

2011

سياسات أمن المعلومات



Abuzar

National Information Center - Information
Security Department

5/20/2011

سياسات أمن المعلومات

النسخة الأولى



المحتويات

المقدمة

الجزء 1: السياسات العامه

١.٠ سياسة أمن المؤسسة

٢.٠ سياسة الإستخدام المتفق عليها

٣.٠ سياسة الوعي الأمني

الجزء 2: السياسات المفصلة

سياسة ملكية وحماية البيانات

٤.٠ سياسة حماية البيانات

٥.٠ سياسة وقاية المعلومات

سياسة البرامج المضادة للفيروسات والبرامج الخبيثة

٦.٠ سياسة مضاد الفيروسات

السياسات المتعلقة بالإنترنت

٧.٠ سياسة إستخدام الإنترنت

٨.٠ سياسة إستخدام البريد الإلكتروني

سياسات التحكم بالدخول

٩.٠ سياسة الدخول

١٠.٠ سياسة حماية كلمة السر

سياسات الشبكة

١١.٠ سياسة أمن الجدار الناري والموجهات

١٢.٠ سياسة أمن الإتصال الهاتفي

١٣.٠ سياسة الشبكة الافتراضية الخاصة (VPN)

١٤.٠ سياسة الإتصال الاسلكي

١٥.٠ سياسة الدخول عن بعد

سياسات تطوير البرمجيات

١٦.٠ سياسة توظيف وتطوير البرامج العامة

١٧.٠ سياسة تطوير برامج الشبكة العنكبوتية

سياسة الأمن المادي

١٨.٠ سياسة الأمن المادي العامة

١٩.٠ سياسة أمن مركز البيانات/غرفة المخدمات

٢٠.٠ سياسة وسائط التخزين الممغنطة

٢١.٠ سياسة أمن الخوادم

سياسات إدارة العمليات

٢٢.٠ سياسة إدارة التهيئة (Configuration)

٢٣.٠ سياسة إدارة التغيير (Updating)

٢٤.٠ سياسة المخرجات المطبوعة والتوزيع

سياسات إستمرارية العمل

٢٥.٠ سياسة إستمرارية العمل العامة

٢٦.٠ سياسة النسخ الإحتياطي والإستعادة (Backup & Recovery)

سياسات الموظفين والطرف الثالث

٢٧.٠ سياسة الموظفين

٢٨.٠ سياسة الطرف الثالث

المقدمة

تعتبر المعلومات ذات أهمية قصوى للمنظمات والشركات والدول وحماية هذه المعلومات أمر حيوي للحفاظ على أعمالنا. لذا ومن أجل ضمان سلامة هذه الممتلكات الفكرية، فإن سياسة أمن المعلومات مطلب لا غنى عنه لاي مؤسسة او وزارة . ونحن هنا نضع بين أيديكم سياسة أمن المعلومات، والذي يتناول أهم المخاوف المتعلقة بأمن المعلومات وقد حرصنا على ان يكون شامل بقدر الامكان بحيث يكون نموذج قومي تأخذ منه الوزارات والوحدات الحكومية بقدر حاجتها بما يتناسب وبنية انظمة معلوماتها الداخلية .

إن هذا الدليل مبني على أفضل الأساليب المجربة. وراعينا أن يكون مختصر، وموجز وبسيط. في خضم مشاغل الحياة اليومية، فإن الرسائل والتوجيهات يجب أن تكون موجّهة وذات هدف واضح. لذا ولهذا السبب، فإن السياسات في هذا الدليل تم وضعها بشكل مختصر وبحدود سطر أو إثنين، بما يسهل عملية إتباعها وفهمها.

هذه السياسات تعتبر وثيقة ادارية ذات التزامات قانونية لذا ينبغي مراجعة الصياغة القانونية بواسطة الادارة القانونية للمركز خصوصا في ما يتعلق بالعقوبات المترتبة على مخالفة لوائح السياسات الامنية.

آخذين بعين الاعتبار بأن دليل السياسة هذا قد تم تقسيمه إلى جزئين رئيسيين هما: السياسات العامة، والسياسات المفصلة.

الجزء 1: السياسات العامة. يتناول هذا القسم الأمن والحماية بشكل عام ودون الدخول في تفاصيل، ومكون من ثلاث سياسات:

- **سياسة أمن المؤسسة:** وهي السياسة التي توضع بواسطة الإدارة العليا، و تختص بالأمن بشكله العام والموسع. هذا ويعتبر المستهدف الأول والأساسي لهذه السياسة هم مديري الادارات بينما يعتبر باقي الموظفين في المؤسسة كمستهدف ثاني ثانوي.

● سياسة الإستخدام المتفق عليها : هذه الإستراتيجية تلخص كل المبادئ العامة المتفق عليها لافضل الأساليب في مجال حماية المعلومات. لذا فهي تحوي الحد الأدنى من الأساسيات التي يجب أن يعرفها جميع الموظفين.

● سياسة الوعي الأمني : وهنا مرة أخرى، هذه السياسة تشدد على مبدأ أن الأمن هو مسؤولية الجميع، وأن كل فرد في المؤسسة ملزم بالإطلاع والإلمام بمبادئ الأمن والسلامة وأن كل فرد ملزم بحضور الندوات والبرامج المتعلقة في مجال الأمن.

الجزء 2: السياسات التفصيلية : هذا الجزء يقسم سياسات وإستراتيجيات الأمن إلى عشرة أجزاء رئيسية: ملكية المعلومات، البرامج الخبيثة والمضادة، سياسات ذات الصلة بالإنترنت، الرقابة والتحكم بالوصول إلى المعلومات، سياسات إستخدام الشبكة، تطبيقات الشبكة العنكبوتية والقديمة، الأمن المادي، إدارة العمليات، سياسة إستمرارية العمل، و سياسات الموظفين والطرف الثالث. وكل جزء من هذه الأجزاء تم تقسيمه إلى سياسات إضافية والتي تتناول مجمل أمن المعلومات .

ختاماً نرجو ان تحظى هذه السياسات بمناقشات متعمقة للوصول لصيغة المثلى لسياسات امنية شاملة ومحكمة

مهندس ابوزر عثمان محمد

ع/ مدير دائرة امن المعلومات

الاحد 2011/5/22





الجزء الأول: السياسات العامه

سياسة أمن المؤسسة

الغرض

إن الهدف الأساسي من سياسة أمن المؤسسة هي تحديد المتطلبات والضوابط لأمن المؤسسة وذلك من خلال المنظور الشمولي للإدارة العليا.

المجال

إن المستهدف الأساسي لهذه السياسة هم مدراء الإدارات، بينما يعتبر باقي الموظفين في المؤسسة المعنية كمستهدف ثانوي لهذه السياسة.

السياسة

١.١ أمن وحماية المعلومات هو مسؤولية الجميع.

١.٢ جميع عمليات الوصول إلى موارد ومعلومات المؤسسة يجب أن تكون مبنية على أساس "الحاجة للمعرفة"

١.٣ يجب تعيين مسؤول لأمن المعلومات يقوم بتنسيق الجهود لتطبيق كل سياسات الأمن. هذا وفي حالة إقتضاء الضرورة فإنه يمكن لاحقاً تشكيل لجنة لأمن المعلومات

١.٤ يجب حماية المعلومات من ناحية السرية، والتكاملية وسلامة المحتوى، بالإضافة إلى ضمان إستمرارية توفرها، وذلك خلال جميع مراحل التعامل مع هذه المعلومات من تخزين ومعالجة او نقل، بغض النظر عن الوسائط أو الطرق المستخدمة في الحفظ و النقل.

١.٥ يجب تحديد وإتباع الأساليب المناسبة لحماية جميع المعدات الحيوية المتاحة بالمؤسسة (من أجهزة أو برامج أو معدات أو بيانات)

١.٦ يجب إعداد قائمة رسمية لحصر وتحديد جميع المعدات الموجودة في المؤسسة مع مراعاة حسن تصنيفها وعنونها بما يناسب مع طبيعة المواد وذلك ليسهل الرجوع إليها عند الحاجة.

١.٧ حقوق الموارد التي لم يتم منحها صريحاً، يجب أن تعتبر ممنوعة.

١.٨ يجب إتباع تدابير وضوابط خاصة في حالة نقل المعلومات خارج نطاق المؤسسة وذلك للحفاظ على سريتها.

١.٩ يجب إخضاع وفحص جميع البرامج المطورة بغرض الإستخدام أوالمستخدمة في المؤسسة لقواعد ومعايير أمن مناسبة وذلك قبل السماح بتداولها أو إستخدامها في بيئات العمل.

١.١٠ للمؤسسة الحق الكامل والمكفول لمراقبة حركة المعلومات وجميع الإتصالات بغض النظر عن الأدوات والوسائط المستخدمة في تداول المعلومات.

١.١١ جميع المعلومات المصنفة تحت بند " سرى للغاية" يجب إنشائها وإنجازها بطريقة ما بحيث يمنع الإطلاع أو إعادة الكتابة عليها.

١.١٢ ضرورة حماية الشبكة المحيطة بكل الوسائل المتاحة والمناسبة من برامج أو أجهزة .

١.١٣ يجب إخضاع الشبكة المحيطة والداخلية لعمليات المراقبة الملائمة وبشكل منتظم .

١.١٤ لتوفير الحماية للمؤسسة ضد التهديدات والمخاطر الشائعة، فإنه يتعين توفير آليات مناسبة للوقاية بما يشمل "مضادات الفيروسات، جدران نارية، ونظم تحري الإختراق والمجسات الأخرى".

١.١٥ يجب إدارة عمليات فحص دورية ومنتظمة للشبكة والخدمات ولجميع الآلات الأخرى المرتبطة بالشبكة، وذلك للتأكد من أن الشبكة مؤمنة ومحمية بشكل مناسب.

١.١٦ يجب إبلاغ مسؤول أمن المعلومات بأي محاولات لإختراق المعلومات أو تهديدات للأمن.

١.١٧ يجب التأكد من إستمرارية أعمال المؤسسة بإتخاذ التدابير المناسبة لذلك.

١.١٨ مسؤول أمن المعلومات يقع على عاتقه تنظيم برامج وندوات من شأنها رفع وتعزيز مستوى الوعي الأمني للمؤسسة.

١.١٩ يجب إستخدام الموارد المؤسسية المتاحة للأغراض الإدارية المعتمدة والموافق عليها فقط.

١.٢٠ يجب تطوير الإجراءات والتدابير التفصيلية المناسبة لتغطية مناطق العمل الهامة.

