦. يجب تعطيل مشاركة الملفات على أجهزة الكمبيوتر المتصلة عبر وسائط غير موثوق بها.

٨,٧. يجب تشفير كل حركة المرور بين الشبكة اللاسلكية المحلية ويستخدم المسؤول بروتوكولات WPA أو WPA2. يحظر استخدام بروتوكول WEP.

٨,٨. يجب أن تكون إدارة نقاط الوصول من خلال المتصفح من إدارات معرفة مسبقًا يتم التحكم فيها بواسطة قوائم الوصول.

٨,٩. تتم إدارة جميع نقاط الوصول اللاسلكية، إذا تم نشرها، بواسطة نظام التحكم اللاسلكي.

٨,١٠. لا يمكن لغير العاملين بالجامعة الإسلامية الوصول إلى الشبكة اللاسلكية المحلية دون موافقة قسم تقنية المعلومات.

٨,١١. يجب تغيير اسم الشبكة من الإعدادات الافتراضية إلى اسم بلا معني بالنسبة للغرباء. وألا يكون ذو دلالة لأسماء عامة او مواقع أو المنتج الذي يُستخدم.

٨,١٢. يتم فحص الشبكة اللاسلكية للجامعة، إذا تم نشرها، بواسطة قسم تقنية المعلومات مرة واحدة على الأقل كل ثلاثة أشهر.

٨,١٣. يجب تثبيت ونشر جميع نقاط الوصول بطريقة آمنة. أيضًا يجب أن يتم الالتزام بجميع متطلبات الأمان السيبراني المنصوص عليها في هذه السياسة وجميع الإجراءات والمعايير ذات الصلة.

٨,١٤. يجب أن يكون لدى جميع أنظمة شبكات الجامعة والأجهزة والخوادم مزود طاقة غير منقطع في حالة انقطاع التيار الكهربائي الرئيسي.

٨,١٥. يجب أن يستخدم قسم تكنولوجيا المعلومات اثنين على الأقل من خوادم DNS تجنباً للفشل.

٨,١٦. يجب على قسم تكنولوجيا المعلومات تثبيت إعدادات DNS على أجهزة الشبكة.

٨,١٧. يجب أن تكون جميع خوادم DNS (الداخلية أو الموجودة بمنطقة DMZ) مثبت عليها برنامج مكافحة البرامج الضارة مع المراقبة والتنبيه فعلياً للأنشطة غير الطبيعية وأيضًا تثبيتها بأحدث برامج مكافحة الفيروسات وتحديث أنماط الفيروسات بشكل منتظم.

٨,١٨. يجب على الجامعة الاستفادة من عوامل تصفية خوادم البروكسي المستندة إلى http وخوادم البروكسي المعتمدة علي التطبيقات أو خوادم البروكسي العكسية لحماية التطبيقات من المدخلات غير المرغوب بها.

٨,١٩. يجب على جميع خوادم البروكسي الموجودة في منطقة DMZ الداخلية إجراء الترجمة بواسطة خوادم DNS الداخلية.

٨,٢٠. يجب على جميع خوادم البروكسي الموجودة في منطقة DMZ الخارجية إجراء الترجمة بواسطة خوادم DNS خارجية.

٨,٢١. يجب تثبيت برامج مكافحة الفيروسات وبرامج مكافحة التجسس المرخصة على خادم البروكسي و يُحدث بانتظام.

٨,٢٢. تتم تصفية الإنترنت باستخدام تطبيق تصفية محتوى الويب الذي يعمل بالتزامن مع خادم (خوادم) البروكسي.

٨,٢٣. يجب أن تحتوي جميع خوادم تصفية محتوى الويب على برنامج مثبت لمكافحة البرامج الضارة، مع المراقبة والتنبيه فعلياً للأنشطة غير الطبيعية.

أمان خدمات الشبكة

٨,٢٤. يجب تعريف اتفاقية لخدمات الشبكة المقدمة داخليا أو من خلال جهات أخرى ويجب أن تشمل ميزات الأمان ومتطلبات الإدارة ومستويات الخدمة.

