2017

سياسات أمن المعلومات

National Information Center

Government Information Security Center

1/6/2017

سياسات أمن المعلومات

النسخة الثالثة

المحتويات

15.0 سياسة الدخول عن بعد

سياسات تطوير البرمجيات

16.0 سياسة توظيف وتطوير البرامج العامة

17.0 سياسة تطوير برامج الإنترنت

سياسة الأمن المادي

18.0 سياسة الأمن المادي العامة

19.0 سياسة أمن مركز البيانات/غرفة الكمبيوتر

20.0 سياسة وسائط التخزين الممغنطة

21.0 سياسة أمن الخوادم

سياسات إدراة العمليات

22.0 سياسة إدارة التهيئة

23.0 سياسة إدارة التغيير

24.0 سياسة المخرجات المطبوعة والتوزيع

سياسات إستمرارية العمل

25.0 سياسة إستمرارية العمل العامة

26.0 سياسة النسخ الإحتياطي(backup) و الإستعادة (Recovery)

سياسات الموظفين والطرف الثالث

27.0 سياسة الموظفين

28.0 سياسة الطرف الثالث

المقدمة

يعتبر موضوع أمن المعلومات من المواضيع الساخنة والمتجددة في عالم تقنية المعلومات وذلك في ظل الاعتماد الكبير للمنظمات على التقنية. ومما لا يخفى على الجميع ما للمعلومات وأنظمتها في عصرنا هذا من أهمية قصوى لكونها تمثل القلب النابض لعمل المنظمات وتمثل أحد أهم الممتلكات (Asset) – إن لم تكن الأهم – مثلها مثل أي أصول ثمينة لدى المنظمة. فالكل يعي أهمية حماية المباني من الحريق أو الكوارث الطبيعية، ولكن لا يعي الكل أهمية حماية المعلومات من المخاطر المحيطة بها. لذا ولكي يتم حماية المنظمات وعملها يتوجب حماية المعلومات وأنظمتها.

ويعرف أمن المعلومات على أنه المحافظة على دقة وسرية وتوفر البيانات ضد أي مؤثرات سواءً كانت متعمدة أم عرضية. وتتمثل المحافظة على دقة المعلومات (Integrity) بمنع أي محاولات تهدف إلى التأثير على دقة وصحة البيانات كعمل تغييرات غير صحيحة في محتوى البيانات. بينما تتمثل المحافظة على سرية البيانات (Confidentiality) بمنع أي محاولات قد تؤدي إلى كشف محتوى البيانات لأشخاص غير مصرح لهم بذلك وغير معنيين. أما العنصر الثالث والأخير لأمن المعلومات فهو المحافظة على توفر وتواجد البيانات (Availability) في الوقت الذي تطلب به.

أمن المعلومات هو تعبير واسع يغطى مجموعة (كبيرة – مرتبة) من النشاطات. وهو يتضمن كل (المنتجات والعمليات) التي تتم بهدف منع وصول الأفراد غير المصرح لهم إلى المعلومات، ومنع تعديل المعلومات، ومنع حذفها، وحماية المصادر..

وقد يعتقد البعض أن الحلول التقنية الأمنية وحدها كفيلة بتأمين جانب الحماية للمعلومات، وهذا بالطبع اعتقاد خاطئ. إذ أن حماية المعلومات ترتكز على ثلاثة عناصر أساسية مكملة لبعضها البعض وهي:-

1) العنصر البشري.

2) الحلول التقنية.

3) السياسات الأمنية للمعلومات، والتي بدورها تحكم وتنظم كيفية تعامل العنصر البشري مع المعلومات بشكل سليم للوصول إلى الهدف المنشود. إذ أن نقطة تقاطع هذه العناصر الثلاثة هي أعلى مستوى من مستويات أمن المعلومات.

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. ونحن هنا نضع بين أيديكم سياسة أمن المعلومات، والتي تتناول أهم المخاوف المتعلقة بأمن المعلومات.

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

آخذين بعين الإعتبار بأن دليل السياسة هذا قد تم تقسيمه إلى جزئيين 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 الأقسام بينما يعتبر باقي الموظفين في المؤسسة كمستهدف ثاني ثانوي.

- **سياسة الإستخدام المتفق عليها**: هذه الإستراتيجية تلخص كل المبادئ العامة المتفق عليها لأفضل 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 شبكة الانترنت والتطبيقات التقليدية، 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 .

م . أبوذر عثمان محمد خالد

مدير مركز أمن المعلومات الحكومية.

الجزء الأول: السياسات العامة

1.0 سياسة أمن المؤسسة

أ. **الغرض**

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

ب. **المجال**

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

ت. **السياسة**

1.1 أمن وحماية المعلومات هو مسؤولية الجميع.

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

1.3 يجب تعيين مسؤول أو فريق لأمن المعلومات يقوم بتنسيق الجهود لتطبيق كل سياسات الأمن. هذا وفي حالة إقتضاء الضرورة فإنه يمكن لاحقا تشكيل لجنة لأمن المعلومات

1.4 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.

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

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

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

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

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

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

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

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

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

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

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

1.16 يجب إبلاغ مسؤول أمن المعلومات بأي محاولات لإختراق المعلومات أوتهديدات للأمن.