١.٢١ يعتبر توفير الحماية المادية المناسبة مسألة جوهرية يجب مراعاتها.

- ١.٢٢ يجب مراجعة وتنقيح وثيقة أمن المعلومات وبشكل دوري.
- ١.٢٣ سيتم فرض وتطبيق عقوبات تأديبية مناسبة تتراوح ما بين لفت النظر إلى إنهاء الخدمة وذلك بناءً على خطورة وطبيعة الانتهاك.
- ١.٢٤ يجب وضع الخطط والإجراءات المناسبة للتعامل مع المخاطر والحوادث والاعتداءات في حالة حدوثها.
- ١.٢٥ مسؤول أمن المعلومات يقع على عاتقه تعيين أشخاص في فريق الإستجابة لحوادث وأعطال الكمبيوتر، لديهم الكفاءة والقدرة على التعامل مع الحوادث والانتهاكات الأمنية في حالة التعرض لها.
- ١.٢٦ يجب أن يتم تبليغ مسؤول أمن المعلومات بجميع الحوادث والفشل والقصور الأمني. حيث سيتكفل تطبيق لوائح منظمة المقاييس الدولية (ISO) بمعالجة المسألة، وستأخذ الإجراءات والتدابير المناسبة لمنع تكرار ذلك في المستقبل.
- ١.٢٧ يجب أن يكون لفريق الإستجابة لحوادث وأعطال الكمبيوتر خطة للإستجابة لحالات طوارئ الكمبيوتر موثقة، على أن تحوي هذه الوثيقة كل الإجراءات الضروري إتخاذها في مثل هذه الحالات.
- ١.٢٨ يجب تنمية المهارات المناسبة للتعامل مع أي حوادث متعلقة بالأمن.
- ١.٢٩ يجب القيام بعمليات الفحص المناسبة وبشكل منتظم لضبط أي حالات ضعف أو قصور أمني، وذلك بإجراء إختبار الإختراق القياسي.
- ١.٣٠ يجب تدعيم وتقوية جميع النظم، وبخاصة نظم التشغيل، لمستوى قياسي متفق عليه.

١.٣١ يعتبر الأمن المادي ذو أهمية جوهرية لا يجب إغفالها، لذا فإن كل الجهود يجب ان تبذل لتدعيم البيئة المادية المحيطة ونقاط العبور المادية و المكاتب.

١.٣٢ يجب اتخاذ التدابير والمقاييس المناسبة لتأمين جميع معدات ومصادر وأسلاك الطاقة.

١.٣٣ ينبغي ضمان المحافظة على سرية المعدات عندما يتم تخزينها أو صيانتها خارج مباني المؤسسة.

١.٣٤ على كل الموظفين إرتداء الشارات التعريفية الخاصة بهم وذلك خلال تواجدهم في مباني المؤسسة.

١.٣٥ يمنع منعاً باتاً، مناقشة الأمور الخاصة بالمؤسسة في الأماكن العامة من مثل المصاعد او المقاهي.

١.٣٦ في نهاية أي إجتماع رسمي فإنه ينبغي مسح جميع الملاحظات المدونة على اللوح البيضاء والتخلص من جميع الأوراق والرسوم التوضيحية إن وجدت.

١.٣٧ ضرورة تطبيق سياسة "المكتب النظيف" في كل أنحاء المؤسسة المعنية.

١.٣٨ يحظر إستخدام أو تخزين الألعاب الإلكترونية على أجهزة وكمبيوترات المؤسسة.

١.٣٩ جميع إعلانات الأعمال والمساعدة يجب أن تخضع لمراجعة وتنقيح تام، كما يتوجب الا تتضمن هذه الإعلانات اي معلومات حساسة تخص المؤسسة أو أن تفشي أي خطط مستقبلية للمؤسسة.

١.٤٠ إذا كان يتعين على أحد موظفي المؤسسة تقديم ورقة علمية، أو إقامة عرض تقديمي أو إلقاء محاضرة في منتدى عام أو مؤتمر ما، فإن جميع أدوات ومواد العرض يجب أن تخضع لمراجعة دقيقة من قبل المدير المباشر للموظف وذلك قبل تقديم العرض.

١.٤١ يجب إجراء فحص سنوي للنظام وذلك لفحص التحكم بالأنظمة.

١.٤٢ يجب كتابة جميع ما يعرف بسجلات الأداء (أو سجلات النفاذ الى النظام) الهامة على أقراص ممغنطة تسمح بالقراءة فقط -ولا تسمح بإعادة الكتابة- وذلك لمنع أي محاولة لتغيير محتوى هذه السجلات. آخذين بعين الاعتبار أن هذه السجلات يجب أن تراجع بواسطة الأشخاص المفوضين فقط.

١.٤٣ يجب أن تحتوي جميع الوثائق في المؤسسة على صفحة لضبط الإصدار بالإضافة لتاريخ الوثيقة، هذا مع مراعاة أن تكون جميع صفحات الوثيقة مرقمة.

١.٤٤ العقوبات التأديبية ستطبق على أي إخلال أو تهاون بتطبيق السياسة الأمنية هذه.

١.٤٥ يجب القيام بعملية تحليل للحوادث وتقدير للمخاطر مناسبة لكل أنظمة العمل الحيوية، وذلك إما بواسطة مسؤول أمن المعلومات أو بالإستعانة بشركة متخصصة خارجية.

١.٤٦ يمكن وعند الحاجة لمشورة متخصصة، فإنه يمكن الإستعانة بشركة إستشارية خارجية للمساعدة.

١.٤٧ يجب أن تتوافق المؤسسة مع جميع المتطلبات القانونية والموضوعة بواسطة الحكومة ، وبأن موظفيها سوف لن يتورطوا بأي نشاط يعتبر غير شرعي بنظر القانون المحلي او الدولي.

التطبيق

في حالة الإخلال بنود هذه السياسة، فإن عقوبات تأديبية قد تصل إلى حد إنهاء الخدمة ستطبق على المخالف.

المسؤولية

هذه السياسة هي مسؤولية جميع الموظفين، ومديري الإدارات ومسؤول أمن المعلومات.



الغرض من سياسة الإستخدام المتفق عليها هو تعريف السلوك المقبول للموظف، والذي يعتبر ضرورياً لتحقيق سرية، وإستمرارية وسلامة كلاً من الأنظمة والمعدات والمعلومات.

المجال

المجال لهذه السياسة يغطي كل الموظفين الدائمين/ذوي العقود، والمستشارين و البائعين/الأطراف الثالثة المنسوب لهم أعمال تخص المؤسسة.

- ٢.١ أمن المعلومات هو مسؤولية الجميع اليومية، وعلى جميع موظفي المؤسسة إتباع سياسة الأمن كلاً حسب موقعه.
- ٢.٢ موارد المؤسسة مخصصة لإستخدام العمل ويجب أن تستخدم لهذا الغرض فقط.
- ٢.٣ بين الحين والآخر، سيقوم مسؤول أمن المعلومات المعين من قبل المؤسسة بنشر تعليمات وإرشادات وعلى الجميع الإلتزام بها.
- ٢.٤ يعتبر أي عذر للجهل بسياسة الأمن غير مقبول بتاتاً.
- ٢.٥ جميع المعلومات المخزنة والمتبادلة من خلال موارد المؤسسة تبقى ملكية خاصة بالمؤسسة، وللمؤسسة الحق الكامل المكفول بمراقبتها والتدقيق عليها.
- ٢.٦ جميع معلومات المؤسسة السرية يجب التعامل معها بسرية تامة، كما يمنع منعاً باتاً نسخ أو نقل هذه المعلومات إلا إذا لزم الأمر لشؤون المؤسسة.
- ٢.٧ يقع على عاتق الموظفين حماية كلمات السر والعبور الخاصة بهم، ولا يجدر بهم تشارك هذه المعلومات مع أي أحد كان.
- ٢.٨ يجب تغيير كلمة السر بما يتوافق مع سياسة كلمة السر.

٢.٩ يجب إن تحوي جميع أجهزة الحاسوب المكتبية والمحمولة على كلمة سر لحماية شاشة الحفظ، على أن تفعل هذه الشاشة بعد مدة لا تزيد عن 10 دقائق من عدم الإستخدام.

٢.١٠ جميع المعلومات الهامة والحساسة المخزنة على أجهزة الحاسوب المحمولة يجب أن تكون محمية بكلمة سر.

٢.١١ يجب تشغيل برنامج مكافح فيروسات محدث على جميع الأجهزة. ولا يسمح لأي موظف كان بتعطيل أو إيقاف محرك إستكشاف الفيروسات.

٢.١٢ يجب إتباع سياسة الإنترنت والبريد الإلكتروني وذلك عند إستخدام البريد الإلكتروني أو الإنترنت.

٢.١٣ يحظر النسخ الغير قانوني للبرامج.

٢.١٤ يحظر إستخدام موارد المؤسسة لإختبار أي برنامج وذلك لإحتمالية أن يكون هذا البرنامج معطل أو أن يكون خبيث بطبيعته. هذا ويستثنى من ذلك البرامج المراد إستخدامها لأغراض المؤسسة.

٢.١٥ أخذ الحيطة والحذر الشديدين عندما يتم إرسال معلومات ذات حساسية عالية بوساطة الفاكس. على أن تدار مثل هذه العمليات بحيث يراعى بأن الطرفين (المرسل والمستقبل) متواجدان عند آلتهم لحظة الإرسال.

٢.١٦ لايسمح لأي شخص بتصفح شبكة المؤسسة من كمبيوتره الشخصي أو من أي مورد آخر.

٢٠١٧ يمنع منعاً باتاً إستكشاف ومسح المنافذ والثغرات للحوادم الداخلية والخارجية، إلا إذا كان هذا العمل جزءاً من إختبار الإختراق الرسمي المجرى بواسطة المؤسسة، وباتخاذ التدابير المضادة المناسبة.

٢٠١٨ لا يسمح بتثبيت برامج إستكشاف الثغرات أو أي برامج أخرى مشابهة على أي حاسب آلي إلا في حالة استخدام مثل هذا البرامج بواسطة مدير النظام ولأغراض التقييم، على أن يتم إزالة هذه البرامج كلياً حالما تتم عملية التقييم.

التطبيق

في حالة خرق السياسة، فإنه سيتم تطبيق عقوبات تأديبية قد تصل إلى حد إنهاء الخدمة.

المسؤولية

جميع الموظفين.