٨,٢٥. يجب إجراء تقييمات دورية للثغرات على جميع أنظمة شبكات **الجامعة** والأجهزة والخوادم بشكل منتظم

التحكم في الوصول إلى الشبكة

سياسة استخدام خدمات الشبكة

٨,٢٦. يجب أن يكون الوصول إلى الشبكات وخدماتها مصرحًا به على وجه التحديد وفقًا لسياسات إدارة الهوية وإدارة الأصول بالجامعة والإجراءات المرتبطة بها .

٨,٢٧. يجب التحكم في الوصول إلى الشبكات وخدماتها على أساس متطلبات العمل والأمن، ومبدأ " الوصول على قدر الحاجة" وقواعد التحكم في الوصول المحددة لكل شبكة.

٨,٢٨. يقتصر الوصول إلى أجهزة وبرامج الشبكات على الموظفين المصرح لهم بشكل صحيح.

٨,٢٩. يقتصر الوصول إلى أجهزة الشبكة القابلة للبرمجة (مثل المبدل والموزع والجدار الناري) على الشخص المصرح له فقط.

٨,٣٠. يقتصر استخدام أدوات تشخيص الشبكة والحماية على الموظفين المعينين خصيصًا، ووفقًا لمسؤوليات وظيفتهم.

٨,٣١. يقتصر الوصول إلى جميع إعدادات الشبكة والبيانات المتعلقة بالأمان (مثل أرقام الطلب الهاتفي وعناوين الIP) للمستخدمين المصرح لهم.

٨,٣٢. يجب تهيئة نظام مراقبة الشبكة (NMS) للتنبيه في الوقت الفعلي.

مصادقة المستخدم للاتصالات الخارجية

٨,٣٣. يخضع وصول المستخدم عن بُعد إلى شبكات **الجامعة** لطرق معتمدة من قبل الجامعة.

٨,٣٤. على جميع اتصالات VPN استخدام بروتوكولات آمنة مثل IPSec و SSL VPN ، إلخ.

٨,٣٥. يجب استخدام AES أو خوارزميات تشفير أقوى لإنشاء اتصالات VPN.

٨,٣٦. يجب مزامنة جميع مركزات VPN مع خوادم وقت محددة.

٨,٣٧. يجب وضع جميع مركزات VPN في منطقة DMZ الخارجية.

٨,٣٨. يجب ان يكون لمركزات VPN القدرة علي مصادقة المستخدمين قبل السماح بالوصول إلى الموارد المحمية بواسطة الأنظمة والسماح للمستخدم بالوصول إلى أنظمة أو تطبيقات محددة بناءً على احتياجات العمل.

٨,٣٩. يُمنح الوصول إلى شبكة الجامعة للمستخدمين عن بعد عبر مركز VPN باستخدام رموز آمنة أو مصادقة كلمة المرور لمرة واحدة أو نظام مفتاح عام / خاص مع كلمات مرور قوية.

تحديد المعدات في الشبكات

٨,٤٠. يجب على قسم تكنولوجيا المعلومات تحديد جميع معدات الشبكات بأسماء فردية والاحتفاظ بسجل لجميع معدات الشبكات إلى جانب موقع الجهاز والغرض منه. يجب أن يكون هذا جزءًا من سجل الأصول الشامل الذي تحتفظ به إدارة تكنولوجيا المعلومات.

٨,٤١. يعتبر التعرف التلقائي على المعدات وسيلة لتوثيق الاتصالات من مواقع ومعدات محددة.

٨,٤٢. يجب فهرسة خطوط الاتصالات السلكية (مثل خطوط الشبكة وخطوط الهاتف وما إلى ذلك) وتحديدها بشكل فريد للنظام الذي يتم الوصول إليه لتسهيل الصيانة والأمان. يجب توثيق وصيانة جميع الخطوط مع قدرتها من قبل فريق تكنولوجيا المعلومات.

٨,٤٣. يجب على قسم تكنولوجيا المعلومات أيضًا الاحتفاظ برسم مُحدث للشبكة. يجب إجراء المراجعات الدورية بواسطة إدارة امن المعلومات لضمان تحديث المخطط لتعكس بنية الشبكة الحالية .يجب تحديث مخططات الشبكة عند حدوث تغييرات في بنية الشبكة.

