بسم الله الرحمن الرحيم

السلطة الوطنية الفلسطينية
مجلس الوزراء
الأمانة العامة

Palestinian National Authority
Council of Ministers
Cabinet Secretariat

الإشارة (أ.ع.م.و/2012/ 375)

19 آذار 2012

معالي الأخ د. مشهور أبو دقة حفظه الله
وزير الاتصالات وتكنولوجيا المعلومات

الموضوع: المصادقة على وثيقة ونظام أمن المعلومات

تحية طيبة وبعد،،،

تهديكم الأمانة العامة لمجلس الوزراء أطيب تحياتها، وتعلمكم بقرار مجلس الوزراء الصادر في جلسته الأسبوعية رقم (127) بتاريخ 2012/03/14م، والقاضي بالمصادقة على وثيقة ونظام أمن المعلومات، وذلك وفقاً لقرار مجلس الوزراء المرفق.

يرجى من معاليكم التكرم باتخاذ الإجراءات اللازمة لتنفيذ القرار.

وتفضلوا بقبول فائق الاحترام والتقدير،،،

د. نعيم أبو الحمص
أمين عام مجلس الوزراء

مرفق: القرار المذكور.
الوثيقة والنظام المذكورين.

نسخة: دولة رئيس الوزراء/ وزير المالية حفظه الله

السلطة الوطنية الفلسطينية
الأمانة العامة لمجلس الوزراء
Palestinian National Authority
Cabinet Office

دولة فلسطين
رئاسة الوزراء
State of Palestine

علاء كميل/Log-op

بسم الله الرحمن الرحيم

السلطة الوطنية الفلسطينية

مجلس الوزراء

قرار مجلس الوزراء رقم (٤٥/13/127/م.و/س.ف) لعام 2012م

بشأن المصادقة على وثيقة ونظام أمن المعلومات

بناءً على الصلاحيات المخولة لنا قانوناً

وتنسيب وزير الاتصالات وتكنولوجيا المعلومات

وبناءً على مقتضيات المصلحة العامة

وبعد الاطلاع على القانون الأساسي المعدل لسنة 2003م وتعديلاته؛

وعلى قانون تنظيم الموازنة العامة والشؤون المالية رقم (07) لسنة 1998م وتعديلاته؛

وعلى قرار مجلس الوزراء رقم (13/109/01/م.و/س.ف) لعام 2011م؛

وعلى قرار مجلس الوزراء رقم (13/123/02/م.و/س.ف) لعام 2012م؛

قرر مجلس الوزراء في جلسته المنعقدة بمدينة رام الله بتاريخ (2012/03/14م) ما يلي:

المادة الأولى

المصادقة على وثيقة سياسة أمن المعلومات، والمرفق بهذا القرار.

المادة الثانية

المصادقة على النظام الداخلي للفريق الوطني لأمن الأنظمة والمعلومات، والمرفق بهذا القرار.

المادة الثالثة

إدراج موازنة الفريق الوطني لأمن الأنظمة والمعلومات ضمن المركز المالي لوزارة الإتصالات وتكنولوجيا المعلومات في الموزانة العامة للسلطة الوطنية الفلسطينية للعام 2012م.

المادة الرابعة

على الجهات المختصة تنفيذ أحكام هذا القرار كل فيما يخصه، ويعمل به من تاريخ صدوره، وينشر في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ 2012/03/14م.

الواحد والعشرين من ربيع الآخر لعام 1433هـ.

سلام فياض

رئيس الوزراء

دولة فلسطين رئاسة الوزراء

L.D

وثيقة سياسة أمن المعلومات

إعداد:

الفريق الوطني لأمن الأنظمة والمعلومات

كانون ثاني ٢٠١٢

فهرس المحتويات

١. ضبط التعديلات على الوثيقة

تفاصيل الوثيقة			
المسمى \ الدائرة	مثال [دائرة أمن المعلومات أو دائرة تقنية المعلومات] [أو مدير دائرة أمن المعلومات]		
الوثيقة	مثال [سياسة أمن المعلومات]		
تاريخ الإصدار			
التصنيف	○ عام	○ للاستخدام الداخلي	⊙ سري
عدد الصفحات			
رقم الإصدار			
نوع الوثيقة	⊙ مسودة	○ إصدار	
تصنيف فئة الوثيقة	أمن معلومات		

سجل التعديلات			
التاريخ	رقم		ملاحظات
	١.١		المسودة الأولى

٢. الموافقة على التعديلات

٣. التوزيع

رقم النسخة		
١		
٢		
٣		

٤. التخزين

يجب تخزين هذه الوثيقة

موقع			
مثال: [الموقع الالكتروني للمؤسسة]	مثال: [نسخة الكترونية]	مثال: [مؤسسة الاتصالات وتكنولوجيا المعلومات]	

١. المقدمة:

تعتمد مؤسسات السلطة الوطنية على أنظمة المعلومات والتقنيات الحديثة والمعلومات في عملها، وتسريب معلومات من هذه المؤسسات عن طبيعة عملها أو معلومات تتعلق بالمواطنين يؤدي إلى إلحاق خسائر مادية ومعنوية بالمؤسسة، لذلك يجب حمايتها والتاكد من خصوصيتها Confidentiality وتكاملها Integrity وتوفرها availability. وللحفاظ على امن المعلومات يجب وضع السياسات والاجراءات لكيفية حماية المعلومات. حيث أن الحفاظ على أمن هذه الأنظمة والمعلومات يعتبر من الاهتمامات الرئيسية للإدارة العليا في المؤسسة التي تعمل جنباً إلى جنب مع مجلس الوزراء لإطلاق ودعم الجهود المبذولة لتعزيز أمن المعلومات. وتعتبر هذه السياسة من العناصر الرئيسية في أمن المعلومات.

إن العمل في أمن المعلومات يحتاج إلى العمل بروح الفريق ويحتاج إلى المشاركة والدعم من كافة الموظفين الذين يستخدمون أنظمة المعلومات، وإدراكاً منا إلى أهمية العمل بروح الفريق فإن هذه السياسة توضح مسؤوليات المستخدمين والخطوات الواجب إتباعها للمساعدة في حماية المعلومات وأنظمة المعلومات، كما تتضمن هذه السياسة الطرق الواجب إتباعها في مواجهة التهديدات المختلفة مثل الاستخدام غير المسموح به والاختراق ونشر ونسخ وتغيير وتدمير وفقد المعلومات وسوء الاستخدام ومنع الاستخدام وغيرها من التهديدات. يجب ان يتم تحديد المخالفات، العقوبات، والإجراءات التأديبية المترتبة على عدم الالتزام وانتهاك سياسات وإجراءات أمن المعلومات المعتمدة في المؤسسة وكذلك يجب تحديد الجهة المخولة والمسؤولة عن تنفيذ العقوبات، وتحديد آلية التبليغ عن المخالفات.

لقد تم كتابة وتعميم هذه السياسة لتحديد الاتجاه المناسب للتعامل مع أمن المعلومات في المؤسسة وبما يتناسب مع المعايير العالمية بهذا الشأن وخاصة معايير أل ISO 27001. إن الأهداف المطلوب تحقيقها من هذه السياسة تتحقق بتطبيق بنود هذه السياسة بالطريقة الأنسب لطبيعة عمل وبيئة المؤسسة. فعلى سبيل المثال البند رقم "١" "صلاحيات الاستخدام" في بيان السياسة العامة يمكن تحقيقه من خلال: إما تطوير وتطبيق إجراء عمل أو أكثر بما يتماشى مع هذه السياسة أو من خلال فرز سياسة متخصصة لتناول هذا البند بشمولية وتخصص أو من خلال الطريقتين معا: الإجراءات وفرز السياسات المتخصصة.

وعلى كل مؤسسة اصدار التعليمات بما يتماشا مع هذه السياسات العريضة في هذه الوثيقة كل فيمل يخصه بما ينسجم مع طبيعة عمل وهكلية المؤسسة.

٢. الأهداف

تُطبق هذه السياسة على كافة الأنظمة والشبكات التي تملكها أو تديرها المؤسسة ، وتشمل المعدات وأنظمة التشغيل والتطبيقات المختلفة وتغطي كافة المعلومات والبيانات التي يتم التعامل معها من خلال أنظمة الحاسوب والشبكات المختلفة. يجب أن يتم تطبيق كل البنود الواردة في هذه السياسة كحد أقصى مع نهاية العام ٢٠١٢.

٣. الفئة المستهدفة

يجب على جميع موظفي المؤسسة الالتزام بجميع سياسات أمن المعلومات التي تتضمنها هذه السياسة والسياسات الأخرى ذات الصلة، والموظف الذي ينتهك أي سياسة من سياسات أمن المعلومات يضع نفسه تحت طائلة المسؤولية ويعرض نفسه للعقوبات التي تصل إلى الفصل من العمل.

٤. الالتزام بسياسة أمن المعلومات

التقيد بتعليمات هذه الوثيقة مطلوب من جميع موظفي المؤسسة، المستشارين، والأطراف الأخرى الذين يتم التعاقد معهم من قبل المؤسسة أو من قبل أي طرف آخر للعمل بالمؤسسة. يجب الالتزام بالتعليمات والمسؤوليات والسياسات ضمن هذه الوثيقة لضمان السرية، والسلامة، وعدم الانقطاع للمعلومات المتعلقة بعمل المؤسسة.