سياسة الوعي الأمني

الغرض

الغرض من هذه السياسة هو إبقاء الموظفين مواكبين لتطورات سياسة الأمن والتي تتغير بسرعة مذهلة.

المجال

هذه السياسة لجميع الموظفين بغض النظر عن المراكز التي يشغلونها.

السياسة

٣٠١ سيقوم مسؤول أمن المعلومات بتنظيم ورشة عمل واحدة على الأقل سنوياً، وحضور كل الموظفين إلزامي.

٣٠٢ في حالة عدم حضور أي موظف لورشة العمل، فإنه سيتم إعلام المدير المختص بذلك.

٣٠٣ إذا دعت الحاجة، فإن مسؤول أمن المعلومات قد يلجأ للإستعانة بالنشرات والملصقات و/أو شاشة حفظ خاصة للوعي الأمني وذلك لزيادة أمن المعلومات.

٣.٤ سيتم إعطاء كل موظف جديد نشرة وكتيب توعوي للأمن، وستكون آخر صفحة من هذا الكتيب تعهد بالإلتزام بالسياسة الأمنية يتعين على الموظف التوقيع عليه.

٣.٥ يقع على عاتق كل فرد تطوير نفسه أو نفسها، وذلك بالإشتراك ببرنامج التدريب الأمني الذي تنظمه المؤسسة.

٣.٦ يجب إبلاغ مسؤول أمن المعلومات مباشرة بأي إنتهاك أو إستفسار يتعلق بأمن المعلومات.

٣.٧ سيكون الوعي بسياسة الأمن أحد المحاور التي يتم بموجبها تقييم الموظف.

التطبيق

في حالة خرق السياسة، فإنه سيتم تطبيق عقوبات تأديبية قد تصل إلى حد إنهاء الخدمة.

المسؤولية

كل الموظفين، وبخاصة مسؤول أمن المعلومات و مدير تكنولوجيا المعلومات.





الجزء الثاني: السياسات التفصيلية



سياسات ملكية وحماية البيانات

سياسة حماية المعلومات

الغرض

الغرض من هذه السياسة تطبيق ملكية البيانات المناسبة لأمن المعلومات. حيث يتعين أن يتم تحديد مالك البيانات بوضوح مع الواجبات والمسؤوليات المتعلقة به.

المجال

السياسة تنطبق على كل الموظفين اللذين يكونوا مسؤوليين عن التعامل أو إستخدام أو إمتلاك البيانات في ذلك الوقت.

السياسة

٤.١ يجب تحديد مالك البيانات لكل تطبيق، على أن يكون مالك البيانات هو الشخص الذي يترأس أو يقود الفريق. فعلى سبيل المثال: مدير قسم المالية ، وليس قسم تقنية المعلومات، يملك البيانات المالية. أما تقنية المعلومات فهو مجرد حارس أو مؤتمن على البيانات.

٤.٢ على مالك البيانات توصيل أهمية البيانات، ودرجة حساسيتها، والضوابط ومطالب المراقبة إلى متعهد البيانات.

٤.٣ لا يمكن لمتعهد البيانات التصرف بأي شكل من الأشكال بالبيانات دون الحصول على تصريح بذلك من مالك البيانات.

٤.٤ من مسؤوليات متعهد البيانات التأكد من أنه تم عمل نسخة احتياطية للبيانات وحفظت في مكان آمن.

٤.٥ سيتأكد متعهد البيانات من توافر الوقاية المناسبة للتعافي من أي كارثة.

٤.٦ ستكون المسؤولية على المستخدم التأكد من أن إستعادة البيانات، الغير محملة على الخادم أو الغير منسوخة احتياطياً بواسطة وسيلة النسخ الاحتياطي المشتركة، (على سبيل المثال: بيانات الكمبيوتر المحمول أو الكمبيوتر المكتبي الكبير) ، ممكنة في حالة فشل النظام أو توقف القرص الصلب.

٤.٧ سيقوم متعهد البيانات من التأكد من أن جميع الضوابط الكافية متوفرة، كما تحدد بواسطة مالك البيانات.

٤.٨ على متعهد البيانات الإحتفاظ بالوثائق لكل الأنشطة التي تتضمن بيانات المالك.

٤.٩ سيقوم متعهد البيانات بإعلام مالك البيانات بأي مخاطر أو عيوب تصيب البيانات بمجرد أن يتعرف عليهم.

التطبيق

في حالة خرق السياسة، فإنه سيتم تطبيق عقوبات تأديبية قد تصل إلى حد إنهاء الخدمة.

المسؤولية

مالك البيانات، متعهد البيانات ومسؤول أمن المعلومات ومدير تكنولوجيا المعلومات.



الغرض

هذه السياسة تتناول التحكم و الوقاية المناسبة للمعلومات المولدة والمخزنة والمنقولة في المؤسسة.

المجال

هذه السياسة تنطبق على كل أشكال المعلومات وذلك بغض النظر عن الوسط المستخدم في تخزينها أو نقلها.

السياسة

٥.١ مالك الكمبيوتر سيقدر معدل حفظ البيانات إحتياطياً، وذلك على اساس أهمية ومدة بقاء المعلومات.

٥.٢ يجب تحديد وتطبيق معدل النسخ الإحتياطي ومدة الإحتفاظ بالبيانات على خادم النسخ الإحتياطي المشترك، وذلك بالتنسيق بين كلا من: مالك البيانات ومدير تكنولوجيا المعلومات و مسؤول أمن المعلومات.

٥.٣ يجب التحقق من كل النسخ الإحتياطي للتأكد من أنه يمكن استعادتها.

٥.٤ ينصح وبشدة عمل النسخ الإحتياطي للبيانات والتطبيقات في الأجهزة المرحجة خارج الموقع ، على أن تتم على الأقل مرة كل أسبوعين.

٥.٥ يجب تجنب إستخدام الأقراص المرنة، وإستخدام أقراص مدمجة قابلة للقراءة فقط عند عمل نسخ إحتياطي للإعدادات والملفات الأخرى.

٥.٦ على مالك البيانات تحديد مدة الإبقاء على البيانات.

٥.٧ يمنع إستخدام برامج القرصنة أو أي برامج أخرى غير قانونية في المؤسسة.

٥.٨ يجب الحصول على التصريح المناسب من قبل رئيس القسم ومسؤول أمن المعلومات، وذلك قبل تثبيت أي برنامج مشترى من بائع أو متعهد خارجي

٥.٩ يجب الفصل بين برامج التطبيقات وبين البيانات للأغراض الأمنية.

٥.١٠ يجب إخضاع البرامج للتجربة في بيئة مخصصة لذلك، قبل نقلها للإستخدام في أجهزة الإنتاج.

٥.١١ يجب إتخاذ التدابير المناسبة من مثل: تثبيت برنامج مكافح فيروسات، جدران نارية، نظام تحري الإختراق والشمام وغيرها، وذلك لتصدي للتهديدات الأمنية الداخلية والخارجية.

التطبيق

في حالة خرق السياسة، فإنه سيتم تطبيق عقوبات تأديبية قد تصل إلى حد إنهاء الخدمة.

المسؤولية

جميع الموظفين، مدراء الادارات، و مسؤول أمن المعلومات.



سياسة مكافحة الفيروسات والبرامج الخبيثة



سياسة مكافحة الفيروسات

الغرض

هذه الوثيقة تفصل سياسة المؤسسة المتعلقة بالبرامج الخبيثة من مثل: الفيروسات والديدان وأحصنة طرواده وغيرها.

المجال

المجال لهذه السياسة يشمل كل وسائط الإتصال الإلكترونية بالإضافة لكل وسائط التخزين التي يمكن أن تتضرر، أو أن تخزن أو حتى أن تنشر البرامج الخبيثة.

السياسة

- ٦.١ يجب أن يتم تشغيل أحدث برنامج مكافحة فيروسات كما تقرره إدارة المؤسسة.
- ٦.٢ يجب عدم فتح البريد الإلكتروني والمتضمن مرفقات إذا كان قادم من جهة مشبوهة أو غير معروفة، كما ينبغي حذف مثل هذه الإيميلات من نظام البريد ومن سلة المحذوفات على السواء. ويمنع منعاً باتاً على أي شخص إعادة توجيه أي بريد إلكتروني يعتقد أنه من الممكن إحتوائه على فايروس.
- ٦.٣ جميع أوساط التخزين القابلة للنقل (من مثل القرص المرن وغيرها) يجب أن تخضع للتدقيق للتأكد من خلوها من الفيروسات وذلك قبل أن يتم إستخدامها.
- ٦.٤ يجب إلا يتم إستخدام أي برنامج قرصنة على الشبكة الداخلية للمنظمة.

٦.٥ في حالة إكتشاف فيروس، فإنه يتوجب إعلام مسؤول أمن المعلومات فوراً بذلك. حيث سيقوم مسؤول أمن المعلومات بتحري الأمر وسيأخذ الإجراءات المناسبة لتجنب هذا الحدث في المستقبل.

٦.٦ لا يسمح لأي مستخدم بالتخلص من أي فيروس إلا إذا صرح له بذلك من قبل مسؤول أمن المعلومات.

٦.٧ يجب أن يتم فك شيفرة جميع المواد المشفرة وأن يتم إخضاعها لفحص الفيروسات وذلك قبل إستخدامها.

٦.٨ يجب أن يحوي خادم الإيميل على برنامج مكافح للفيروسات مثبت، كما يجب أن يتم فحص جميع مرفق الإيميلات وذلك قبل إرسالها إلى صندوق بريد المستلم.

٦.٩ يجب أن تكون جميع التحديثات الخاصة ببرنامج مكافح الفيروسات تلقائية من الشبكة العنكبوتية أو من الخادم المركزي.

٦.١٠ يجب أن يتم تضمين برنامج مكافح الفيروسات بالمكونات التالية:

أ - جدار ناري شخصي.

ب - نظام تحري إختراق شخصي.

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

جميع الموظفين، ومدير تكنولوجيا المعلومات ومسؤول أمن المعلومات.



السياسات المتعلقة بالإنترنت



سياسة استخدام الإنترنت

الغرض

هذه الوثيقة تفصل سياسة المؤسسة المتعلقة بتصفح واستخدام الإنترنت.

المجال

المجال لهذه السياسة يستهدف جميع الموظفين بغض النظر عن موقعهم.

السياسة

٧.١ يسمح باستخدام اتصالات الإنترنت الرسمية فقط، ولا يسمح لأي شخص بالاتصال عن طريق مودم الحاسب الشخصي لما قد ينطوي عليه ذلك من فتح باب خلفي (ثغرة) غير آمن على المؤسسة.