٨,٤٤. يجب أن يحتوي مخطط الشبكة على التفاصيل التالية:

أ. مخططات مستوى متعددة من شبكة WAN إلى قطاع LAN

ب. المستوى الاول WAN

ت. المستوى الثاني LAN

ث. المستوى الثالث- قطاعات LAN

ج. جميع معدات الشبكات مع عناوين IP الخاصة بهم

ح. جميع روابط الاتصالات (الابتدائية والاحتياطية) مع عرض النطاق الترددي ونوع البيانات الذي يستخدم الخط فيه (الصوت / البيانات)

خ. يجب وضع آليات تحكم مناسبة لإصدار مخطط الشبكة

٨,٤٥. يضمن قسم تكنولوجيا المعلومات ما يلي:

أ. إجراء مصادقة المعدات في طبقة التطبيق أو طبقة الشبكة بحسب نموذج OSI

ب. استخدام الإصدار الثالث من بروتوكول إدارة الشبكات البسيطة (SNMP) إن أمكن وبروتوكولات إدارة الشبكات الأخرى لتحديد معدات الشبكة ومراقبتها.

ت. يتم تهيئة مجال أو مقطع SNMP وفقًا للتجزئة المطلوبة لتجميع معدات الشبكات لسهولة الإدارة والمراقبة، وأيضًا للحماية من التعرض لنطاقات البروتوكول الافتراضية.

التشخيص عن بعد وحماية نو افذ التهيئة

٨,٤٦. يجب دائمًا التأمين والتحكم في كل اتصال عن بُعد للصيانة والدعم والخدمات الخاصة (مثل الإدارة)

٨,٤٧. رئيس قسم تقنية المعلومات هو المسؤل عن تفويض أفراد دعم معينين للوصول إلى منافذ التشخيص والتكوين .يجب توفير هذه الاتصال فقط عند الحاجه .بعد الاستخدام يجب تعطيله

الفصل بين الشبكات (ISO 27001 A.13.1.3)

٨,٤٨. يجب تقسيم شبكة نظم المعلومات إلى مقاطع منطقية بناءً على متطلبات الوصول .يجب أن تأخذ معايير تقسيم الشبكات في الاعتبار التأثير النسبي للتكلفة والأداء لدمج التكنولوجيا المناسبة

٨,٤٩. يجب فصل الشبكة الداخلية عن الشبكة الخارجية مع وجود ضوابط أمنية مختلفة للمحيط على كل شبكة من الشبكات

٨,٥٠. يجب التحكم بإحكام في الاتصال بين الشبكات الداخلية والخارجية

التحكم في اتصال الشبكة

٨,٥١. تقتصر قدرة المستخدمين على الاتصال بالشبكات المشتركة وخصوصا تلك الممتدة عبر حدود **الجامعة** ، تمشيا مع إدارة الهوية وسياسة إدارة الوصول ومتطلبات تطبيقات الأعمال

٨,٥٢. يجب صياغة جدول سياسة خدمة الشبكة لكل خدمة مسموح بها من خلال كل جدار حماية. يجب أن يسرد الجدول الخدمة ، واتجاه الخدمة ، ومخاطر العمل المرتبطة بالسماح بالخدمة ، ومبرر العمل للسماح بالخدمة. تكون إدارة الأمن السيبراني مسؤولة عن الموافقة على جدول سياسة خدمة الشبكة النهائي

٨,٥٣. يجب تزويد المستخدمين فقط بوصول مباشر إلى الخدمات التي أذن لهم باستخدامها فقط

التحكم في توجيه الشبكة

٨,٥٤. كل مرور عبر الموجه يُعتمد من رئيس قسم تقنية المعلومات بناءً على احتياجات الاتصالات وبالتنسيق مع مالكيها

٨,٥٥. يجب نشر آليات التحكم في التوجيه المناسبة لتقييد اتصالات الكمبيوتر ولا تنتهك تدفق المعلومات سياسة إدارة الهوية والوصول لتطبيقات الأعمال

٨,٥٦. يضمن توجيه الشبكة من بوابة المستخدم إلى وجهة الإنترانت الخاصة بالمستخدم (المكاتب المحلية / البعيدة) بقاء حركة مرور شبكة المستخدم ضمن نفس قطاع الشبكة الذي أذن للمستخدم باستخدامه، لضوابط لتحقيق ذلك تشمل على سبيل المثال لا الحصر:

أ. تعطيل التجوال غير المحدود للشبكة (سيكون للمستخدم حق الوصول إلى شبكة محلية محددة ما لم يُصرح بذلك)

ب. شبكات محلية منطقية لعزل قطاعات الشبكة وتنفيذ البوابات (أجهزة التوجيه وجدران الحماية).