٥. تحديد الثغرات والمخاطر

هناك العديد من الأدوات والوسائل التي تساعد في تحليل النظام وإيجاد الثغرات الممكن استغلالها في النظام. بجانب المخاطر الإلكترونية، هناك مخاطر مادية مثل سرقة وسائط التخزين. القائمة التالية توضح بعض المخاطر المحتملة:

- تعديل قواعد البيانات Database modification
- التهديد من قبل الاشخاص المخولين للدخول Internal Attack
- التهديد الخبيث Malicious attack
- تعطل الخدمة Denial of service attack

٦. المسؤوليات

تعتمد المؤسسة أربع تصنيفات رئيسية من حيث علاقة الموظف بأنظمة المعلومات فيما يتعلق بأمن المعلومات، بحيث ينطبق واحد منها على الأقل على كل موظف يستخدم أنظمة المعلومات، وهي: ملكية النظام، تقنية المعلومات، إدارة الشبكة والنظام، والمستخدم، وتشمل هذه التصنيفات تعريف عام بالمسؤوليات مع مراعاة الحرص على تنفيذ سياسات وإجراءات أمن المعلومات:

مسؤوليات إدارة الأمن وأملكية النظام – مالكي الأنظمة والمعلومات هم مدراء الإدارات والدوائر وأعضاء الإدارة العليا أو من ينوب عنهم في المؤسسة ممن يتحملون مسؤولية تنفيذ وتطوير ومتابعة الأنظمة والبرامج والتطبيقات المختلفة التي تتعامل مع البيانات والمعلومات بما يخدم مصلحة العمل، ويجب أن يتم اعتماد مدير أمن\ مالك لكل نظام، وهو مسئول عن تصنيف المعلومات من حيث السرية ويملك قرار السماح باستخدام النظام.

مسؤوليات تقنية أمن المعلومات – يجب أن يتم تعيين فني واحد أو أكثر لكل نظام من أنظمة المعلومات أو مصادر المعلومات، وفني الأمن يمتلك الصلاحيات الكاملة لتطبيق السياسات الأمنية على النظام أو مصدر المعلومات المسئول عنه. فني الأمن وبالتعاون مع الموظفين الآخرين من دائرة تقنية المعلومات مسئول عن حماية المعلومات من المخاطر المختلفة وتنفيذ وتطبيق السياسات والإجراءات الأمنية المعتمدة، ويعتبر أي موظف فني في إدارة تقنية المعلومات فني أمن وكذلك يعتبر المستخدم فني أمن على المعلومات المحفوظة على جهاز الحاسوب الذي يستخدمه.

مسؤوليات إدارة الشبكة أو/ و النظام – لدى المدير الكثير من المسئوليات من نظم التشغيل و كلمات مرور تأتي بحسابات مستخدمين و المحولات (راوتر) والموجهات الافتراضية، لذا يجب أن يؤخذ الحذر فور استعماله، كإجراء أولي مناسب في هذا الصدد هو تغيير أسماء حسابات المدراء وتعطيل أي حساب موجود مسبقًا وعدم استخدامه لاحقا مهما كان عدد هذه الحسابات. إن ترك هذه الحسابات وكلمات المرور كما هي يجعل من السهل على المخترقين التسلل إلى الشبكة.

مسؤوليات المستخدم – المستخدم مسئول عن الالتزام بسياسات ومعايير وإجراءات أمن المعلومات المعتمدة وتعلمها.

السياسات العامة

١. صلاحيات الاستخدام

الصلاحيات التي يملكها الموظف لاستخدام أنظمة المعلومات تعتمد على حاجات العمل، بحيث يسمح للموظف استخدام المعلومات التي تمكنه من القيام بعمله على الأنظمة المختلفة وذلك من خلال اعتماد نظام طلب صلاحيات الاستخدام والموافقة عليه من قبل مسئوله المباشر ومدير أمن \ مالك النظام قبل أن يتم إعطاء صلاحيات استخدام للموظف، ويمنع الموظف من استخدام أو محاولة استخدام المعلومات أو الأنظمة التي لا يحتاجها في عمله أو استخدامها لغير غايات وأهداف العمل.

في حال تغيير الوضع الوظيفي للموظف من حيث الترقية أو تغير مهام العمل أو النقل أو انتهاء عمله في المؤسسة أو غيره من الأسباب، يجب على مديره المباشر إبلاغ دائرة تقنية المعلومات وفني الأمن على النظام أو الأنظمة التي يستخدمها الموظف وبشكل خطي. يفضل أن يحدد تاريخ انتهاء لكل الصلاحيات لا يتجاوز السنة من تاريخ إعطاء الصلاحية، ويتم تجديدها حسب الحاجة.

٢. الإقرار والتعهد

يجب أن يوقع كل موظف يستخدم أنظمة المعلومات على إقرار وتعهد بأن الموظف قد قرأ وفهم ويوافق على الالتزام بسياسات ومعايير وإجراءات أمن المعلومات المعتمدة في المؤسسة قبل أن يتم إنشاء اسم مستخدم خاص به على أي نظام

من أنظمة المعلومات. وفي حال كان الموظف حاصل على اسم مستخدم مسبقاً فإنه يجب أن يوقع على هذا الإقرار قبل أن يتم تجديد كلمة المرور الخاصة به حيث تتم عملية تجديد كلمة المرور بشكل دوري للجميع.