٧.٢ سيتم تقديم خدمات الإنترنت فقط للموظفين اللذين يحتاجونها لحاجة العمل، ولا يسمح باستخدام الإنترنت للأغراض الشخصية.

٧.٣ عند إستخدام الإنترنت فإنه لا يسمح لأي شخص بقذف أو ملاحقة أو إزعاج أو تهديد أي شخص آخر، كما لا يسمح بإختراق أي حقوق قانونية محلية أو دولية.

٧.٤ لا يسمح لأي شخص رفع، أو إرسال، أو نشر، أو توزيع أي معلومات أو مواد غير ملائمة أو غير محتشمة أو فاحشة أو محرمة أو إنتهاكية أو تشهيرية على الإنترنت بإستخدام موارد المؤسسة.

٧.٥ لا يسمح لأي شخص بإستخدام موارد المؤسسة لتثبيت إعلانات شخصية أو لعرض أي سلع أو خدمات.

٧.٦ في حالة تحميل أي ملف بحجم أكبر من 3 ميجابايت، فإنه يتعين الحصول على موافقة مسبقة من المدير المباشر.

٧.٧ أي زيارة لأي مواقع غير لائقة أو ليس لها علاقة بالعمل، سيتم إعتبرها مخالفة خطيرة.

٧.٨ لا يسمح لأي شخص بإستخدام خدمات المحادثة من مثل الأم إس إن (شبكة مايكروسوفت) او الياهو أو آي إس كيو. وفي حالة ما دعت الضرورة لإستخدام أي من هذه الخدمات لغرض التواصل مع مستشار خارجي لحل مشكلة أو لهدف التباحث، فإنه يجب الحصول على موافقة مسبقة من قبل المدير المباشر.

٧.٩ لا يجب إستخدام خدمات الهاتف الإنترنتي أو المقابلة الإنترنتية لمناقشة معلومات عمل حساسة.

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

جميع الموظفين، ومدير تكنولوجيا المعلومات ومسؤول أمن المعلومات.



سياسة استخدام البريد الإلكتروني

الغرض

هذه الوثيقة تفصل سياسة المؤسسة المتعلقة باستخدام البريد الإلكتروني، بما يشمل وظائف الإستقبال، أو الرد أو إعادة الإرسال أو الرد التلقائي.

المجال

المجال لهذه الإتفاقية يشمل كل الموظفين الدائمين وذوي العقود المحدودة بغض النظر عن مركزهم في المؤسسة.

السياسة

٨.١ خدمة البريد الإلكتروني هي للإستخدام الرسمي فقط، وغير مسموح إطلاقاً إستخدام عنوان البريد الإلكتروني الممنوح للموظف من قبل المؤسسة لأي أغراض شخصية.

٨.٢ لا ينبغي استخدام أي خدمة بريد إلكتروني مجانية، لإستقبال أو إرسال معلومات متعلقة بشؤون العمل.

٨.٣ لا يمكن إضافة أي مجموعة إخبارية غير ذات صلة بالعمل للدليل عناوين البريد الإلكتروني لمنظمتك.

٨.٤ لا يجوز استخدام خدمة البريد الإلكتروني للمؤسسة لإرسال أي مزعج للمستخدمين الآخرين سواء أكانوا من داخل أو خارج المؤسسة.

٨.٥ لا ينبغي إرسال أي رسائل مؤذية أو مهينة، سواء داخل أو خارج المؤسسة.

٨.٦ غير مسموح لأي شخص بتمرير رسائل مسلسلة أو هرمية التوزيع بغرض الدعاية أو أي نوع من البريد الغير مرغوب فيه (spam) باستخدام البريد الإلكتروني المشترك.

٨.٧ لا يسمح بإرسال أي وثيقة سرية خاصة بالمؤسسة لأي شخص آخر، بما فيهم حساب بريدك المجاني الشخصي الآخر.

٨.٨ إذا ما احتاج الأمر إلى إرسال معلومات حساسة لشخص ما خارج المؤسسة، فإنه يجب أخذ التدابير المناسبة كما يحددها مسؤول أمن المعلومات.

٨.٩ لا يصرح باستخدام عنوان البريد الإلكتروني للمؤسسة عند التراسل مع مجموعات الأخبار، لما قد يقوم به هذا الأمر من إفشاء معلومات عن المؤسسة. ولكن وعلى أي حال، فإنه يمكن الإشتراك بمجموعات الأخبار ذات الصلة بالعمل، بشرط الحصول على الموافقة من المدير المعني.

٨.١٠ يجب عدم تشغيل برامج البريد الإلكتروني من مثل الآوت لوك " Outlook " بعد مغادرة الموظفين بنهاية يوم العمل، وذلك لإمكانية إساءة إستخدام هذه البرامج من قبل قراصنة الإنترنت.

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

جميع الموظفين، ومدير تكنولوجيا المعلومات ومسؤول أمن المعلومات.



سياسات التحكم بالعبور



سياسة تسجيل الدخول

الغرض

هذه الوثيقة تختص بسياسة المؤسسة المتعلقة بتسجيل الدخول إلى الأجهزة الهامة، كما أنها تناقش بالتفصيل المعايير المرتبطة بذلك.

المجال

المجال لهذه السياسة يتضمن كل عمليات الدخول إلى التطبيقات الهامة والخوادم ، وذلك بغض النظر عن نظم تشغيلهم.

السياسة

٩.١ يجب أن يمتلك كل مستخدم اسم دخول خاص وفريد بالإضافة إلى كلمة سر وذلك للوصول إلى أنظمة كمبيوتر المؤسسة.

٩.٢ كل شخص مسؤول عن اسم الدخول الممنوح له/ها.

٩.٣ يجب تعطيل اسم الدخول بعد ثلاث محاولات فاشلة، على أن يتم إعادة تفعيل الاسم بعد طلب ذلك من مدير النظام.

٩.٤ يجب أن لا تكون كلمة السر مقروءة من على الشاشة.

- ٩.٥ في حالة ما تم إدخال اسم دخول أو كلمة سر غير صحيحان فإنه لا يجب إعطاء أي إستجابة قد تفشي بمعلومات. فمثلا، يجب أن لا تستجيب الأنظمة برسالة مثل " كلمة سر غير صحيحة لاسم الدخول الفلاني"، لأن مثل هذه الرسالة تكشف أن اسم الدخول صالح وموجود وتمنح الفرصة للمهاجم فقط بتخمين كلمة السر.
- ٩.٦ نظام الدخول يجب أن يظهر تاريخ ووقت آخر دخول، ذلك بأن هذا سينبه المستخدم لأي إستخدام للنظام باسمه بواسطة شخص غير مفوض.
- ٩.٧ يجب أن يخرج النظام تلقائيا وذلك بعد خمسة عشر دقيقة من عدم الفاعلية أو بعد أي فترة زمنية محدد من قبل مسؤول أمن المعلومات،
- ٩.٨ في حالة ما كان مهام العمل تعتمد على اسم المستخدم العام، فإنه يجب تغيير اسم المستخدم لآخر فريد.
- ٩.٩ يجب تطبيق نظام دخول مبني على الوقت لدخول المستخدم، كلما أمكن.
- ٩.١٠ في حالة ما إذا كان النظام الأساسي للمؤسسة حساس، فإنه يجب منع المستخدم من الدخول إلى نظام التشغيل سطر الأوامر.
- ٩.١١ في حالة إصدار اسم دخول جديد، فإنه يتوجب إستخدام نموذج تأشيري، إما مطبوع أو كجزء من عمل برنامج، يحدد الصلاحيات الممنوحة لهذا الإسم.
- ٩.١٢ يجب مراجعة الصلاحيات الممنوحة لكل أسماء الدخول وذلك خلال فترات منتظمة وبالتعاون مع وظائف الموارد البشرية.

٩.١٣ يجب تسجيل اي محاولة دخول غير ناجحة، على أن يتم مراجعة السجل خلال فترات زمنية منتظمة.

٩.١٤ في حالة ترك الموظف للمؤسسة، فإنه يتعين على مدير القسم التأكد من أنه تم حذف كل البطاقات التعريفية الخاصة بهذا الموظف من النظام، وذلك قبل التسوية النهائية لمغادرته.

٩.١٥ سيتم تعطيل أي أسم دخول تعريفي غير مستخدم لمدة 90 يوم، على أن يتم لاحقاً حذفه نهائياً وذلك بتصريح من مدير القسم التابع له الموظف.





سياسة حماية كلمة السر

الغرض

هذه الوثيقة تحدد سياسة المؤسسة المتعلقة بحماية كلمة السر، وتغييرها وصيانتها.

المجال

المجال لهذه السياسة يتضمن كل الموظفين بغض النظر عن مواقعهم.

السياسة

١٠٠١ جميع كلمات السر الافتراضية يجب تغييرها بواسطة المستخدم وذلك قبل إستخدام النظام.

١٠٠٢ يجب ألا تقل كلمة السر عن 8 حروف مكونة من خليط من الحروف والأرقام، مدججة بأحرف صغيرة وكبيرة.

١٠٠٣ يجب تغيير كلمة السر كل 30 يوم او كلما تم كشفها.

١٠٠٤ لا يجب إستخدام الاسم الشائع أو أي معلومات شخصية ككلمة سر ، على سبيل المثال: مثل تاريخ الميلاد، أسم القرين أو اسم الحيوان الأليف او رقم الهاتف.

١٠٠٥ يجب ان تكون كلمة السر مختلفة عن آخر 12 كلمة سر تم إستخدامها.

١٠٠٦ يجب أن تحفظ كلمة السر بسرية دائما ، ولا يجب إطلاع الأصدقاء أو زملاء العمل عليها.

١٠٠٧ جميع أجهزة الحاسب الشخصية يجب أن يتم تفعيل بها خيار " كلمة سر الجهاز" (كلمة السر عند التشغيل BIOS) ، كما يجب إعطاء كلمة السر هذه لمدير القسم في مظروف مغلق مختوم.

١٠.٨ غير مسموح لأي شخص مغادرة كمبيوتره/ها الشخصي أو جهازه دون أن يسجل خروجه من النظام، أو دون أن تكون الشاشة محمية بكلمة سر.

١٠.٩ يجب عدم حفظ كلمة السر في ملف مشفر داخل ملفات النظام، كما يجب ألا يتم إطلاقاً حفظها في ملف نصي.