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

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

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

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

1.21 يعتبر توفير الحماية المادية المناسبة مسألة جوهرية يجب مراعاتها.

1.22 يجب مراجعة وتنقيح وثيقة أمن المعلومات وبشكل دوري.

1.23 سيتم فرض وتطبيق عقوبات تأديبية مناسبة تتراوح مابين لفت النظر إلى إنهاء الخدمة وذلك بناءاً على خطورة وطبيعة الإنتهاك.

1.24 يجب وضع الخطط والإجراءات المناسبة للتعامل مع المخاطر والحوادث والاعتداءات في حالة حدوثها.

1.25 مسؤول أمن المعلومات يقع على عاتقة تعيين أشخاص في فريق الإستجابة لحوادث وأعطال الكمبيوتر، لديهم الكفاءة والقدرة على التعامل مع الحوادث والإنتهاكات الأمنية في حالة التعرض لها.

1.26 يجب أن يتم تبليغ مسؤول أمن المعلومات بجميع الحوادث والفشل والقصور الأمني. حيث سيتكفل تطبيق لوائح منظمة المقاييس الدولية (ISO 7002) بمعالجة المسألة، وستتأخذ الإجراءات والتدابير المناسبة لمنع تكرار ذلك في المستقبل.

1.27 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.

1.28 يجب تنمية المهارات المناسبة للتعامل مع أي حوادث متعلقة بالأمن.

1.29 يجب القيام بعمليات الفحص المناسبة وبشكل منتظم لضبط أي حالات ضعف أو قصور أمني، وذلك بإجراء إختبار الإختراق القياسي.

1.30 يجب تدعيم وتقوية جميع النظم، وبخاصة نظم التشغيل، لمستوى قياسي متفق عليه.

1.31 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.

1.32 يجب أتخاذ التدابير والمقاييس المناسبة لتأمين جميع معدات ومصادر وأسلاك الطاقة.

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

1.34 على كل الموظفيين إرتداء الشارات التعريفية الخاصة بهم وذلك خلال تواجدهم في مباني المؤسسة.

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

1.36 في نهاية أي إجتماع رسمي فإنه ينبغي مسح جميع الملاحظات المدونة على اللوح الابيض والتخلص من جميع الأوراق والرسوم التوضيحة إن وجدت.

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

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

1.39 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.

1.40 إذا كان يتعيين 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.

1.41 يجب إجراء فحص سنوي للنظام وذلك لفحص التحكم بالأنظمة.

1.42 يجب كتابة جميع ما يعرف بسجلات الأداء (او سجلات النفاذ الى النظام) الهامة على أقراص ممغنطة تسمح بالقراءة فقط —ولا تسمح بإعادة الكتابة– وذلك لمنع أي محاولة لتغيير محتوى هذه السجلات. آخذين بعيين الإعتبار أن هذه السجلات يجب أن تراجع بواسطة الأشخاصالمفوضيين فقط.

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

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

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

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

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

ث. التطبيق

في حالة الإخلال ببنود هذه السياسة، فإن عقوبات تأديبية قد تصل إلى حد إنهاء الخدمةستطبق على المخالف.

ج. المسؤولية

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

2.0 سياسة الإستخدام المتفق عليها

أ. الغرض

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

ب. المجال

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

ت. السياسة

2.1 أمن المعلومات هو مسؤولية الجميع اليومية، وعلى جميع موظفي المؤسسة إتباع سياسة الأمن كلاً حسب موقعه.

2.2 موارد المؤسسة مخصصة لإستخدام العمل ويجب أن تستخدم لهذا الغرض فقط.

2.3 بين الحين والآخر، سيقوم مسؤول أمن المعلومات المعين من قبل المؤسسة بنشر تعليمات وإرشادات وعلى الجميع الإلتزام بها.

2.4 يعتبر أي عذر للجهل بسياسة الأمن غير مقبول بتاتاً.

2.5 جميع المعلومات المخزنة والمتبادلة من خلال موارد المؤسسة تبقى ملكية خاصة بالمؤسسة، وللمؤسسة الحق الكامل المكفول بمراقبتها والتدقيق عليها.

2.6 جميع معلومات المؤسسة السرية يجب التعامل معها بسرية تامة، كما يمنع منعاً باتاً نسخ أو نقل هذه المعلومات إلا إذا لزم الأمر لشؤون المؤسسة.

2.7 يقع على عاتق الموظفيين حماية كلمات السر والعبور الخاصة بهم، ولا يجدر بهم تشارك هذه المعلومات مع أي أحد كان.

2.8 يجب تغيير كلمة السر بما يتوافق مع سياسة كلمة السر.

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

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

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

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

2.13 يحظر النسخ الغير قانوني للبرامج.

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

2.15 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 آلاتهم لحظة الإرسال.

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

2.17 يمنع منعاً باتاً إستكشاف ومسح المنافذ والثغرات للخوادم الداخلية والخارجية، إلا إذا كان هذا العمل جزء من إختبار الإختراق الرسمي المجرى بوساطة المؤسسة، وباتخاذ التدابير المضادة المناسبة.

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

ث. التطبيق

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

ج. المسؤولية

جميع الموظفيين.

3.0 سياسة الوعي الأمني

أ. الغرض

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

ب. المجال

هذه السياسة لجميع الموظفيين بغض النظر عن المراكز التي يشغلونها.

