سياسة حماية البيانات

أولاً: سياسات تصنيف المعلومات:

مقدمة:

من الضروري أن تقوم "جهة العمل" بتصنيف أصول معلوماتها للمساعدة في إدارتها وحمايتها، وذلك من خلال النظر في مدى إمكانية أن يُلحق ضرر بـ "جهة العمل" في حالة لنشر غير المقصود أو التعديل أو الخسارة لهذه المعلومات. ويمكن القيام بذلك عن طريق تحديد ما ينبغي حمايته وما يمكن الاطلاع عليه ومن المصرّح له بذلك من الموظفين والعامة والأطراف الأخرى

الغرض:

تصف سياسة تصنيف المعلومات المبادئ التي يجب اتباعها لحماية المعلومات، وذلك من خلال تحديد كيف ولمن يمكنك نشر هذه المعلومات بتصنيف معين من أجل الحفاظ على خصوصية وسلامة وتوفر أصول المعلومات بـ "جهة العمل". ومن خلال إنشاء هذا النظام، ستحدد هذه السياسات متطلبات التعامل مع البيانات لتوفير أساسيات حمايتها في "جهة العمل."

النطاق:

تسري هذه السياسة على جميع البيانات أو المعلومات التي يتم إنشاؤها أو جمعها أو تخزينها أو معالجتها في "جهة العمل"، سواء كانت في شكل إلكتروني أو غير إلكتروني، وبصرف النظر عن مكان وجود هذه البيانات أو نوع الجهاز المخزنة به، وبالتالي ينبغي أن يستخدمها جميع الموظفين، والأطراف الأخرى التي تتعامل مع البيانات التي تحتفظ بها "جهة العمل" أو تخصها.

السياسة

يجب وضع جميع البيانات في "جهة العمل" في أحد التصنيفات التالية:

- ✓ **المستوى الأول: سرية (مقيدة)** تعرف البيانات السرية على أنها عالية الحساسية، ويسبب الكشف عنها أو فقدانها أو تدميرها أضرار كبيرة لشخص أو أكثر أو جهة العمل .ويمكن أن تشمل ما يلي:
  - البيانات الشخصية للموظفين أو العملاء في جهة العمل، مثل هوية المستخدم (User ID) والضمان الاجتماعي أو أرقام الهوية الوطنية وأرقام جواز السفر وأرقام بطاقات الائتمان وأرقام رخصة القيادة، والسجلات الطبية.
  - بيانات المصادقة: مثل مفاتيح التشفير الخاصة، واسم المستخدم وكلمة المرور.
  - لسجلات المالية: مثل أرقام الحسابات المالية.
  - المواد التجارية: مثل الوثائق أو البيانات التي تكون ملكية فكرية فريدة أو محددة.

- البيانات القانونية: بما في ذلك البيانات المصرح بها للجهات القانونية فقط.

✓ **المستوى الثاني: حساسة (داخلية)** وهي البيانات ذات المخاطر المنخفضة ونشرها أو فقدها أو تدميرها لن يكون له تأثير كبير على الأشخاص أو جهة العمل، ولكن لا يجوز نشرها خارج جهة العمل، وغالباً تشتمل على ما يلي:

- البريد الإلكتروني، معظم الرسائل يمكن حذفها أو نشرها دون أن تتسبب في أضرار (باستثناء البريد الإلكتروني من الأشخاص الذين يتم تحديدهم في التصنيف السري.(
- الوثائق والملفات التي لا تتضمن بيانات سرية.
- أي بيانات مصنفة على أنها غير سرية. ويمكن أن تشمل معظم بيانات الأعمال، حيث أن معظم الملفات التي يتم إدارتها أو استخدامها يومياً يمكن تصنيفها على أنها حساسة. ومن أمثلة هذه البيانات محاضر الاجتماعات وخطط العمل والتقارير الداخلية للمشاريع.

✓ **المستوى الثالث: عامة (غير مقيدة):** وهي البيانات التي يمكن الكشف عنها للعامة وتشمل البيانات والملفات التي لا تعتبر حرجة بالنسبة لاحتياجات وعمليات العمل، والتي يتم نشرها عمداً لاستخدامها حيث يكون تأثيرها محايداً أو إيجابياً على "جهة العمل"، مثل المواد التسويقية أو الإعلانات.