ت. مسار معرف مسبقا لشبكة المستخدم ، لمنع أي تدخل للمستخدم والقضاء على فرصة لاستكشاف الشبكة

ث. تنفذ **الجامعة** تدابير محددة لحماية أنظمة مواجهة الويب من هجمات الحرمان المتعمد من الخدمة .سوف تشمل هذه التدابير عادة الخدمات غير الضرورية

جدار الحماية

٨,٥٧. تنشر **الجامعة** تقنيات جدار الحماية المعترف بها دوليًا عند كل تقاطع بين شبكاتها وشبكاتها العامة أو الخارجية

٨,٥٨. يجب تكوين جدران الحماية على أساس جدول سياسة خدمة الشبكة الذي يغطي جميع الخدمات المسموح بها والتي تم التصريح بها على وجه التحديد

٨,٥٩. يجب على الإدارة ضمان ممارسة الإدارة المناسبة والإشراف الفني على هيكل جدار الحماية والتكوين الحالي ، ويتم تغطية ما يلي:

أ. يجب مراجعة قواعد جدار الحماية بشكل دوري (على الأقل كل ثلاثة أشهر) أو قبل التغييرات المهمة في بنية شبكة **الجامعة**

ب. يتم تسجيل وتوثيق إجراءات صيانة جدار الحماية والتغييرات التشغيلية والموافقة عليها من قبل الإدارة

ت. يتم اعتماد التغيير في قواعد جدار الحماية من خلال عملية رسمية، قبل التنفيذ

٨,٦٠. يجب تحديث ملف تكوين جدار الحماية بانتظام .يجب أن يتضمن ملف التكوين، على سبيل المثال لا الحصر قائمة بالخدمات المعتمدة والمنفذ ومبرر الأعمال ورقم الطلب التشغيلي وتاريخ ووقت التغيير ومدة التغيير .يجب تحديث ملف التكوين عند أي تغيير في تكوين جدار الحماية ؛ يجب الموافقة على كل تغيير والتحقق من صحته من خلال تبرير عملي صحيح وموافق عليه

٨,٦١. يجب تزويد المراجعين الداخليين / الخارجيين بنسخة من سجلات جدار الحماية عند الطلب بعد الحصول على موافقة إدارة الأمن السيبراني

التحكم في أنظمة كشف/منع التسلل

٨,٦٢. يجب نشر تقنيات منع اقتحام/كشف الشبكة أو أي تقنيات مماثلة في قطاعات الشبكة الخارجية

الأنظمة الوسيطة

٨,٦٣. أثناء تطوير التطبيقات بنظام الوسيطة ، يجب مراعاة الأمان أثناء تطوير مرحلة مواصفات المتطلبات في دورة حياة تطوير البرمجيات(SDLC)

٨,٦٤. يجب أن يكون جدار الحماية الخاص بتطبيقات الويب مطبقًا أمام تطبيقات الويب التي تواجه الجمهور للكشف عن الهجمات المستندة إلى الويب ومنعها

٨,٦٥. بالنسبة لتطبيقات الانترنت ، يجب إجراء المراجعة التلقائية أو اليدوية لكافة الأكواد أو التطبيقات التي تم تطويرها بالجامعة أو الاستعانة بمصادر خارجية اخرى من أجل تطويرها. يجب إجراء المسح والمراجعة من قبل طرف مستقل

٨,٦٦. يجب تحديد خدمات النظام والشبكة اللازمة لدعم الأنظمة الوسيطة في اتفاقيات الخدمة الموثقة ، مثل العقود أو اتفاقيات مستوى الخدمة

٨,٦٧. يقتصر الوصول الخارجي إلى الأنظمة الوسيطة من خلال:

أ. إخضاع المستخدمين الخارجيين لمصادقة قوية (مثل أجهزة التحدي / الاستجابة التي تضم كلمات مرور لمرة واحدة ، أو رموز أخرى)

ب. توجيه حركة المرور من خلال جدران الحماية

ت. منح الوصول فقط إلى أجزاء محددة من التطبيق / الخدمات

٨,٦٨. يجوز لأي أطراف أخرى تقديم الدعم عن بعد على الأنظمة الوسيطة بشرط الامتثال لإدارة الهوية وسياسة إدارة الوصول **بالجامعة**

٨,٦٩. يجب على الاطراف الاخرى التوقيع على اتفاقية عدم افشاء المعلومات لأي دخول أو دعم على الأنظمة الوسيطة

الاتصال الهاتفي عبر بروتوكول الإنترنت

٨,٧٠. يوفر النظام القدرة على مصادقة المستخدمين قبل السماح بالوصول إلى الموارد المحمية بواسطة الأنظمة

٨,٧١. يجب علي ملفات تعريف الدخول التي تسمح للمستخدم للحصول على امتياز إجراء المكالمات المحلية، المكالمات الوطنية، مكالمات GSM ، أن تكون وفقاً لإدارة الهوية وسياسة إدارة الوصول **بالجامعة**

٨,٧٢. إذا أمكن، يجب على المستخدم تقديم كلمة مرور / اسم مستخدم أو رمز PIN ، لاستخدام اتصال IP

٨,٧٣. تتم مصادقة المستخدم بعد مصادقة الهاتف على خادم إدارة المكالمات. (تمكين الخيار "تسجيل الخروج" عندما يكون الموظف في إجازة)

٨,٧٤. يقتصر الوصول إلى الرسائل المسجلة على المستخدمين المصرح لهم فقط

٨,٧٥. يجب الاحتفاظ بجميع سجلات نظام الاتصال الهاتفي عبر بروتوكول الإنترنت لـ "رفض الوصول" أو "المكالمات المسموح بها" أو "المكالمات المسقطة" أو "المكالمات المرفوضة" في مدير الاتصال

٨,٧٦. يجب تفعيل و تهيئة المراقبة الحية لنظام الاتصال الهاتفي عبر بروتوكول الإنترنت بطريقة آمنة

مصادقة المستخدم وتحديد الهوية

٨,٧٧. يجب مصادقة جميع المستخدمين مباشرة على وحدة التحكم أو من خلال جلسات Secure Shell (SSH)

٨,٧٨. يجب على جميع أجهزة تسجيل الدخول على جهاز التوجيه استخدام مصادقة كلمة المرور قبل السماح بالوصول لتقييد أي دخول مستخدم غير المصرح به. يجب تهيئة جهاز التوجيه لتشفير جميع كلمات مرور تسجيل الدخول

٨,٧٩. يجب تنفيذ إجراءات حقوق الوصول وضوابط كلمة المرور والامتيازات لإنشاء قائمة التحكم في الوصول ACL وتعديلها وصيانتها ومراجعتها. يجب الوصول إلى جداول جهاز التوجيه و ACL من أجهزة محددة على الشبكة ويجب السماح بالوصول فقط لمسؤول جهاز التوجيه / مسؤول النظام

٨,٨٠. يجب استخدام قوائم التحكم بالوصول الديناميكي فقط إذا كانت مدعومة من قبل حالة عمل قوية حيث يتيح ذلك الحدث الخارجي إنشاء فتحة في تدابير الأمان الخاصة بالرواتر. أثناء وجود هذا الرابط ، يصبح جهاز التوجيه عرضة لهجمات خداع IP. يجب أن يستخدم الوصول الديناميكي نظام تشفير على مستوى الارتباط بالجلسة

٨,٨١. يجب تعيين قائمة التحكم في الوصول على جهاز التوجيه باستخدام سياسات وإجراءات الأمان وقواعد التصفية المحددة في نظام جدار الحماية

٨,٨٢. تطبق **الجامعة** مهلة الجلسة لأجهزة الشبكة والأمان بعد فترات محددة من عدم نشاط المستخدم

استخدام الأدوات المساعدة للنظام (ISO 27001 A.9.4.4)

٨,٨٣. يجب تقييد و تحجيم استخدام الأداة المساعدة التي قد تتجاوز أنظمة التحكم في التطبيق

٨,٨٤. يجب استخدام أدوات تهيئة الشبكة التي يوفرها البائع أو أدوات الجهات الاخري للاتصال بالموجهات. لا ينبغي مطلقًا استخدام Telnet لإنشاء جلسات لأجهزة التوجيه وأي أجهزة شبكة.