ت. السياسة

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

3.2 في حالة عدم حضور اي موظف لورشة العمل، فإنه سيتم إعلام المدير المختص بذلك.

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

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

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

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

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

ث. التطبيق

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

ج. المسؤولية

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

الجزء الثاني: السياسات التفصيلية

سياسات ملكية وحماية البيانات

4.0 سياسة حماية المعلومات

أ. الغرض

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

ب. المجال

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

ت. السياسة

4.1 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.

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

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

4.4 من مسؤوليات متعهد البيانات التأكد من أنه تم عمل نسخة إحتياطية للبيانات وحفظت في مكان آمن.

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

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

4.7 سيقوم متعهد البيانات من التأكد من أن جميع الضوابط الكافية متوفرة، كما تحدد بوساطة مالك البيانات.

4.8 على متعهد البياناتالإحتفاظ بالوثائق لكل الإنشطة التي تتضمن بيانات المالك.

4.9 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 تكنولجيا المعلومات.

5.0 سياسة وقاية المعلومات

أ. الغرض

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

ب. المجال

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

ت. السياسة

5.1 مالك الكمبيوتر سيقرر معدل حفظ البيانات إحتياطياً، وذلك على اساس أهمية ومدة بقاء المعلومات.

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

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

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

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

5.6 على مالك البيانات تحديد مدة الإبقاء على البيانات.

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

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

5.9 يجب الفصل بين برامج التطبيقات وبين البيانات للأغراض الأمنية.

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

5.11 يجب إتخاذ التدابير المناسبة من مثل: تثبيت برنامج مكافح فيروسات، جدران نارية، نظام تحري الإختراق وبرامج التصنت على الشبكة (الشمام) وغيرها، وذلك لتصدي للتهديدات الأمنية الداخلية والخارجية.

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، مدراء الأقسام، و مسؤول أمن المعلومات.

سياسة مكافحة الفيروسات والبرامج الخبيثة

6.0 سياسة مكافحة الفيروسات

أ. الغرض

هذه الوثيقة تفصل سياسة المؤسسة المتعلقة بالبرامج الخبيثة مثل: الفيروسات والديدان(Worms) وأحصنة طروادة (Trojan) وبرامج الفدية (Ransomware) وغيرها.

ب. 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.

ت. السياسة

6.1 يجب أن يتم تشغيل أحدث برنامج مكافح فيروسات كما تقرره إدارة المؤسسة.

6.2 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 توجية أي بريد الإلكتروني يعتقد أنه من الممكن إحتوائه على فايروس.

6.3 جميع وسائط التخزين القابلة للنقل (مثل القرص المرن وغيرها) يجب أن تخضع للتدقيق للتأكد من خلوها من الفيروسات وذلك قبل أن يتم إستخدامها.

6.4 يجب إلا يتم إستخدام أي برنامج قرصنة على الشبكة الداخلية للمنظمه.

6.5 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.

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

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

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

6.9 يجب أن تكون جميع التحديثات الخاصة ببرنامج مكافح الفيروسات تلقائية من الإنترنت أو من الخادم المركزي.

6.10 يجب أن يتم تضمين برنامج مكافح الفيروسات بالمكونات التالية:

أ- جدار ناري شخصي(Firewall) .

ب- نظام تحري إختراق شخصي (Intrusion Detection System) .

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، ومدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

السياسات المتعلقة بالإنترنت

7.0 سياسة إستخدام الإنترنت

أ. الغرض

هذه الوثيقة تفصل سياسة المؤسسة المتعلقة بتصفح وإستخدام الإنترنت.

ب. المجال

المجال لهذه السياسة يستهدف جميع الموظفين بغض النظر عن موقعهم.

ت. السياسة

7.1 يسمح بإستخدام إتصالات الإنترنت الرسمية فقط، ولا يسمح لأي شخص بالإتصال عن طريق مودم الحاسب الشخصي لما قد ينطوي عليه ذلك من فتح باب خلفي(ثغرة) غير آمن على المؤسسة.

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

7.3 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.

7.4 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 أوتشهيرية على الإنترنت بإستخدام موارد المؤسسة.

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

7.6 في حالة تحميل أي ملف بحجم أكبر من300ميجابايت، فإنه يتعين الحصول على موافقة مسبقة من المدير المباشر.

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

7.8 لا يسمح لأي شخص بإستخدام خدمات المحادثة من مثل الواتس أب او الايمو أو التلغرام أو السكايب أو اي برنامج مشابه. وفي حالة ما دعت الضرورة لإستخدام أي من هذه الخدمات لغرض التواصل مع مستشار خارجي لحل مشكلة أولهدف التباحث، فإنه يجب الحصول على موافقة مسبقة من قبل المدير المباشر.

7.9 لا يجب إستخدام خدمات الهاتف الإنترني أو المقابلة الإنترنتية لمناقشة معلومات عمل حساسة.

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، ومدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

8.0 سياسة إستخدام البريد الإلكتروني

أ. الغرض

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

ب. المجال

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

ت. السياسة

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

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

8.3 لا يمكن إضافة أي مجموعة إخبارية غير ذات صلة بالعمل لدليل عناوين البريد الإلكتروني لمنظمتك.