٣. اسم المستخدم وكلمة المرور

يجب أن يتم إنشاء اسم مستخدم لكل موظف يستخدم أنظمة المعلومات وترتبط صلاحيات الاستخدام للموظف باسم المستخدم الخاص به، ويتحمل الموظف المسئولية الكاملة عن الأعمال التي تتم من خلال استخدام المستخدم الخاص به وكذلك اختيار كلمة مرور تتوافق مع سياسة أمن كلمة المرور التالية:

صعوبة كلمة المرور- يجب على الموظف أن يختار كلمة مرور من الصعب أن يتوقعها غيره، وأن لا ترتبط بعمل الموظف أو حياته الشخصية ويجب أن لا تكون كلمة معروفة أو جزء من مقولة مشهورة، مثل رقم تسجيل السيارة، اسم الابن، رقم الهاتف الجوال، رقم الموظف، اسم مكان عام، مصطلح فني أو غيرها.

حفظ كلمة المرور- يجب على الموظف أن يستخدم كلمة مرور من السهل عليه حفظها وأن يكون من الصعب على غيره توقعها وذلك من خلال:

- دمج مجموعة كلمات مع بعضها البعض.
- استخدام الأحرف الكبيرة والصغيرة في كلمة المرور.
- استخدام الأرقام وعلامات الترقيم في كلمة المرور.
- إنشاء كلمة من الأحرف الأولى لعبارة مشهورة تتألف من عدة كلمات.
- تعمد كتابة الكلمات خطأ.
- دمج عدة كلمات غير مترابطة مع بعضها البعض.

تكرار كلمة المرور- يجب على الموظف عدم إتباع نمط معين في تغيير كلمة المرور بأن يقوم بتغيير جزء من كلمة المرور مثل تغيير رقم أو غيره من الأنماط التي يسهل على الآخرين توقعها، كما يحظر عليه استخدام كلمة مرور تم استخدامها سابقاً بشكل كلي أو جزئي.

مواصفات كلمة المرور- يجب أن تكون كلمة المرور مكونة من ٨ مقاطع على الأقل (تشمل حروف صغيره وكبيرة وأرقام ورموز)، كما يجب أن يتم تغييرها مره واحده على الأقل كل ٦٠ يوم، وفي حال شك الموظف أن كلمة المرور الخاصة به قد تم اكتشافها من قبل شخص أخر فيجب عليه أن يقوم بتغييرها فوراً.

تخزين كلمة المرور- يحظر تخزين كلمة المرور الكترونياً على أجهزة الحاسوب في أي شكل من الأشكال مثل تخزينها داخل ملف أو تفعيل حفظ كلمة المرور على البرامج والأنظمة أو غير ذلك ، كما يحظر كتابتها وحفظها على الورق.

مشاركة كلمة المرور – يمنع بشكل مطلق مشاركة كلمة المرور الخاصة بالموظف أو إعطائها لشخص أخر، ولا يحق لأي أحد بما فيه فريق عمل إدارة تقنية المعلومات أن يطلب من الموظف الكشف عن كلمة المرور الخاصة به والحالة الوحيدة التي تكون فيها كلمة المرور معروفة لشخص آخر غير الموظف فقط عن إصدارها لأول مرة من قبل مدير النظام ويجب على الموظف أن يقوم بتغييرها فوراً عند استلامها، وإذا كان هناك حاجة لمشاركة الملفات بين أكثر من موظف فيجب استخدام تقنيات مشاركة الملفات المعتمدة من دائرة تقنية المعلومات وليس الاشتراك في استخدام كلمة المرور من قبل أكثر من موظف.

إيقاف كلمة المرور – يجب إيقاف كلمة المرور في الحالات التالية :

- تكرار إدخال كلمة مرور أكثر من ثلاثة محاولات
- استقالة أو توقف عمل احد الموظفين أو أصحاب الطرف الثالث
- في حالة اكتشاف أي نوع من التهديد قد يسبب ضرر للمنشأة.

٤. عملية أخذ النسخ الاحتياطية و الاستعادة من الكوارث

تعتبر عملية أخذ النسخ الاحتياطية من الأمور والإجراءات المهمة التي يجب على المؤسسة مراعاتها وإتباعها بآلية مناسبة.

من الأفضل تحديد المعلومات الحساسة و التي تحتاج إلى أن تنسخ احتياطيًا. ليس هناك حاجة لإنفاق المزيد من المال والوقت على شيء لا يمثل أي قدر من الأهمية. النسخ الاحتياطي مهم إلى درجة كبيرة لأسباب كثيرة منها:

- فشل وانهيار النظام و فقد جميع البيانات.
- تلقي فيروسات مدمرة.
- سرقة جهاز الحاسب نفسه.
- تشويه أو تحطيم البيانات على يد المخترقين
- المستخدم يحذف ملفاته بدون قصد.
- كوارث طبيعية – حريق ,فيضان, إعصار.