١٠.١٠ سيقوم مدير النظام أو مدير الأمن بإعطاء كلمة السر بمظروف مغلق إلى مديره، أو من يتم تحديده من قبل موظف أمن المعلومات.

١٠.١١ في حالة الطوارئ أو في حالة عدم تواجد مدير النظام، فإنه يمكن الحصول على كلمة السر من الموظف المعين من قبل مسؤول أمن المعلومات.

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

جميع الموظفين، ومدير تكنولوجيا المعلومات ومسؤول أمن المعلومات.



سياسات الشبكة

سياسة أمن الجدار الناري والموجه

الغرض

تعتبر الموجهات والجدران النارية أكثر مكون عرضة للإختراق في الأمن المحيط. هذه الوثيقة تقدم أدنى حد للحماية المطلوبة للموجهات والجدران النارية المحيطة.

المجال

هذه السياسة تغطي الجدران النارية والموجهات في الشبكة المحيطة، كما أنها أيضا قابلة للتطبيق على الأجهزة من مثل الخوادم الوكيلية أو موجهات خطوط الأشتراك الرقمي الغير متماثل ADSLs الذكية .

السياسة

١١.١ يجب وضع الموجهات والجدران النارية في مكان مؤمن ومحمي مادياً.

١١.٢ يجب ألا يتم تهيئة حسابات الدخول المحلي على الموجه، كما يجب فصل محطة إدارة الجدار الناري عن الوحدة الرئيسية.

١١.٣ يجب إستخدام بروتوكول التحكم بالدخول TACACS Plus وذلك للتأكد من هوية المستخدم للموجه.

- ١١.٤ يجب تشفير الكلمة السرية للموجهات وذلك بتفعيل خاصية "تفعيل التشفير".
- ١١.٥ أي خدمة غير مرخصة وبشكل واضح على الجدار الناري، يجب منعها.
- ١١.٦ كمبيوتر الجدران الناري يجب أن يكون جهاز مستقل، ولا يجب إستخدامة لتشغيل وكيل، مواقع، أو أي خدمات أخرى.
- ١١.٧ يجب أن تقوم الموجهات والجدران النارية بمنع أي عنوان بروتوكول إنترنت "IP" غير صحيح يأتي عن طريق الإنترنت من مثل:
10.0.0.1 إلى 10.255.255.254 و 172.16.0.1 إلى 172.16.255.254، و 192.168.0.1 إلى 192.168.255.254
- ١١.٨ يجب ألا تسمح الموجهات والجدران النارية بإذاعة أي عنوان بروتوكول إنترنت IP.
- ١١.٩ يجب ألا يتم بالسماح بتوجيه بث عنوان البروتوكول على الجدران النارية أو الموجهات.
- ١١.١٠ يجب أن يتم تعطيل توجيه المصدر على الموجهات.
- ١١.١١ يجب ألا يتم تفعيل بروتوكول إدارة الشبكة البسيطة (SNMP) على أياً من الجدران النارية أو الموجهات، وفي حالة ما دعت الضرورة لتفعيل هذا البروتوكول لإدارة النظام، فإنه يجب إستخدام بروتوكول لإدارة الشبكة البسيطة على أن يكون معياري ومن السلسلة الموحدة.
- ١١.١٢ خدمة الشبكة العنكبوتية مسموحة على الموجه.
- ١١.١٣ يجب تهيئة الجدران الناري لإيقاف هجوم المزامنة SYN.
- ١١.١٤ يجب أن يقوم الجدار الناري بوقف عمليات الدخول بإستخدام عناوين وهمية أو عمليات تجزئة حزم البيانات أوالمهجوم بإستخدام ما يعرف بالحزم الدامعة.

- ١١.١٥ يجب أن يوافق مدير القسم المعني على قائمة قوانين الدخول وذلك قبل إستخدامها على الموجهات.
- ١١.١٦ يجب تخزين النسخة الاحتياطية من ملفات تهيئة الجدار الناري والموجهات في مكان آمن.
- ١١.١٧ يجب مراجعة سجل الدخول على الجدار الناري بانتظام.
- ١١.١٨ يجب أن يقوم الجدار الناري بحجب جميع عناوين الشبكة الداخلية عن العالم الخارجي.
- ١١.١٩ يجب أن يقوم الجدار الناري بعمل فلترة أو ترشيح لبرامج الجافا وعنصر التحكم .ActiveX
- ١١.٢٠ الخروج، أي الإشارات المغادرة للنظام يجب أيضاً أن يتم مراجعتها من قبل الجدار الناري.
- ١١.٢١ يجب التأكد من مستوى المستخدم على مستوى الجدار الناري، بدلاً من على مستوى بروتوكول عنوان الإنترنت IP، بشرط أن تكون الفاعلية ليست القضية.
- ١١.٢٢ يجب ألا تظهر أي رسائل ترحيب على بانر الدخول للموجه، ولكن يجب أن تظهر بدلاً من ذلك رسالة تحذيره: "تحذير: هذه شبكة خاصة. أي دخول غير مصرح له ممنوع منعاً باتاً. إذا لم يكن مصرح لك، سجل خروجك فوراً. سيتم محاكمة أي مخالف".

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

مدير الشبكة، ومدير الجدار الناري ومسؤول أمن المعلومات.

١.٠ سياسة أمن الإتصال بالطلب الهاتفي

الغرض

هذه الوثيقة تحدد سياسة المؤسسة المتعلقة بالخطوط الهاتفية للكمبيوترات ولأجهزة الفاكس.

المجال

الهدف لهذه السياسة يتضمن كل الخطوط لغرض توصيلات الكمبيوتر والفاكس.

السياسة

١٢.١ لا يجب توصيل أي جهاز مودم خارجي في جهاز حاسب آلي.

١٢.٢ يجب ألا يتم إستخدام أجهزة المودم الداخلية، لأجهزة الكمبيوتر المكتبي أو للأجهزة المحمولة، خلال الإتصال بشبكة المؤسسة.

١٢.٣ إذا ما دعت الحاجة لإستخدام "مودم" جهاز فاكس لشؤون العمل، فإنه يتعين الحصول على موافقة مسؤول أمن المعلومات مسبقاً.

١٢.٤ يجب أن يتم إستخدام أجهزة الفاكس لشؤون العمل فقط.

١٢.٥ لن يتم تمديد أي خط هاتف تناظري لأي موظف بإستثناء المدراء.

١٢.٦ لا يتعين إرسال أي فاكسات مباشرة من الكمبيوتر، إلا إذا كان لخدم فاكس المؤسسة، حيثما أمكن.

١٢.٧ يجب فحص أي شيء يتم تحميله للتأكد من خلوه من الفيروسات وذلك قبل الإستخدام.

التطبيق

في حالة إنتهاك سياسة الأمن، فإنه سيتم تطبيق عقوبات تأديبية بمستوى وقد تصل لحد إنهاء الخدمة.

المسؤولية

جميع الموظفين، مدراء الادارات، و مسؤول أمن المعلومات.



سياسة الشبكة الافتراضية الخاصة (VPN)

الغرض

الهدف من سياسة الشبكة الافتراضية الخاصة هو تقديم الإرشادات الازمة لتأمين الدخول عن بعد للشبكات المحلية.

المجال

سياسة الشبكة الافتراضية الخاصة تنطبق على الإتصالات إلى المؤسسة و إلى الأطراف الثالثة بما فيهم المستشارون الباعون المتعاقدون.

السياسة

١٤.١ على إعتبار أن الشبكة الافتراضية الخاصة هي إمتداد لشبكة المؤسسة، فإن كل قواعد الأمن تنطبق على العميل البعيد كما لو كان داخل المؤسسة.

١٤.٢ يجب إستخدام قناة وصل آمنة وذلك لكل الإتصالات الهامة، علماً بأن الإختيار الشائع هو إستخدام IPSEC للإتصال مع الشبكة الافتراضية الخاصة كلما كان ذلك ممكن.

١٤.٣ ينصح وبشدة إستخدام كلمة السر ولمرة واحدة.

١٤.٤ يفضل إستخدام نظام النفق "Tunnel Mode" عند إستخدام الشبكة الافتراضية الخاصة، ولكن إذا كانت الفاعلية مسألة هامة فإنه يمكن إستخدام نظام النقل "Transport Mode" بعد أخذ تصريح بذلك من مسؤول أمن المعلومات.

١٤.٥ جميع الملفات المنقولة من خلال الشبكة الافتراضية الخاصة يجب أن تخضع للفحص ضد الفيروسات.

١٤.٦ المدة اللازمة لإغلاق الإتصال أوتوماتيكياً من الشبكة الافتراضية الخاصة هو 30 دقيقة من عدم الفاعلية.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير الشبكة، و مستخدم الشبكة الافتراضية الخاصة ومسؤول أمن المعلومات.



٢.٠ سياسة الإتصال اللاسلكي

الغرض

الغرض من هذه السياسة هو توضيح الإرشادات لإتصالات الشبكة بواسطة الإتصال اللاسلكي

المجال

هذه السياسة تغطي جميع أجهزة اللاسلكي من مثل الهواتف المحمولة، المساعد الرقمي الشخصي PDA وأجهزة الكمبيوتر المحمولة وماشابهه من أجهزة تتصل بالشبكة العامة للمؤسسة.

السياسة

١٥.١ يجب أن يعتمد مسؤول أمن المعلومات إتصال كل الأجهزة اللاسلكية إلى الشبكة الداخلية للمؤسسة.

١٥.٢ يجب إستخدام خادم توثيق قوي لتحويل التصريح للأجهزة اللاسلكية.

١٥.٣ يجب تشفير جميع الأجهزة الاسلكية خلال إتصالها، كلما أمكن ذلك.

١٥.٤ يفضل وقبل تحويل أي إتصال إلى شبكة الأجهزة أن يقوم خادم التوثيق من التحقق من الجهاز عن طريق التأكد من عنوانه (مثل عنوان ترشيح التحكم بالدخول)

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير الشبكة، مستخدم الجهاز المتنقل، ومسؤول أمن المعلومات.

سياسة الدخول عن بعد

الغرض

هذه السياسة تصف الطرق المقبولة للإتصال بشبكة المؤسسة.

المجال

هذه السياسة تغطي كل الإتصالات المتلقاة (بدلا من المتصلة) بوساطة الموظفين، الأطراف الثالثة بما فيهم المستشارين والبائعين والمتعاقدين.

السياسة

١٦.١ يجب أن يتم إستخدام الإتصال عن بعد لأهداف العمل فقط.