8.4 لا يجوز إستخدام خدمة البريد الإلكتروني للمؤسسة لإرسال أي رسالة مزعجة للمستخدمين الآخرين سواءاً كانوا من داخل أو خارج المؤسسة.

8.5 لا ينبغي إرسال أي رسائل مؤذية أو مهينة، سواءاً داخل أو خارج المؤسسة.

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

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

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

8.9 لايصرح بإستخدام 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.

8.10 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.

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، ومدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

سياسات التحكم بالعبور

9.0 سياسة تسجيل الدخول

أ. الغرض

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

ب. المجال

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

ت. السياسة

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

9.2 كل شخص مسؤول عن اسم الدخول الممنوح له/لها.

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

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

9.5 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 لهذا المستخدم"، لأن مثل هذه الرسالة تكشف أن اسم الدخول صالح وموجود وتمنح الفرصة للمهاجم فقط بتخمين كلمة السر.

9.6 نظام الدخول يجب أن يظهر تاريخ ووقت آخر دخول، ذلك بأن هذا سينبه المستخدم لأي إستخدام للنظام باسمه بواسطة شخص غير مفوض.

9.7 يجب أن يخرج النظام تلقائيا وذلك بعد عشرة دقايق من عدم الفاعلية أو بعد أي فترة زمنية محدده من قبل مسؤول أمن المعلومات،

9.8 في حالة ما كان مهام العمل تعتمد على اسم المستخدم العام، فإنه يجب تغيير اسم المستخدم لآخر فريد.

9.9 يجب تطبيق نظام دخول مبني على الوقت لدخول المستخدم، كلما أمكن.

9.10 في حالة ما إذا كان النظام الأساسي للمؤسسة حساس، فإنه يجب منع المستخدم من الدخول إلى نظام التشغيل سطر الأوامر(cmd).

9.11 في حالة إصدار اسم دخول جديد، فإنه يتوجب إستخدام نموذج تأشيري ،إما مطبوع أو كجزء من عمل برنامج، يحدد الصلاحيات الممنوحة لهذا الإسم.

9.12 يجب مراجعة الصلاحيات الممنوحة لكل أسماء الدخول وذلك خلال فترات منتظمة وبالتعاون مع موظفين الموارد البشرية.

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

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

9.15 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.

ث. الإلزام

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

ج. المسؤولية

جميع الموظفين، ومدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

10.0 سياسة حماية كلمة السر

أ. الغرض

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

ب. المجال

المجال لهذه السياسة يتضمن كل الموظفيين بغض النظر عن مواقعهم.

ت. السياسة

10.1 جميع كلمات السر الإفتراضية يجب تغييرها بواسطة المستخدم وذلك قبل إستخدام النظام.

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

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

10.4 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.

10.5 يجب ان تكون كلمة السر مختلفة عن آخر 6 كلمة سر تم إستخدامها.

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

10.7 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.

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

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

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

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

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، ومدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

سياسات الشبكة

11.0 سياسة أمن الجدار الناري والموجه

أ. الغرض

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

ب. المجال

هذه السياسة تغطي الجدران النارية والموجهات **(Routers)** في الشبكة المحيطة، كما أنها أيضا قابلة للتطبيق على الأجهزة مثل الخوادم الوكيلة أو موجهات **(Routers)** وخطوط الإشتراك الرقمي الغير متماثل(ADSLs) الذكية .

ت. السياسة

11.1 يجب وضع الموجهات**(Routers)** والجدران النارية في مكان مؤمن ومحمي مادياً.

11.2 يجب ألا يتم تهيئة حسابات الدخول المحلي على الموجه **(Router)** ، كما يجب فصل محطة إدارة الجدار الناري عن الوحدة الرئيسية.

11.3 يجب إستخدام برتوكول التحكم بالدخولTACACS Plusوذلك للتأكد من هوية المستخدم للموجه **(Router)** .

11.4 يجب تشفيير الكلمة السرية للموجهات **(Routers)** وذلك بتفعيل خاصية "تفعيل التشفير".

11.5 أي خدمة غير مرخصة وبشكل واضح على الجدار الناري، يجب منعها.

11.6 يجب تخصيص جهاز مستقل للجدار الناري ، وعدم إستخدامه لأي خدمات أو برامج أخرى.

11.7 يجب أن تقوم الموجهات **(Routers)** والجدران النارية بمنع أي عنوان برتوكول 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

11.8 يجب ألا يوجد جهاز في الشبكة الداخلية ذو عنوان خارجي (Public) .

11.9 يجب ألا يتم السماح بتوجيه بث عنوان بروتكول (Broadcast)على الجدران النارية أو الموجهات **(Routers)** .

11.10 يجب أن لا يتم توجيه المصدر على الموجهات **(Routers)** .

11.11 يجب ألا يتم تفعيل بروتوكول إدارة الشبكة البسيطة(SNMP) على أياً من الجدران النارية أو الموجهات **(Routers)** ، وفي حالة ما دعت الضرورة لتفعيل هذا البرتوكول لإدارة النظام، فإنه يجب إستخدام برتوكول لإدارة الشبكة البسيطة على أن يكون معياري ومن السلسلة الموحدة.

11.12 خدمة الإنترنت (Internet) مسموحة على الموجه (Router)

11.13 يجب تهيئة الجدران النارية لإيقاف هجوم المزامنة SYN.