ونظرًا لأهمية النسخ الاحتياطي فإن السياسات يجب أن تخصص خططًا لكل من :

- جدول النسخ الاحتياطي – متى وكل كم من الوقت يعاد النسخ
- ما نوع النسخ الاحتياطي
- ما نوع الأدوات المستخدمة في عملية النسخ
- أين سيتم تخزين النسخ الاحتياطية -في نفس الموقع في مكان آمن أم خارج الموقع أم كلاهما

٥. إطلاع طرف خارجي على المعلومات

تعتبر جميع المعلومات في المؤسسة خاصة ما لم يتم نشرها ضمن وسائل الإعلام العامة ويمنع إطلاع أطراف خارجية عليها، وأي طرف خارجي يحتاج الاطلاع على معلومات خاصة بالمؤسسة يجب أن يتبع الإجراءات الداخلية المتبعة لذلك بالإضافة إلى الحصول على الموافقة الخطية من الموظف الذي تم تعينه مدير أمن النظام وتوقيع اتفاقية عدم نشر المعلومات المعتمدة في المؤسسة. في حال تم فقد أو تسريب معلومات خاصة بالمؤسسة لطرف خارجي غير مسموح له الإطلاع عليها أو لمجرد الشك في حدوث ذلك يجب على الموظف إبلاغ دائرة تقنية المعلومات أو الموظف المسؤول عن إدارة أمن المعلومات مباشرة وبشكل خطي.

٦. حماية المكاتب

يجب أن يتم حماية المكاتب والقاعات والمواقع التي تحتوي أجهزة حاسوب أو معلومات هامة بحيث يكون الدخول إليها محصوراً في الموظفين التي تتطلب مهام عملهم ذلك وذلك حسب السياسة الخاصة بحماية مباني المؤسسة (Physical Security)، كما يجب على كافة الموظفين تثبيت شاشات أجهزة الحاسوب التي يعملون عليها في وضعية لا تسمح للآخرين بالاطلاع على محتواها.

٧. الشبكة الداخلية

يجب أن يتم حماية جميع الأنظمة والمعدات وأجهزة الحاسوب الشخصية التي تحتوي على معلومات أو تتعامل بالمعلومات الخاصة بالمؤسسة والمتصلة بالشبكة الداخلية بشكل دائم أو مؤقت بأنظمة التحكم بالنفاذ المعتمدة من قبل دائرة تقنية المعلومات والتي تعتمد على اسم المستخدم لتحديد الصلاحيات التي يملكها الموظف، ويجب على كافة الموظفين استخدام شاشات التوقف المحمية بكلمات المرور والتي تقوم بقفل الشاشة بعد فترة من توقف العمل على الجهاز إلى حين إعادة إدخال كلمة المرور الخاصة بالمستخدم، كما يجب استخدام خاصية إخراج المستخدم عن الأنظمة المختلفة بعد فترة محددة من توقفه عن العمل.

٨. الشبكات الخارجية

يجب أن يتم حماية الشبكات والأنظمة بحيث يكون النفاذ إليها من الخارج محمي باستخدام أنظمة التحكم بالنفاذ للتحقق من هوية المستخدم والخدمات المسوح له النفاذ إليها، كما يجب أن يتم استخدام الوسائل والآليات المعتمدة من قبل دائرة تقنية المعلومات للنفاذ للشبكات الخارجية المختلفة. أما بخصوص الاتصال بالمكاتب الفرعية للوزارة فيجب الانتباه جدا لأمن

سرية نقل البيانات بين المكاتب والمكتب الرئيسي للوزارة و ما بين المكاتب نفسها لأن هذه الخطوط تمر فيها جميع البيانات السرية و المهمة و يمكن عن طريقها في حال عدم ضمان أمانها أن تستخدم للهجوم على شبكة الوزارة.

٩. العمل عن بُعد

يسمح للموظف القيام بالعمل عن بُعد بعد الحصول على موافقة مديره المباشر وذلك بناءً على مهام العمل المكلف بها، ويجب على الموظف الالتزام بسياسة أمن المعلومات المتعلقة بالعمل عن بُعد.

١٠. شبكة الانترنت

يجب أن يكون استخدام الانترنت للقيام بمهام العمل، والحصول على صلاحية استخدام الانترنت يتطلب موافقة المسئول المباشر للموظف، ويمنع استخدام شبكة الانترنت لتمثيل المؤسسة بأي شكل من الأشكال مثل المجموعات الحوارية والقوائم البريدية وغيرها من الوسائل لغير المخولين بذلك، هذا ويمنع استخدام شبكة الانترنت لعمل ترتيبات تجارية أو لتبادل معلومات سرية مثل كلمات المرور أو أرقام بطاقات الائتمان ما لم يتم اعتماد ذلك من قبل دائرة أمن المعلومات، كما ويمنع نشر معلومات خاصة بالمؤسسة على شبكة الانترنت ما لم يتم الموافقة على ذلك من مدير أمن \ مالك النظام الخاص بالمعلومات المراد نشرها ودائرة أمن المعلومات، وتقوم المؤسسة بمراقبة استخدام الانترنت للتأكد من الالتزام بسياسات أمن المعلومات وأن استخدامها يتم للقيام بمهام العمل.