- ١٦.٢ على إعتبار أن الإتصال عن بعد هو إمتداد لشبكة المؤسسة، فإن جميع سياسات المؤسسة تنطبق على الإتصال عن بعد.
- ١٦.٣ يجب أن يتم تطبيق ميزة إعادة الإتصال، وذلك للإتصال عن بعد بإستخدام خدمة الطلب الداخلي.
- ١٦.٤ يجب أن تقوم ميزة إعادة الإتصال بالتأكد من أن الرقم المطلوب إعادة الإتصال به مخول، وذلك بالبحث عنه في قائمة الأرقام المخولة لقاعدة البيانات، وذلك قبل الإتصال.
- ١٦.٥ يجب أن يتم تأمين الإتصال عن بعد بإستخدام آلية تفويض قوية، كما يتم تحديدها من قبل مسؤول أمن المعلومات.
- ١٦.٦ في حالة إستخدام شبكة رقمية للخدمات المتكاملة ISDN فإنه يجب إستخدام بروتوكول مصادقة مصادحة الاستبيان CHAP للتوثيق.
- ١٦.٧ يفضل أن يتم إستخدام جدار ناري لإتصالات الطلب الداخلي.
- ١٦.٨ في حالة ما إذا كانت المؤسسة تستخدم بروتوكول ترحيل الاطارات (frame relay)، فإنه يجب القيام بعملية توثيق مناسبة لمعرف قناة ارتباط البيانات DLCI
- ١٦.٩ يجب فحص جميع الملفات المحملة من خلال الإتصال عن بعد للتأكد من خلوها من الفيروسات.
- ١٦.١٠ يجب تسجيل ومراقبة كل الإتصالات عن بعد.
- ١٦.١١ في حالة توظيف نظام تحري الإختراق فإنه يجب عمل تنبيه لمدير النظام كلما تم إكتشاف هجوم.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير الشبكة، ومستخدم الإتصال عن بعد، ومسؤول أمن المعلومات





سياسة توظيف وتطوير التطبيقات العامة

الغرض

هذه السياسة تحدد متطلبات تطوير التطبيقات سواء أكانت داخلية أو بطلب من المؤسسة.

المجال

هذه السياسة قابلة للتطبيق على كل برمجيات المؤسسة الأساسية والبرمجيات الأخرى، ولكنها على كل حال تستثني أنظمة التشغيل.

السياسة

١٧.١ متطلبات الأمن الرسمي مطلوبة لكل تطورات الأنظمة سواء أكانت داخلية أو خارجية.

١٧.٢ يجب عدم استخدام أجهزة العمل للإعتبارات التجريبية.

- ١٧.٣ يجب أن يتم الفصل بين بيئة الإنتاج وبيئة الإختبار/التطوير.
- ١٧.٤ يجب تسجيل أي خطأ يحصل في النظام وإرساله للمبرمج الذي قام بتطوير البرنامج.
- ١٧.٥ قبل أن يتم نقل النظام إلى بيئة الإنتاج (العمل الحقيقي) فإنه يجب توثيق البرنامج بشكل مناسب.
- ١٧.٦ يجب ألا يتم إستخدام أي نسخ تجريبية، أو مجانية أو تحت التطوير في بيئات العمل الحقيقي إلا بموافقة الإدارة.
- ١٧.٧ يجب أن يتم تثبيت منطق الملكية التجارية على الجهاز الأساسي المركزي بدلاً من أنظمة أجهزة سطح المكتب.
- ١٧.٨ يجب أن يمتلك برنامج المهمة الحاسمة تسوية ضمان، كما يجب أن يتم إختباره و المصادقة عليه من قبل طرف ثالث لإثبات كفاءته لتأدية ما هو مطلوب.
- ١٧.٩ يجب أن تظهر جميع برامج الكمبيوتر، أجزاء البرامج، برمجيات الجافا الصغيرة، والوثائق بيانات حقوق النسخ.
- ١٧.١٠ بعد التحقق من هوية المستخدم، فإنه يجب عدم تسجيل معلومات الدخول من مثل أسم المستخدم وكلمة السر على الخادم.
- ١٧.١١ جميع عمليات الدخول يجب أن تبنى على أساس " الحاجة للمعرفة".
- ١٧.١٢ يجب أن يكون ملف التطبيق المخزن للمعلومات محمي بكلمة سر.

١٧.١٣ يجب أن تمتلك المؤسسة أكواد المصدر الأساسية للتطبيق أو يجب أن يكون هناك إتفاقات ضمان مع المورد المزود للتطبيقات.

١٧.١٤ يجب أن يخضع التطبيق لتجربة مستفيضة وذلك قبل نقله لبيئة الإنتاج أو العمل الحقيقية.

١٧.١٥ لا يجب نقل أي تطبيق إلى بيئة العمل بدون إجتياز إختبار قبول المستخدم.

١٧.١٦ قبل أن يتم نقل التطبيق إلى بيئة الإنتاج، يجب أن يتم حذف أي حسابات خاصة بالمطور هناك، بحيث ألا يملك المطور أي حساب في آلة الإنتاج.

١٧.١٧ يجب أن تتبع قواعد البيانات سياسة كلمة السر.

١٧.١٨ أي عملية لتحديث قاعدة البيانات يجب أن تتم بطريقة صحيحة وبقناة آمنه.

١٧.١٩ عند إستخدام تطبيق مستودع البيانات فإن عملية الدخول يجب أن تقتصر على الإدارة العليا والوسطى.

التطبيق

مخالفة السياسة سيكون موضوع لعقوبات تأديبية، والتي قد تذهب بعيداً لحد إنهاء الخدمة.

المسؤولية

مدير تكنولوجيا المعلومات، محلل النظم، المبرمج و مسؤول أمن المعلومات



سياسة تطوير برمجيات الشبكة العنكبوتية

الغرض

هذه السياسة تحدد متطلبات تطوير التطبيقات سواء أكانت داخلية أو بطلب من المؤسسة.

المجال

هذه السياسة ملائمة لجميع تطبيقات الشبكة العنكبوتية، والتي تطور حالياً أو تم تطويرها أو سيتم تطويرها في المستقبل.

السياسة

١٨.١ يجب خلق أسم دخول وكلمة سر مناسبين لمستخدم تطبيق الشبكة العنكبوتية، على أن يتم إستخدام بروتوكول طبقة الوصلات أو المقاييس الآمنة "SSL" لأي صفحة تتواصل مع المستخدم بإستخدام اسم المستخدم وكلمة السر.

١٨.٢ يجب أن لا يتم إظهار كلمة السر على الشاشة، كما يتوجب تعطيل خاصية "النسخ واللصق" في حقل إدخال كلمة السر.

١٨.٣ يفضل أن يتم حفظ كلمة السر بإستخدام طريقة الترميز أحادية الإتجاه.

١٨.٤ يجب إستخدام قناة مؤمنة وذلك للبيانات ذات الطبيعة السرية.

- ١٨.٥ يجب أن يمسخ زر العودة للخلف كل الحقول ذات البيانات الهامة.
- ١٨.٦ يجب أن يكون للإتصال بواسطة طبقة الوصلات أو المقابس الآمنة SSL وقت إنتهاء محدد.
- ١٨.٧ في حالة حدوث اي خطأ، فإنه يجب برمجته التطبيق بحيث يخلق صفحة خطأ متعارف عليها، بدلا من رسالة الخطأ المولدة من قبل النظام والتي قد تقوم بكشف معلومات عن الشبكة الداخلية.
- ١٨.٨ خادم الشبكة العنكبوتية يجب ألا يقدم معلومات اعلانية للجميع عن تفاصيل الخادم.
- ١٨.٩ يجب ألا تكون قائمة الدليل لواجهة البنية الثنائية للبوابة المشتركة متاحة للعميل.
- ١٨.١٠ يجب أن يتم التحقق من المعطيات والكلمات المدخلة بواسطة العميل وذلك قبل التنفيذ، وذلك لإحتمالية تحويل إستخدام هذه المدخلات لاختراق قواعد البيانات.
- ١٨.١١ يجب أن يكون هنالك خطة منهجية للإستجابة للإختراقات في حالة حدوث أي اختراق على الخادم أو في حالة إنتهاك للأمن.
- ١٨.١٢ يتعين القيام بإختبار للإختراق على التطبيق، كما يحدد من قبل مسؤول أمن المعلومات.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير تكنولوجيا المعلومات، محلل النظم، مدير موقع الشبكة العنكبوتية، مبرمج موقع الشبكة العنكبوتية، ومسؤول أمن المعلومات.





سياسة الأمن المادي العامة

الغرض

هذه السياسة تحدد متطلبات الأمن المادي. إذا ما كان الأمن المادي ضعيف، كل شيء يصبح غير آمن، بغض النظر عن جودة حلول و نتائج الأمن الأخرى.

المجال

هذه السياسة صالحة لكل المناطق المادية لمكاتب المؤسسة، متضمنة تلك الموجودة حالياً أو تلك التي من الممكن إضافتها لاحقاً.

السياسة

- ١٩.١ يجب أن يقوم مسؤول أمن المعلومات بتعريف مناطق الأمن في المؤسسة. فمثلاً:
- المنطقة أ: منطقة الإستقبال، حيث بإستطاعة أي شخص أي أن يدخلها (تعتبر الأقل أمناً).

- المنطقة ب: وهي المنطقة المتاحة للموظفين والزوار المصرح لهم.
- المنطقة ج: وهي المنطقة التي يسمح فقط لبعض الموظفين بدخولها من مثل غرفة الكمبيوتر و مناطق العمل الأخرى الهامة.

١٩.٢ يجب أن يطبق مسؤول أمن المعلومات المعايير المناسبة لكل منطقة من المناطق.

١٩.٣ يجب أن يتم توثيق وحفظ المخططات الخاصة بأرض المكتب والرسوم البيانية لكل خطوط كابل الهاتف، والكهرباء والماء والشبكة، بالإضافة إلى أماكن مطافئ الحريق.

١٩.٤ يجب أن يتم عمل وحفظ قائمة للتحكم بالدخول للمرافق مرتبطة بأوقات العمل فيها.

١٩.٥ يجب أن يتم حراسة مدخل المؤسسة أو المؤسسة بشكل كافي.

١٩.٦ يجب أن يتم توفير آليات مناسبة لمقاومة واكتشاف الحرائق.

١٩.٧ يجب أن يتم حفظ دليل هواتف لأرقام الطوارئ في مكان يسهل الوصول إليه عند الحاجة.