11.14 يجب أن يقوم الجدار الناري بوقف عمليات الدخول بإستخدام عناوين وهمية أو عمليات تجزئة حزم البيانات أوالهجوم بإستخدام ما يعرف بالحزم الدامعة.

11.15 يجب أن يوافق مدير القسم المعني على قائمة قوانين الدخول وذلك قبل إستخدامها على الموجهات **(Routers)** .

11.16 يجب تخزين النسخة الإحتياطية من ملفات تهيئة الجدار الناري والموجهات **(Routers)**في مكان آمن.

11.17 يجب مراجعة سجل الدخول على الجدار الناري بإنتظام.

11.18 يجب أن يقوم الجدار الناري بحجب جميع عناوين الشبكة الداخلية عن العالم الخارجي.

11.19 يجب أن يقوم الجدار الناري بعمل فلتره أو ترشيح لبرامج الجافا وعنصر التحكم ActiveX.

11.20 يجب مراجعة كل الإشارات المغادرة للنظام من قبل الجدار الناري.

11.21 يجب أن يتأكد الجدار الناري من حزم البيانات على مستوى المستخدم وعلى مستوى برتوكول عنوان الإنترنت IP، بحيث تكون الفاعلية ليست المقياس.

11.22 يجب أن لا يتم عرض أي رسالة ترحيب على شاشة الدخول للموجه (Router) ولكن يجب أن تظهر بدلاً من ذلك رسالة تحذيرية: "تحذير: هذه شبكة خاصة. أي دخول غير مصرح له ممنوع منعاً باتاً. إذا لم يكن مصرح لك، سجل خروجك فوراً. سيتم محاكمة أي مخالف".

ث. التطبيق

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

ج. المسؤولية

مدير الشبكة، ومدير الجدار الناري ومسؤول أمن المعلومات.

12.0 سياسة أمن الإتصال بالطلب الهاتفي

أ. الغرض

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

ب. المجال

الهدف لهذه السياسة يتضمن كل الخطوط لغرض توصيلات الكمبيوتر والفاكس.

ت. السياسة

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

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

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

12.4 يجب أن يتم إستخدام أجهزة الفاكس لشؤون العمل فقط.

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

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

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

ث. التطبيق

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

ج. المسؤولية

جميع الموظفين، مدراء الأقسام، و مسؤول أمن المعلومات.

13.0 سياسة الشبكة الإفتراضية الخاصة(VPN)

أ. الغرض

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

ب. المجال

سياسة الشبكة الإفتراضية الخاصة تنطبق على الإتصالات إلى المؤسسةو إلى الأطراف الثالثة بما فيهم المستشارون البائعون المتعاقدون.

ت. السياسة

13.1 على إعتبار أن الشبكة الإفتراضية الخاصة هي إمتداد لشبكة المؤسسة، فإن كل قواعد الأمن تنبطق على العميل البعيد كما لو كان داخل المؤسسة.

13.2 يجب إستخدام قناة وصل آمنة وذلك لكل الإتصالات الهامة، علماً بأن الإختيار الشائع هو إستخدامIPSECللإتصال مع الشبكة الإفتراضية الخاصة كلما كان ذلك ممكن.

13.3 ينصح وبشدة إستخدام كلمة السر ولمرة واحدة.

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

13.5 جميع الملفات المنقولة من خلال الشبكة الإفتراضية الخاصة يجب أن تخضع للفحص ضد الفيروسات.

13.6 المدة اللازمة لإغلاق الإتصال أوتوماتيكياً من الشبكة الإفتراضية الخاصة هو 15 دقيقة من عدم الفاعلية.

ث. التطبيق

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

ج. المسؤولية

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

14.0 سياسة الإتصال اللاسلكي

أ. الغرض

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

ب. المجال

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

ت. السياسة

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

14.2 يجب إستخدام خادم توثيق(Authentication) قوي لتخويل التصريح للأجهزة اللاسليكة.

14.3 يجب تشفير جميع الأجهزة اللاسلكية خلال إتصالها، كلما أمكن ذلك.

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

ث. التطبيق

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

ج. المسؤولية

مدير الشبكة، مستخدم الجهاز المتنقل، ومسؤول أمن المعلومات.

15.0 سياسة الدخول عن بعد

أ. الغرض

هذه السياسة تصف الطرق المقبولة للإتصال بشبكة المؤسسة.

ب. المجال

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

ت. السياسة

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

15.2 على إعتبار أن الإتصال عن بعد هو إمتداد لشبكة المؤسسة، فإن جميع سياسات المؤسسة تنطبق على الإتصال عن بعد.

15.3 يجب أن تقوم ميزة إعادة الإتصال بالتأكد من أن الرقم المطلوب إعادة الإتصال به مخول، وذلك بالبحث عنه في قائمة الأرقام المخولة لقاعدة البيانات قبل الإتصال.

15.4 يجب أن يتم تأمين الإتصال عن بعد بإستخدام آلية تفويض قوية، كما يتم تحديدها من قبل مسؤول أمن المعلومات.

15.5 في حالة إستخدام شبكة رقمية للخدمات المتكاملة ISDN فإنه يجب إستخدام برتوكول مصادقة مصافحة الاستبيانCHAP للتوثيق.