٨,٨٥. يجب استخدام أدوات النظام المناسبة لرصد وإدارة استخدام عرض النطاق الترددي للوصلات الهامة

التطبيق والتحكم في الوصول إلى المعلومات

تقييد الوصول إلى المعلومات

٨,٨٦. يجب على قسم تكنولوجيا المعلومات تقييد الوصول إلى المعلومات للمستخدمين على أساس الحاجة إلى المعرفة .يجب أن تتم إدارة تكوين الشبكة لتقييد الوصول المتاح للمستخدمين الفرديين فقط إلى أصول المعلومات المسموح لهم باستخدامها

٨,٨٧. يجب أن تظهر لافتة تحذير تفيد بأن الوصول إلى النظام مخصص للأفراد المصرح لهم فقط قبل تسجيل الدخول إلى جميع الأنظمة والتطبيقات. يجب أن تعكس لافتة التحذير أيضًا التشريعات المحلية فيما يتعلق بعقوبات الوصول غير المصرح به

٨,٨٨. لا ينبغي أن يسمح لجميع الموظفين لتوصيل أي جهاز (مثل أجهزة الكمبيوتر الشخصية، وكمبيوتر محمول، ومعدات الشبكات، ومودم) إلى شبكة **الجامعة**، دون الحصول على الإذن المناسب والموافقة عليها

٨,٨٩. يجب تمكين مستويات محددة وكافية من مسارات التدقيق في أجهزة الشبكة والأمن ، استنادًا إلى أهمية البيانات

٨,٩٠. يجب ان تتأكد الجامعة من أن مسؤولي النظام ليس لديهم إذن لتعديل أوإلغاء سجلات أنشطتها الخاصة

٨,٩١. يجب أن يضمن قسم تكنولوجيا المعلومات تكوين جميع أنظمة التشغيل بالجامعة وخوادم التطبيقات وأجهزة المستخدم والأجهزة المتصلة بالشبكة والمكونات المدارة للإبلاغ عن معلومات تسجيل الأحداث المفصلة إلى خادم syslog مركزي.

٨,٩٢. يجب أن يكون لسلامة الملفات الهامة على الخوادم الهامة مراقبة وتنبيه في الوقت الفعلي للتغييرات غير المتوقعة

٨,٩٣. يجب تخزين جميع السجلات المتعلقة بتفاصيل تسجيل الدخول وكذلك جميع الهجمات الخبيثة بشكل آمن على الجهاز المخصص كنسخة غير متصلة بالإنترنت من خلال خادم السجلات (مثل خادم syslog).

٨,٩٤. يجب التأكد في الجامعة من أن جميع التغييرات، بما في ذلك الصيانة الطارئة الثغرات، المتعلقة بالبنية التحتية والتطبيقات ضمن بيئة الإنتاج يجب أن تدار رسميا في الطريقة التي تسيطر عليها. يجب تسجيل التغييرات (بما في ذلك الإجراءات والعمليات ومعلمات النظام والخدمة) وتقييمها والإذن بها قبل التنفيذ ومراجعتها مقابل النتائج المخططة بعد التنفيذ.

٨,٩٥. يجب الاحتفاظ بالنظام وأجهزة الشبكة والخوادم وسجلات خادم الويب لفترة مناسبة حسب متطلبات العمل

عزل النظام الحساس

٨,٩٦. يجب تصميم شبكات الجامعة الحاسوبية وتنفيذها بطريقة لضمان خدمات التطبيقات الحساسة و التطبيقات المطورة بالجامعة الموجودة في قطاع شبكي منفصل مع تصفية جدار الحماية ونظام كشف / منع التسلل و تفتيش جميع البيانات المتدفقة للداخل و الخارج