١١. البريد الإلكتروني

يجب أن يتم استخدام نظام البريد الالكتروني الخاص بالمؤسسة في كافة المراسلات المتعلقة بالعمل ويمنع استخدام البريد الإلكتروني الشخصي للمراسلات التي تتعلق بالعمل ما لم يتم الحصول على موافقة المسئول المباشر للموظف ودائرة تقنية / أمن المعلومات، كما يمنع تبادل أي معلومات سرية بواسطة البريد الإلكتروني مثل كلمات المرور وأرقام بطاقات الائتمان.

إضافة إلى ذلك يجب عدم استخدام البريد الالكتروني بطريقة غير مقبولة، فقد يتسبب البعض في جعل المؤسسة هدفًا للرسائل التطفلية وغير الأخلاقية، كذلك عدم استخدام لغة تعسفية تجاه زملاء العمل أو عملاء المؤسسة، أو استخدام البريد في معاملات تجارية خاصة. من الجيد استخدام برامج SPAM filters لتصفية الرسائل من وإلى المؤسسة من أجل منع أنواع معينة من الملفات يحتمل أن تحمل فيروسات أو ما شابه.

١٢. الفيروسات

يجب تركيب واستخدام برامج الحماية من الفيروسات المعتمدة من دائرة تقنية المعلومات على جميع أجهزة الحاسوب في المؤسسة، بحيث يتم تفعيل الحماية التلقائية وتفعيل التحديث التلقائي، هذا ويجب أن يتم فحص الملفات والبرمجيات التي يتم الحصول عليها من أطراف خارجية قبل أن يتم استخدامها بأي شكل على أجهزة الحاسوب، كما يحظر على الموظفين محاولة معالجة الفيروسات والقضاء عليها من دون الحصول على المساعدة الفنية اللازمة من المختصين في دائرة دعم المستخدمين وفي حال اشتباه الموظف باحتمال إصابة جهاز الحاسوب الذي يستخدمه بالفيروسات أو أن برنامج الحماية كشف أن جهاز الحاسوب مصاب بالفيروسات فيجب على الموظف فوراً التوقف عن استخدام الجهاز وفصله عن جميع الشبكات المتصل بها والاتصال بدائرة دعم المستخدمين، كما يمنع استخدام وسائط نقل البيانات المصابة بالفيروسات مثل أجهزة التخزين الخارجية وغيرها قبل أن يتم التخلص من الفيروسات والتأكد من سلامتها، وفي حال وجود احتمال أن يقوم الفيروس بتدمير المعلومات أو البرمجيات الموجودة على الجهاز يجب على الموظف وقف عمل الجهاز فوراً.

١٣. استخدام البرمجيات

تسمح المؤسسة فقط باستخدام البرمجيات التجارية والبرمجيات التي يتم تطويرها داخل المؤسسة والبرمجيات التي يتم الحصول عليها من الجهات الموثوقة لدى المؤسسة، ويمنع استخدام البرمجيات التي يتم الحصول عليها من شبكة الانترنت أو غيرها من المصادر الأخرى ما لم يتم فحصها واعتمادها من قبل دائرة تقنية / أمن المعلومات.

١٤. اعتماد البرمجيات والأنظمة

يجب اعتماد البرمجيات والمعدات والأجهزة والأنظمة الجديدة أو التعديلات التي تتم عليها من قبل تقنية / أمن المعلومات قبل أن يتم استخدامها وذلك فيما يتعلق بتوافقها مع متطلبات واحتياجات أمن المعلومات في المؤسسة.

١٥. نسخ البرمجيات

يمنع الموظفين من نسخ البرمجيات الخاصة بالمؤسسة على وسائط نقل المعلومات مثل الأقراص الليزرية أو الأقراص المرنة وغيرها من الوسائط ويمنع استخدامها على أجهزة حاسوب غير مملوكة للمؤسسة أو تزويدها لأطراف خارجية (ما لم يحصل على موافقة مسؤوله المباشر) وفقط يسمح النسخ الاحتياطي للبرمجيات.