15.6 يفضل أن يتم إستخدام جدار ناري لإتصالات الطلب الداخلي.

15.7 في حالة ما إذا كانت المؤسسة تستخدم بروتوكول ترحيل الإطارات (frame relay)، فإنه يجب القيام بعملية توثيق مناسبة لمعرفة قناة ارتباط البيانات DLCI .

15.8 يجب فحص جميع الملفات المحملة من خلال الإتصال عن بعد للتأكد من خلوها من الفيروسات.

15.9 يجب تسجيل ومراقبة كل الإتصالات عن بعد.

15.10 في حالة توظيف نظام تحري الإختراق فإنه يجب عمل تنبيه لمدير النظام كلما تم إكتشاف هجوم.

ث. التطبيق

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

ج. المسؤولية

مدير الشبكة، ومستخدم الإتصال عن بعد، ومسؤول أمن المعلومات

سياسة تطوير التطبيقات

16.0 سياسة توظيف وتطوير التطبيقات العامة

أ. الغرض

هذه السياسة تحدد متطلبات تطوير التطبيقات سواءاً كانت داخلية أو بطلب من المؤسسة.

ب. المجال

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

ت. السياسة

16.1 متطلبات الأمن الرسمي مطلوبة لكل تطويرات الأنظمة سواءاً كانت داخلية أو خارجية.

16.2 يجب عدم إستخدام أجهزة العمل للإعتبارات التجريبية.

16.3 يجب أن يتم الفصل بين بيئة الإنتاج وبيئة الإختبار/التطوير.

16.4 يجب تسجيل أي خطأ يحصل في النظام وإرساله للمبرمج الذي قام بتطوير البرنامج.

16.5 قبل أن يتم نقل النظام إلى بيئة الإنتاج (العمل الحقيقي) فإنه يجب توثيق البرنامج بشكل مناسب.

16.6 يجب ألا يتم إستخدام أي نسخ تجريبية، أو مجانية أو تحت التطوير في بيئات العمل الحقيقي إلا بموافقة الإدارة.

16.7 يجب أن يتم تثبيت منطق الملكية التجارية على الجهاز الأساسي المركزي بدلاً من أنظمة أجهزة سطح المكتب.

16.8 يجب أن تمتلك البرمجيات– الحساسة و ذات الأهمية للمؤسسة– تسوية ضمان، كما يجب أن يتم اختبارها و المصادقة عليها من قبل طرف ثالث لإثبات كفاءتها لتأدية ماهو مطلوب.

16.9 يجب أن تظهر جميع برامج الكمبيوتر، أجزاء البرامج، برمجيات الجافا الصغيرة، والوثائق بيانات حقوق النسخ.

16.10 بعد التحقق من هوية المستخدم، يجب عدم حفظ معلومات الدخول – مثل أسم المستخدم وكلمة السر– على الخادم.

16.11 جميع عمليات الدخول يجب أن تبنى على أساس " الحاجة للمعرفة".

16.12 يجب أن يكون ملف التطبيق المخزن للمعلومات محمي بكلمة سر.

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

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

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

16.16 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.

16.17 يجب أن تتبع قواعد البيانات سياسة كلمة السر.

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

16.19 عند إستخدام تطبيق مستودع البيانات (data warehouse) فإن عملية الدخول يجب أن تقتصر على الإدارة العليا والوسطى.

ث. التطبيق

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

ج. المسؤولية

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

17.0 سياسة تطوير تطبيقات الإنترنت

أ. الغرض

هذه السياسة تحدد متطلبات تطوير التطبيقات سواءاً كانت داخلية أو بطلب من المؤسسة.

ب. المجال

هذه السياسة ملائمة لجميع تطبيقات الإنترنت والتي تطور حالياً أو تم تطويرها أو سيتم تطويرها في المستقبل.

ت. السياسة

17.1 يجب إنشاء أسم دخول وكلمة سر مناسبين لمستخدم تطبيق الإنترنت على أن يتم إستخدام برتوكول طبقة الوصلات أو المقابس الآمنة"SSL" لأي صفحة تتواصل مع المستخدم بإستخدام اسم المستخدم وكلمة السر.

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

17.3 يفضل أن يتم حفظ كلمة السر باستخدام طريقة التمويه أحادية الاتجاه (Hash function).

17.4 يجب إستخدام قناة مؤمنة وذلك للبيانات ذات الطبيعة السرية.

17.5 يجب أن يمسح زر العودة للخلف كل الحقول ذات البيانات الهامة.

17.6 يجب أن يكون للإتصال بواسطة طبقة الوصلات أو المقابس الآمنةSSL وقت إنتهاء محدد.

17.7 في حالة حدوث اي خطأ، فإنه يجب برمجة التطبيق بحيث يخلق صفحة خطأ متعارف عليها، بدلا من رسالة الخطأ المولدة من قبل النظام والتي قد تقوم بكشف معلومات عن الشبكة الداخلية.

17.8 خادم الإنترنت يجب ألا يقدم معلومات اعلانية للجميع عن تفاصيل الخادم.

17.9 يجب ألا تكون قائمة الدليل للواجهة البينية الثنائية للبوابة المشتركة (API) متاحة للعميل.