١٩.٨ يجب أن يتم توفير صندوق للإسعافات الأولية، على أن يحفظ في مكان يسهل الوصول إليه، مع مراعاة فحصه وإستكمال أي نقص فيه بانتظام.

١٩.٩ يجب أن يتم إضاءة جميع الأماكن في المكتب بشكل مناسب.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

ممثلي الإدارة و قسم إدارة الموارد البشرية، ومسؤول أمن المعلومات. مستقبلاً، فإن بعض المهام المتعلقة بالأمن المادي، قد تأول إلى مسؤول أمن المؤسسة عند شغل هذه المنصب. لكن حالياً فإن مسؤول أمن المعلومات سيكون مسؤول عن هذه المهام.



سياسة أمن مركز بيانات/غرفة الكمبيوتر

الغرض

هذه السياسة تناقش المتطلبات الازمة لحماية أنظمة الكمبيوتر ولإدارة العاملين في مركز بيانات/غرفة الكمبيوتر.

المجال

هذه السياسة صالحة لكل المناطق المادية لمكاتب المؤسسة، متضمنة تلك الموجودة حالياً أو تلك التي من الممكن إضافتها لاحقاً.

السياسة

٢٠٠١ سيكون الدخول إلى غرفة الكمبيوتر مقصوراً على أفراد المؤسسة المخولين فقط.

٢٠٠٢ لا يسمح بالزيارات أو الجولات في غرفة الكمبيوتر.

٢٠٠٣ يجب حراسة مندوبي الطرف الثالث والموردين إذا ما قاموا بزيارة غرفة الكمبيوتر.

٢٠٠٤ يجب حفظ سجل لوقت أي دخول أو خروج على غرفة الكمبيوتر.

٢٠٠٥ يجب توفير نظام إنذار ومقاومة حرائق مناسب.

٢٠٠٦ يجب أن يتم تطبيق ومراقبة نظام تحكم بالرطوبة.

٢٠٠٧ يجب أن يتم المحافظة ومراقبة درجة الحرارة بحدود مناسبة.

٢٠٠٨ يجب تطوير تدابير للطوارئ مناسبة لغرفة الكمبيوتر، على أن يسهل الوصول لهذه الإجراءات. كما يجب أن يتم تدريب الموظفين ليكون تطبيق هذه التدابير فعال عند الحاجة. أخذين بعين الاعتبار أن هذه الإجراءات يجب أن تراجع باستمرار وخلال فترات منتظمة.

٢٠٠٩ سيقوم مسؤول أمن المعلومات بتنسيق الجهود لتطوير المعايير لغرفة الكمبيوتر.

٢٠.١٠ سيقوم مسؤول أمن المعلومات بتنسيق الجهود للتأكد من وجود مزود طاقة ذو كفاءة عالية لغرفة الكمبيوتر، وللتأكد من توفر الضمانات الكافية لحماية الأجهزة.

٢٠.١١ لا يسمح بالأكل أو الشرب أو التدخين في غرفة الكمبيوتر.

٢٠.١٢ يمنع إستخدام الهاتف النقال في مركز البيانات.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.



سياسة الوسائط الممغنطة

الغرض

هذه السياسة تناقش متطلبات التعامل مع الوسائط الممغنطة.

المجال

هذه السياسة قابلة للتطبيق على جميع وسائط التخزين، أي: القرص الصلب، القرص المدمج، القرص المرن، قرص الليزر، القرص المرن العملاق، الشريط الممغنط الملفوف، القرص الضوئي، القرص المضغوط، الشريط الممغنط الخرطوشي، والشريط الصوتي الرقمي.

السياسة

٢١.١ يجب أن يتم عمل قائمة بجميع الوسائط الممغنطة الهامة، على أن يتم حفظها في مكتبة الوسائط الممغنطة الآمنة.

٢١.٢ يجب أن يتم عنونة كل الوسائط بشكل ملائم.

٢١.٣ يجب تدمير جميع الوسائط الممغنطة مادياً وذلك قبل التخلص منها.

٢١.٤ يجب أن يتم التحقق والتأكد من مدة صلاحية جميع الوسائط، عن طريق الإستفسار من المورد المعني.

٢١.٥ يجب أن تفحص جميع الوسائط للتأكد من خلوها من الفيروسات وذلك قبل إستخدامها.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات

سياسة أمن الخادم

الغرض

هذه السياسة تناقش المسائل المتعلقة بأمن الخوادم الداخلية للمؤسسة، وذلك للتأكد من أنه ليس هناك أي دخول غير مخول على معلومات المؤسسة.

المجال

هذه السياسة تنطبق على كل الخوادم المملوكة أو المدارة بواسطة المؤسسة.

السياسة

٢٢.١ يجب وضع الخادم في منطقة مادية آمنة.

٢٢.٢ يجب أن يتم توثيق جميع الإعدادات الخاصة بالخوادم، على أن يتم الموافقة على هذه الوثائق من قبل مدير تكنولوجيا المعلومات و مسؤول أمن المعلومات.

٢٢.٣ يجب أن يمتلك كل خادم وثيقة للتهمية و لنسخة نظام التشغيل المستخدم، وللرقع (patches) المثبتة، ولطريقة عمل النسخ الاحتياطية والإسترجاع.

٢٢.٤ كل سياسات إدارة التغيير يجب أن تطبق بحزم على الخوادم.

- ٢٢.٥ يجب أن يوافق مسؤول أمن المعلومات على كل إعدادات الخوادم.
- ٢٢.٦ يجب أن يتم تعطيل الخوادم الغير ضرورية، من مثل خادم الشبكة العنكبوتية وغيرها.
- ٢٢.٧ يجب مراقبة سجل الخادم بأساس منتظم، كما يتم تحديده من قبل مسؤول أمن المعلومات.
- ٢٢.٨ جميع الرقع الأمنية يجب أن تثبت على الخادم بعد التأكد من أن ليس لها أي تأثير سلبي على التطبيقات المدارة.
- ٢٢.٩ جميع الحسابات التلقائية أو الزائرة سوف يتم إما تعطيلها أو تغيير كلمة السر لها.
- ٢٢.١٠ إذا ما لزم الأمر لإدارة الخادم عن بعد، فإنه يجب إستخدام قناة آمنة لهذا الغرض.
- ٢٢.١١ يجب إستخدام الحساب التحكم بالخادم من مثل مستخدم أول أو المستخدم الجذري فقط عند الحاجة.
- ٢٢.١٢ سيقوم مسؤول أمن المعلومات بعمل مراجعة دورية.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير النظام، مسؤول أمن المعلومات، و مدير تكنولوجيا المعلومات.



سياسات إدارة العمليات

سياسة إدارة التهيئة

الغرض

هذه السياسة الأمنية تتناول التوثيق المناسب لتهيئة الأنظمة الهامة.

المجال

هذه السياسة تنطبق على كل الخوادم، معدات الشبكة وغيرها، سواء أكانت مملوكة أو مشغلة من قبل المؤسسة.

السياسة

٢٣.١ يجب توثيق كل تهيئات النظام متضمناً المعدات، والبرمجيات، و برمجيات العمل الأساسية.

٢٣.٢ يجب أن يتم توفير الوثائق بنسختين، واحدة مطبوعة وأخرى إلكترونية.

٢٣.٣ يجب إعتبار إدارة التهيئة كخط قاعدي للوثيقة، وكل التغييرات التي تطرأ عن هذا الخط القاعدي يجب أن توثق بحسب سياسة إدارة التغيير.

٢٣.٤ أي تغيير يستجد على التهيئة الأساسية يجب أن يتم توثيقه في وثائق إدارة التهيئة، وذلك قبل تسجيل هذه التغييرات على الذاكرة الخارجية.

٢٣.٥ يتعين موافقة أمن المعلومات على كل وثائق التهيئة.

٢٣.٦ يجب إستخدام وثائق إدارة التهيئة وإدارة التغيير معاً في حالة الإسترداد.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير النظام، مسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.

سياسة إدارة التغيير

الغرض

هذه السياسة الأمنية تضع التوثيق المناسب لإدارة التغيير لكل الأنظمة الحيوية.

المجال

هذه السياسة تنطبق على كل الخوادم الحيوية، ومعدات الشبكة، وبرمجيات العمل الحيوية سواء كانت مملوكة أو مشغلة من قبل المؤسسة.

السياسة

٢٤.١ يجب استخدام الإجراءات والأساليب المعيارية للتعامل بفاعلية وحسم مع التغييرات و للتحكم بالتعديلات.

٢٤.٢ يجب تدوقيق كل التغييرات، والحصول على موافقة مسبقة لكل التغييرات المطبقة على أنظمة الإنتاج الحيوية..

٢٤.٣ يجب تقديم "طلب تغيير" للمدير المباشر ليتم إيماده، وسيقوم مسؤول أمن المعلومات بمتابعة سير العمل لإعتماد التغيير.

٢٤.٤ يجب تقييم جميع التغييرات، وتقدير تأثيرها وذلك قبل الموافقة عليها أو رفضها.

٢٤.٥ كل التغييرات، عند الموافقة عليها، يجب ان تجداول بحيث يتم التأكد من توفر فترة زمنية تسمح للعودة إلى ما قبل التغيير، تحسباً لحدوث أي شيء غير متوقع.

- ٢٤.٦ يجب أن يرفق بوثيقة طلب التغيير تفاصيل الإجراءات لعمل التغيير، خطوة بخطوة. كما يجب أن تتضمن أيضاً تفاصيل إجراءات الرجوع إلى ما قبل التغيير، وذلك في حالة ما إذا فشل التغيير ولم يحقق النتيجة المرجوة.
- ٢٤.٧ متى دعت الحاجة لتغيير برنامج التطبيق، أو برنامج النظام، أو الشبكة المحلية أو أي من المعدات، فإن التغيير يجب أن يصرح ويعتمد بالشكل المناسب.
- ٢٤.٨ كل تغيير يجب أن يختبر بالكامل، ويوثق تماماً.
- ٢٤.٩ يجب أن تتم التغييرات في الوقت الذي يكون النشاط على النظام معدوم أو منخفض. وفي حالة ما إذا لزم القيام بأكثر من تغيير في نفس الوقت، فإن التغييرات يجب أن ترتب على حسب الأولوية التقنية والعملية.
- ٢٤.١٠ يجب ان يتم الموافقة على التغييرات بعد القيام بدراسة كافية للآثار المصاحبة والمترتبة على ذلك.
- ٢٤.١١ بمجرد الموافقة على التغييرات، فإنه يجب إدخالها في سجل إدارة التغيير.
- ٢٤.١٢ يجب أن يتم إختبار التغييرات بشكل وافي، وعرض النتيجة على المدير المختص.
- ٢٤.١٣ يجب أن يتم تقديم تقرير ملخص إدارة التغيير إلى الإدارة الأعلى أسبوعياً.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مدير النظام، مسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.