١٦. سياسة حماية قواعد البيانات

يجب إتباع السياسات والإجراءات المقترحة التالية:

- مراجعة كل حسابات وطرق الوصول إلى البيانات ومراقبتها
- استخدام سياسية قوية لحماية اسم المستخدم وكلمة المرور.
- العمل على تقوية الخادم وقواعد البيانات (System Hardening) بحسب المعايير العالمية والنشرات الخاصة بمزود النظام.
- استخدام خيارات تشفير التي توفرها منتجات قاعدة البيانات توفير مبدأ الحماية على مراحل بما فيها جدار الحماية، مضاد الفيروس، مكتشف محاولات الاختراق وغيرها

١٧. الحماية من السرقة

يجب أن يتم حماية جميع أجهزة وأنظمة الكمبيوتر الموجودة في الأماكن المفتوحة في المؤسسة من السرقة وذلك باستخدام الوسائل المناسبة، ويجب استخدام الخزائن والقاعات المغلقة والوسائل الأخرى لحماية الخادمات الرئيسية وأجهزة ومعدات الشبكة من السرقة، ويحتاج نقل أو إخراج أجهزة الكمبيوتر ومعدات الشبكات من مكاتب المؤسسة موافقة خطية من إدارة المبنى وفني الأمن المسئول عن هذه الأجهزة والمعدات.

١٨. معايير أمن المعلومات

تعتبر سياسات وإجراءات ومعايير ومقاييس أمن المعلومات المستخدمة في المؤسسة وكل ما يتعلق بها معلومات سرية لا يسمح نشرها أو إطلاع أطراف خارجية عليها إلا بعد الحصول على الموافقة الخطية المسبقة من دائرة تقنية / أمن المعلومات.

١٩. مراقبة الأنظمة

تمتلك دائرة تقنية / أمن المعلومات موافقة رسمية من إدارة المؤسسة تسمح لها بالمراقبة والفحص والبحث في أنظمة المعلومات في أي وقت كان، وقد تتم هذه العملية بمعرفه ووجود الموظف أو غيابه وتشمل هذه الموافقة كافة أنظمة المعلومات المستخدمة في المؤسسة مثل البريد الالكتروني وأجهزة الحاسوب الشخصية والأقراص الصلبة وغيرها، ولا يتمتع الموظف بأية خصوصية في المعلومات على الأنظمة المستخدمة في المؤسسة لأن هذه الأنظمة مخصصة لإغراض العمل وليس للاستخدام الشخصي.

٢٠. الاستخدام الشخصي

إن أنظمة المعلومات الخاصة بالمؤسسة هي لاستخدامات العمل فقط ولكن يسمح الاستخدام الشخصي لهذه الأنظمة ضمن الشروط التالية:

- أخذ الموافقة اللازمة على ذلك.
- عدم التأخير أو الإضرار بالعمل.
- عدم التعارض مع عمل موظفين آخرين.
- استهلاك جزء بسيط جداً من مصادر أنظمة المعلومات.

وأي استخدام شخصي لا يتوافق والشروط السابقة يحتاج إلى موافقة مالك النظام ومدير الإدارة التي يعمل بها الموظف.

٢١. إلغاء الصلاحيات

تمتلك دائرة تقنية / أمن المعلومات الحق بإلغاء صلاحيات أي موظف في أي وقت بشكل كلي او جزئي ولفترة محدودة او غير محدودة.

٢٢. أدوات اختراق أنظمة المعلومات

يمنع امتلاك أو استخدام أو نشر أو التعامل بالأدوات والبرمجيات والأجهزة التي من الممكن أن تساعد أو تستخدم في اختراق أو محاولة اختراق أنظمة المعلومات وأنظمة الحماية المستخدمة في المؤسسة ما لم يتم الحصول على موافقة خطية مسبقة من دائرة تقنية\ أمن المعلومات.

٢٣. النشاطات المحظورة

يمنع اختراق أو محاولة اختراق أنظمة الحاسوب المستخدمة في المؤسسة في أي شكل من الأشكال، وإذا كان هناك حاجة للقيام بذلك ضمن مهام العمل فيجب الحصول على موافقة خطيه مسبقة من مدير تقنية\ أمن المعلومات تسمح للموظف القيام بذلك، ويعتبر أي اختراق أو محاولة اختراق عمل غير قانوني وانتهاك جدي ومقصود للسياسات الداخلية للمؤسسة.

٢٤. التوعية والتدريب

يجب الاهتمام من قبل المؤسسة بشكل دوري ومخطط له بنشاطات التوعية والتدريب الخاصة بأمن المعلومات لأغراض المساعدة في التنفيذ والالتزام بسياسات أمن المعلومات، تغيير ثقافة الموظف وتوجيهها للاهتمام بتنفيذ مهامه الوظيفية بشكل آمن ومضبوط، وكذلك بناء الكادر الفني القادر على التعامل مع التقنيات والمعايير المختلفة المرتبطة بأمن المعلومات.

٢٥. التقارير

يجب إبلاغ دائرة تقنية / أمن المعلومات فوراً وبشكل خطي عند وجود أي شك بانتهاك سياسات أمن المعلومات أو مهاجمة أنظمة المعلومات أو وجود فيروسات أو غيره من النشاطات التي تهدد أمن المعلومات في المؤسسة.