17.10 يجب أن يتم التحقق من المعطيات والكلمات المدخلة بوساطة العميل وذلك قبل التنفيذ، وذلك لإحتمالية تحويل إستخدام هذه المدخلات لاختراق قواعد البيانات.

17.11 يجب أن يكون هنالك خطة منهجية للإستجابة للإختراقات في حالة حدوث أي اختراق على الخادم أو في حالة إنتهاك للأمن.

17.12 يتعين القيام بإختبار للإختراق على التطبيق، كما يحدد من قبل مسؤول أمن المعلومات.

ث. التطبيق

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

ج. المسؤولية

مدير تكنولجيا المعلومات، محلل النظم، مدير موقع الإنترنت مبرمج موقع الإنترنت ومسؤول أمن المعلومات.

18.0 سياسة أمن مركز بيانات/غرفة الكمبيوتر

أ. الغرض

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

ب. المجال

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

ت. السياسة

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

18.2 لا يسمح بالزيارات أو الجولات في غرفة الكمبيوتر.

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

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

18.5 يجب توفير نظام إنذار ومقاومة حرائق مناسب.

18.6 يجب أن يتم تطبيق ومراقبة نظام تحكم بالرطوبة.

18.7 يجب أن يتم المحافظة ومراقبة درجة الحرارة بحدود مناسبة.

18.8 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. آخذين بعين الإعتبار أن هذه الإجراءات يجب أن تراجع بإستمرار وخلال فترات منتظمة.

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

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

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

18.12 يمنع إستخدام الهاتف النقال في مركز البيانات.

ث. التطبيق

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

ج. المسؤولية

مسؤول أمن المعلومات، ومدير تكنولجيا المعلومات.

19.0 سياسة وسائط التخزين

أ. الغرض

هذه السياسة تناقش متطلبات التعامل مع وسائط التخزين.

ب. المجال

هذه السياسة قابلة للتطبيق على جميع وسائط التخزين .

السياسة

19.1 يجب أن يتم عمل قائمة بجميع وسائط التخزين الهامة، على أن يتم حفظها في مكتبة وسائط التخزين الآمنة.

19.2 يجب أن يتم عنونة كل الوسائط بشكل ملائم.

19.3 يجب تدمير جميع وسائط التخزين مادياً قبل التخلص منها.

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

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

ت. التطبيق

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

ث. المسؤولية

مسؤول أمن المعلومات، ومدير تكنولجيا المعلومات

20.0 سياسة أمن الخادم

أ. الغرض

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

ب. المجال

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

ت. السياسة

20.1 يجب وضع الخادم في منطقة مادية آمنة.

20.2 يجب أن يتم توثيق جميع الإعدادات الخاصة بالخوادم، على أن يتم الموافقة على هذه الوثائق من قبل مدير تكنولجيا المعلومات ومسؤول أمن المعلومات.

20.3 يجب أن يمتلك كل خادم وثيقة للتهيئة و لنسخة نظام التشغيل المستخدم، وللرقع (patches) المثبتة، ولطريقة عمل النسخ الإحتياطية والإسترجاع.

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

20.5 يجب أن يوافق مسؤول أمن المعلومات على كل إعدادادت الخوادم.

20.6 يجب أن يتم تعطيل الخوادم الغير ضرورية، مثل خادم الإنترنت وغيرها.

20.7 يجب مراقبة سجل الخادم بأساس منتظم، كما يتم تحديده من قبل مسؤول أمن المعلومات.

20.8 جميع الرقع الأمنية يجب أن تثبت على الخادم بعد التأكد من أن ليس لها أي تأثير سلبي على التطبيقات المدارة.

20.9 جيمع الحسابات التلقائية أو الزائرة سوف يتم إما تعطيلها أو تغيير كلمة السر لها.

20.10 إذا ما لزم الأمر لإدارة الخادم عن بعد، فإنه يجب إستخدام قناة آمنة لهذا الغرض.

20.11 يجب إستخدام الحساب المتحكم بالخادم المستخدم الأول أو المستخدم الجذري فقط عند الحاجة.

20.12 سيقوم مسؤول أمن المعلومات بعمل بمراجعة دورية.

ث. التطبيق

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

ج. المسؤولية

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

سياسات إدارة العمليات

21.0 سياسة إدارة التهيئة

أ. الغرض

هذه السياسة الأمنية تتناول التوثيق المناسب لتهيئة الأنظمة الهامة.

ب. المجال

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

ت. السياسة

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

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

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

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

21.5 يتعيين موافقة مسؤول أمن المعلومات على كل وثائق التهيئة.

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

ث. التطبيق

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

ج. المسؤولية

مدير النظام، مسؤول أمن المعلومات، ومدير تكنولجيا المعلومات.

22.0 سياسة إدارة التغيير

أ. الغرض

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

ب. المجال

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

ت. السياسة

22.1 يجب إستخدام الإجراءات والأساليب المعيارية للتعامل بفاعلية وحسم مع التغييرات و للتحكم بالتعديلات.

22.2 يجب توثيق كل التغييرات، والحصول على موافقة مسبقة لكل التغييرات المطبقة على أنظمة الإنتاج الحيوية..

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

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

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

22.6 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.

22.7 متى دعت الحاجة لتغيير برنامج التطبيق، أو برنامج النظام، أو الشبكة المحلية او أي من المعدات، فإن التغيير يجب أن يصرح ويعتمد بالشكل المناسب.