سياسة إخراج المطبوعة والتوزيع

الغرض

هذه السياسة تحدد المتطلبات للمخرجات المطبوعة ولتوزيعها.

المجال

هذه السياسة تنطبق على كل الخوادم الحيوية، ومعدات الشبكة، وبرمجيات العمل الحيوية سواء كانت مملوكة أو مشغلة من قبل المؤسسة.

السياسة

- ٢٥.١ يجب أن يكون لجميع التقارير الهامة المولده بالكمبيوتر مستوى تصنيفي، وذلك بناءً على أهمية هذا التقرير
- ٢٥.٢ مالك التطبيق سيحدد مستوى التصنيف.
- ٢٥.٣ إذا كان التقرير مصنف على أنه ليس "عام"، فإن الصفحة الأولى يجب أن تكون صفحة عنوان وأن يتم توضيح "مستوى التصنيف" و "اسم المستخدم" الذي طبع له/لها التقرير.
- ٢٥.٤ سيقوم مسؤول أمن المعلومات من التأكد من أن الإجراءات متوفرة للتأكد من أن التقرير يذهب فقط للشخص المخول.

٢٥.٥ يقع على عاتق الشخص الذي يطبع التقرير مسؤولية التكفل بالحماية المناسبة للمعلومات التي يحوي.

٢٥.٦ إذا ما وجد شخص ما تقرير غير مصنف ولا يخصه/ها، فإن عليه/عليها إخبار مسؤول أمن المعلومات.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

مستخدم طباعة التقرير، ومسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.







سياسة إستمرارية العمل العامة

الغرض

الغرض من هذه السياسة هو تقديم إرشادات متعلقة بإستمرارية العمل.

المجال

هذه السياسة تنطبق على كل أنظمة العمل الحيوية كما يتم الإشارة لها في تحليل حوادث العمل وتقدير المخاطر في سياسة أمن المؤسسة.

السياسة

٢٦.١ سيقوم مسؤول أمن المعلومات من التأكد من أن إستمرارية عمل أنظمة العمل الحيوية مكفولة، بحسب متطلبات تقدير المخاطر للسياسة العامة.

٢٦.٢ ستقوم الإدارة العليا بتقرير المدى لخطة التعافي وذلك بناءً على تقرير تقدير المخاطر (بحسب السياسة الأمنية للمؤسسة).

٢٦.٣ الأنظمة الهامة، بحسب تقدير المخاطر، يجب أن تمتلك إجراءات تعافي فعالة وموثقة في حالة أي كارثة.

٢٦.٤ يجب أن تقوم الإدارة العليا بتعريف الكلمة "كارثة" وطريقة تقييم المخاطر المرتبطة بها. على أن يقوم مسؤول أمن المعلومات بتنسيق هذه المهمة.

٢٦.٥ يجب تحديث جميع الوثائق المتعلقة باستمرارية العمل بانتظام.

٢٦.٦ سيقوم مسؤول أمن المعلومات من التأكد من توفر خطة طوارئ مناسبة، ومن وجود "خطة إستجابة للطوارئ".

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

روؤساء أقسام العمل، مسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.





سياسة الإسترداد والنسخ الإحتياطي

الغرض

هذه السياسة تخصص مقاييس الإسترداد والنسخ الإحتياطي للمؤسسة.

المجال

هذه السياسة تنطبق على كل الخوادم الحيوية، ومعدات الشبكة، وبرمجيات العمل الحيوية سواء كانت مملوكة أو مشغلة من قبل المؤسسة.

السياسة

٢٧.١ يجب أن يكون النسخ الإحتياطي لكل الأجهزة الهامة، شاملاً الخادم وأدوات الإتصال وأدوات وبرامج المهمة الحاسمة، مكفول.

٢٧.٢ سوف يتم تحديد عدد مرات عمل النسخ الإحتياطي وذلك بناءً على طبيعة التطبيق المستخدم.

٢٧.٣ طريقة النسخ الإحتياطي المفضلة هي "النسخ الإحتياطي الكامل" يتبعه "النسخ الإحتياطي التفاضلي".

٢٧.٤ إلا بوجود أسباب مقنعة، فإنه يجب تجنب إستخدام طريقة "النسخ الإحتياطي التزايدى" لأنه في حالة إسترجاع البيانات، قد يؤدي فشل أحد النسخ الإحتياطية إلى فشل عملية الإسترجاع كاملة.

٢٧.٥ عند تخزين بيانات تاريخياً، فإنه يجب مراعاة صلاحية وسط التخزين.

٢٧.٦ يجب أن يخطط الوقت لعملية "النسخ الإحتياطي الموزع" ليكون بأقل تأثير ممكن على الشبكة الداخلية للمؤسسة.

٢٧.٧ يجب ألا تنتهك عملية النسخ الإحتياطي خصوصية النظام.

٢٧.٨ يجب ألا يتم إستخدام أي كمبيوترات عامة لعمل نسخ إحتياطي للبيانات الهامة.

٢٧.٩ يجب فحص البيانات المؤرشفة بإستمرار.

٢٧.١٠ يجب أن يتم التدقيق على كل النسخ الاحتياطية للتأكد من سلامة وسط التخزين، كما يجب تفعيل ميزة "القراءة بعد الكتابة" كلما كانت متاحة.

٢٧.١١ في حالة ما إذا كان عملاء النسخ الاحتياطي الموزعين غير متوفرين، فإنه يجب وضع بيانات العمل الهامة في ملف على الخادم لعمل نسخ احتياطي له، حيث سيقوم مسؤول أمن المعلومات بعمل الترتيبات اللازمة. وسيقوم مسؤول أمن المعلومات، بالتشاور مع مدير تكنولوجيا المعلومات، بعمل الترتيب للقفز الإلكتروني؛ أي تخزين بيانات النسخ الاحتياطية خارج الموقع.

٢٧.١٢ عندما تصبح وسائط التخزين بلافائدة، فإنه يجب أن يتم التخلص منها ماديا بكسرهما أو يفضل حرقها.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

كل الموظفين، ومسؤول أمن المعلومات ومدير تكنولوجيا المعلومات



سياسات الطرف الثالث والموظفين

سياسة الموظفين

الغرض

هذه السياسة تختص بالإرشادات والمقاييس المتعلقة بالموارد البشرية ذات الصلة الخاصة بأمن المعلومات.

المجال

هذه السياسة تنطبق على كل الموظفين ذوي العقود أو الثابتين.

السياسة

٢٨.١ يلزم المواد البشرية وقبل تعيين أي موظف محتمل، البحث في سجل الموظف السابق، الإتصال بالمراجع، والتأكد من صحة الشهادات التعليمية.

٢٨.٢ يجب على الموظفين التوقيع على تعهد بقبول المسؤولية بالإنضمام لسياسات الأمن.

٢٨.٣ ستقوم إدارة الموارد البشرية بالتأكد من أن المسؤولية الأمنية من ضمن مسؤوليات العمل للموظف.

٢٨.٤ سيتم تنبيه كل موظف إلى سياسة أمن المعلومات في وثيقة الشروط والأحكام للعمل.

٢٨.٥ ستقوم إدارة الموارد البشرية من التأكد من أنه يتم الفصل بين الواجبات وتدوير الموظفين في العمل، وإنما يمكن.

٢٨.٦ ستقوم إدارة الموارد البشرية من التأكد من عقد مقابلة مغادرة، وذلك عندما يرغب الموظف بترك الوظيفة بالمؤسسة.

٢٨.٧ ستقوم إدارة الموارد البشرية من التأكد من أنه تم حذف كل حسابات الكمبيوتر للموظف وذلك قبل التسوية النهائية لها.

٢٨.٨ في حالة ما إذا تم إنهاء خدمة الموظف دون موافقته، فإنه يجب أن يتم مرافقته/مرافقتها من مبنى المؤسسة.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة.

المسؤولية

الموارد البشرية، مسؤول أمن المعلومات و قسم ومدير تكنولوجيا المعلومات.



سياسة الطرف الثالث

الغرض

هذه السياسة تختص بالإرشادات والمقاييس المتعلقة للطرف الثالث والمورد الخارجي.

المجال

هذه السياسة تنطبق على الأطراف أياً كانوا، سواء موردين، متعهدين، مستشارين أو موردين خارجيين مختصين.

السياسة

٢٩.١ يجب أن يتم تحديد المخاطر المترتبة على مشاركة طرف ثالث، والمترتبة على الإستعانة بمصدر خارجي، والتدابير المناسبة والمتخذة لمعالجتها.

٢٩.٢ تعتبر الموافقة على إتفاقية المحافظة على السرية - أو كما تسمى أحياناً إتفاقية عدم الكشف (أو الإفصاح)- ضرورية وذلك قبل مشاركة المعلومات الهامة مع أي طرف ثالث.

٢٩.٣ يجب تحديد دور ومسؤوليات الطرف الثالث بوضوح.

٢٩.٤ سيتم إعطاء الطرف الثالث صلاحية الدخول على نظام الكمبيوتر للمؤسسة وذلك فقط بعد التوقيع على عقد رسمي يحوي كل المتطلبات الأمنية الواجب على الطرف الثالث الإلتزام بها.

٢٩.٥ في حالة ما إذا تم تعريف مستخدمين خارجيين أو طرف ثالث على النظام، فإنهم جميعاً يجب أن يكون لديهم تاريخ إنتهاء صلاحية إجباري.

٢٩.٦ في حالة ما إذا إحتاج الطرف الثالث أو المستخدم الخارجي للحصول على إمتيازات إستخدام خدمتي الطلب الهاتفية والطلب الداخلي لتأدية مهامه، فإنه يتوجب تقييد ومراقبة هذه الصلاحيات.

التطبيق

أي إنتهاك للسياسة سيكون موضوع إلى عقوبات تأديبية، والتي قد تذهب إلى حد مثل إنهاء الخدمة. وفي حالة الطرف الثالث قد تصل إلى حد إنهاء العقد.

المسؤولية

رؤساء الادارات، الموارد البشرية، ومسؤول أمن المعلومات، ومدير تكنولوجيا المعلومات.