٢٦. سياسة حماية الأجهزة المحمولة

يجب على جميع مستخدمي الأجهزة المحمولة والتابعين لمؤسسات السلطة او الأطراف الخارجية إتباع السياسة الأمنية الخاصة من خلال:

- تشفير البيانات الخاصة بالأجهزة
- التوعية للموظفين بالية الحفاظ على الأجهزة من الضياع أو السرقة
- تحميل برامج تعقب و استعادة للأجهزة
- استخدام سياسات و إجراءات قوية للدخول و الربط للأجهزة المحمولة على الشبكات الحكومية

٢٧. سياسة استخدام الشبكات اللاسلكية

تعتبر الشبكات اللاسلكية بالمقارنة بالسلكية خطيرة و ذلك لصعوبة حمايتها وتعرضها للخطر مما يجعل حمايتها تقع على عاتق مستخدمها ووعيه أكثر من أي شئ آخر ولذلك يجب على مستخدمي مثل هذه الشبكات اتباع و مراعاة بعض الامور الهامة ومثال ذلك ما يلي:

- تغير كلمة سر الشبكة الرئيسية
- تعطيل خاصية بث اسم الشبكة (SSID)
- تشفير الشبكة اللاسلكية باستخدام لأخر إصدار بروتوكول التشفير
- تحديد عناوين الأجهزة التي تدخل على الشبكة الخاصة بالمؤسسة
- عدم الاتصال بالشبكات اللاسلكية المفتوحة
- تحديث أنظمة التشغيل لمكونات الشبكة
- استخدام عنوان الآي بي الثابت و تعطيل الدينمك آي بي
- يمنع ربط أجهزة العمل بشبكات أخرى غير شبكة المؤسسة
- يمنع استخدام الأجهزة الخاصة بالموظف على شبكة المؤسسة الا بعد الحصول على الموافقات اللازمة.

٢٨. تصنيف المعلومات والأصول

يجب تصنيف المعلومات لبيان مدى حاجتها للحماية وأولويتها والدرجة المطلوبة من الحماية عند التعامل معها. وتتفاوت درجة حساسية المعلومات وأهميتها. فقد تتطلب بعض المواد مزيدا من الحماية ومعاملة خاصة. ويجب استخدام خطة لتصنيف المعلومات لتحديد مجموعة مناسبة من مستويات الحماية وتوضيح الحاجة إلى إجراءات خاصة للتعامل مع المعلومات. وتقع على عاتق مالك الأصل مسؤولية تحديد تصنيفه بشكل دوري والتأكد من تحديثه بالمستوى المناسب.

٢٩. إدارة والتعامل مع الأحداث

يجب وضع آلية للتعامل مع أحداث أمن المعلومات على أن تتضمن هذه الآلية ما يلي :

- يجب التبليغ عن أحداث أمن المعلومات من خلال قنوات الإدارة المناسبة بأسرع وقت ممكن.
- يجب أن يطلب من جميع الموظفين والمتعهدين ومستخدمي الطرف الثالث لأنظمة المعلومات والخدمات أن يلاحظوا ويبلغوا عن أي نقاط ضعف او أحداث تلاحظ أو يشك بها في الأنظمة أو الخدمات.
- ضمان تطبيق توجه فعال وثابت لإدارة أحداث أمن المعلومات.
- يجب تحديد المسؤوليات والإجراءات الإدارية لضمان الاستجابة السريعة والفعالة والمؤسسة لأحداث أمن المعلومات.
- يجب وضع الآليات لتحديد أنواع وأحجام وتكاليف أحداث أمن المعلومات حتى يمكن تقييمها ومراقبتها.

٣٠. التخلص من المعلومات والوسائط

يجب التخلص من الوسائط والمعلومات بشكل آمن وسليم حين تنتهي الحاجة إليها وبعد انتهاء الدورة المستندية (Retention Period) التي تعتمدها للمؤسسة وذلك باتباع الإجراءات الرسمية. يجب أن تعمل الإجراءات الرسمية للتخلص الآمن من الوسائل على الحد من خطر تسرب المعلومات الحساسة للأشخاص غير المصرح لهم. ويجب أن تتناسب إجراءات التخلص الآمن من الوسائط التي تحتوي معلومات حساسة مع درجة حساسية تلك المعلومات.

٣١. صيانة الأجهزة التي تحتوى على بيانات خاصة بالعمل

يجب مراعاة سرية، سلامة، توفر، وعدم ضياع المعلومات الموجودة على الأجهزة التي تمتلكها المؤسسة سواء المعلومات الموجودة على الأقراص الصلبة أو غيرها من أنواع الذاكرة المختلفة أو تلك المعلومات الموجودة على هذه الأجهزة لأغراض العمل وذلك عند الحاجة لصيانة هذه الأجهزة سواء من قبل الطواقم التابعة للمؤسسة أو من قبل الأطراف الخارجية التي تتعامل معها المؤسسة وبالطريقة التي تتناسب مع السياسات التي تعتمدها المؤسسة والخاصة بصيانة الأجهزة.