22.8 كل تغيير يجب أن يختبر بالكامل، ويوثق تماماً.

22.9 يجب أن تتم التغيرات 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.

22.10 يجب ان يتم الموافقة على التغييرات بعد القيام بدراسة كافية للآثار المصاحبة والمترتبة على ذلك.

22.11 بمجرد الموافقة على التغيرات، فإنه يجب إدخالها في سجل إدارة التغيير.

22.12 يجب أن يتم إختبار التغييرات بشكل وافي، وعرض النتيجة على المدير المختص.

22.13 يجب أن يتم تقديم تقرير ملخص إدارة التغيير إلى الإدارة الأعلى أسبوعياً.

ث. التطبيق

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

ج. المسؤولية

مدير النظام، مسؤول أمن المعلومات، ومدير تكنولجيا المعلومات.

23.0 سياسة إخراج المطبوعة والتوزيع

أ. الغرض

هذه السياسة تحدد المتطلبات للمخرجات المطبوعة ولتوزيعها.

ب. المجال

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

ت. السياسة

23.1 يجب أن يكون لجميع التقارير الهامة المولده بالكمبيوتر مستوى تصنيفي، وذلك بناءاً على أهمية هذا التقرير

23.2 مالك التطبيق سيحدد مستوى التصنيف.

23.3 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.

23.4 سيقوم مسؤول أمن المعلومات من التأكد من أن الإجراءات متوفرة للتأكد من أن التقرير يذهب فقط للشخص المخول.

23.5 يقع على عاتق الشخص الذي يطبع التقرير مسؤولية التكفل بالحماية المناسبة للمعلومات التي يحتويها.

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

ث. التطبيق

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

ج. المسؤولية

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

سياسات إستمرارية العمل

24.0 سياسة إستمرارية العمل العامة

أ. الغرض

الغرض من هذه السياسة هو تقديم إرشادات متعلقة بإستمرارية العمل.

ب. المجال

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

ت. السياسة

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

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

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

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

24.5 يجب تحديث جميع الوثائق المتعلقة بإستمرارية العمل بإنتظام.

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

ث. التطبيق

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

ج. المسؤولية

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

25.0 سياسة الإسترداد والنسخ الإحتياطي(Recovery & Back up)

أ. الغرض

هذه السياسة تخصص مقاييس الإسترداد والنسخ الإحتياطي للمؤسسة.

ب. المجال

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

ت. السياسة

25.1 يجب أن يكون النسخ الإحتياطي لكل الأجهزة الهامة، شاملاً الخادم(Server) وأدوات الإتصال وأدوات وبرامج المهمة الحاسمة، مكفول.

25.2 سوف يتم تحديد عدد مرات عمل النسخ الإحتياطي وذلك بناءاً على طبيعة التطبيق المستخدم.

25.3 طريقة النسخ الإحتياطي المفضلة هي "النسخ الاحتياطي الكامل" يتبعه "النسخ الإحتياطي التفاضلي".

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

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

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

25.7 يجب ألا تنتهك عملية النسخ الإحتياطي خصوصية النظام.

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

25.9 يجب فحص البيانات المؤرشفة بإستمرار.

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

25.11 في حالة ماإذا كان عملاء النسخ الإحتياطي الموزعين غير متوفرين، فإنه يجب وضع بيانات العمل الهامة في ملف على الخادم لعمل نسخ إحتياطي له، حيث سيقوم مسؤول أمن المعلومات بعمل الترتيبات اللازمة. وسيقوم مسؤول أمن المعلومات، بالتشاور مع مدير تكنولجيا المعلومات، بعمل الترتيب للقفز الألكتروني؛ أي تخزين بيانات النسخ الإحتياطية خارج الموقع.

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

ث. التطبيق

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

ج. المسؤولية

كل الموظفين، ومسؤول أمن المعلومات ومدير تكنولجيا المعلومات

سياسات الطرف الثالث والموظفين

26.0 سياسة الموظفين

أ. الغرض

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

ب. المجال

هذه السياسة تنطبق على كل الموظفين ذوي العقود أو الثابتين.

ت. السياسة

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

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

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

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

26.5 ستقوم إدارة الموارد البشرية من التأكد من أنه يتم الفصل بين الواجبات وتدوير الموظفين في العمل، إينما أمكن.

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

26.7 ستقوم إدارة الموارد البشرية من التأكد من أنه تم حذف كل حسابات الكمبيوتر للموظف وذلك قبل التسوية النهائية له/ها.

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

ث. التطبيق

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

ج. المسؤولية

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

27.0 سياسة الطرف الثالث

أ. الغرض

هذه السياسة تختص بالإرشادات والمقاييس المتعلقة بالطرف الثالث والمورد الخارجي.

ب. المجال

هذه السياسة تنطبق على الأطراف أياً كانوا، سواء موردين، متعهدين، مستشاريين أو موردين خارجيين مختصيين.

ت. السياسة

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

27.2 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.

27.3 يجب تحديد دور ومسؤوليات الطرف الثالث بوضوح.

27.4 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.

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

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

ث. 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.

ج. المسؤولية

رؤساء الأقسام، الموارد البشرية، ومسؤول أمن المعلومات، ومدير تكنولجيا المعلومات.