✓ **الالتزام:** يجب أن يلتزم الشركاء أو من يعمل مع "جهة العمل" من جهات خارجية بهذا التصنيف الأمني للبيانات.

ثانياً: سياسة حماية البيانات

مقدمة:

البيانات هي أحد الأصول الرئيسية لدى "جهة العمل" التي تتطلب إجراءات ومسؤوليات لحمايتها. وينبغي حماية البيانات المصنفة بشكل مختلف في التخزين والنقل والوصول وغير ذلك لضمان عدم كشفها أو نشرها أو تعديلها.

الغرض

تتناول سياسة حماية البيانات، البيانات المخزنة (الإلكترونية أو السجلات الورقية) التي تحتفظ بها "جهة العمل"، وكذلك الأشخاص الذين يستخدمونها والطرق التي يتبعونها في التعامل بها والأجهزة المستخدمة للوصول إليها، لضمان سرية البيانات، والحفاظ على معايير الجودة في حماية البيانات .

كما تقوم هذه السياسة بتحديد المتطلبات والمسؤوليات الأساسية للإدارة السليمة لأصول البيانات في "جهة العمل"، وتحدد وسائل التعامل مع البيانات ونقلها داخل "جهة العمل."

النطاق

تسري هذه السياسة على جميع من يقوم بالأعمال من النظم والأشخاص وطرق العمل، ويشمل ذلك جميع المدراء التنفيذيين واللجان والإدارات والشركاء والموظفين والأطراف الأخرى الذين لديهم إمكانية الوصول إلى نظم البيانات أو البيانات المستخدمة لأغراض "جهة العمل."

السياسة:

المسؤول عن البيانات

1. يجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته مع قيمة الأصول التي سيتولى إدارتها وحمايتها.
2. يجب عدم تكليف موظف مسؤول رسمي للبيانات التي ليس لها تصنيف أمني وتكون ذات قيمة عملية محدودة، كما يجب التخلص من البيانات إذا لم يكن هناك حاجة قانونية أو تشغيلية لإبقائها، وينبغي تعيين المسؤولين المؤقتين لهذه البيانات داخل كل إدارة لضمان إتمام عملية التخلص منها.
3. يكون منشئ المستندات الجديدة التي لها استخدام داخلي محدد على المدى القصير هو المسؤول عنها، وهذا يشمل الرسائل والخطط والجداول والتقارير، كما يجب إبلاغ جميع الموظفين بمسؤوليتهم عن الوثائق التي ينشئونها.
4. يجب تعيين مسؤول موثوق وتحديد مسؤولياته بشكل واضح اتجاه أصول البيانات التي يتم استخدامها في "جهة العمل" على نطاق واسع. وينبغي أن يملك هذا الشخص القدرة على التحكم في هذه البيانات.

تخزين البيانات

1. يتم تخزين جميع البيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتياطية منتظمة.
2. يجب عدم السماح للموظفين للوصول إلى البيانات إلا بعد أعلامهم وموافقتهم على شروط الاطلاع على البيانات التي سيتعاملون معها.
3. قواعد البيانات التي تحتوي على بيانات شخصية يكون لها إجراءات محددة لإدارتها وتأمين السجلات والوثائق .

الكشف عن البيانات

1. في حالة مشاركة البيانات المقيدة مع "جهة عمل" أخرى، يجب الحرص في الكشف عن هذه البيانات وأن يتم بطريقة آمنة.
2. عندما يتم الإفصاح عن البيانات أو مشاركتها، يجب أن يتم ذلك فقط وفقاً لبروتوكول مشاركة البيانات الموثق أو اتفاقية تبادل البيانات.
3. يحظر الإفصاح عن البيانات المقيدة لأي "جهة عمل" خارجية بدون اتفاق مسبق.

ثالثاً: سياسة الاحتفاظ بالسجلات وإتلافها

مقدمة

تشمل السجلات جميع الوثائق والملفات التي ينتجها الموظفون في "جهة العمل"، سواء كانت إلكترونية أو ورقية. وطرق الاحتفاظ بها وأتلافها يعتبر أمراً ثابتاً وهاماً في العديد من القوانين التي يجب على معظم المؤسسات الامتثال لها.

الغرض

الغرض من هذه السياسة هو التأكد من حماية السجلات والوثائق الضرورية لـ "جهة العمل" والحفاظ عليها وضمان التخلص من السجلات التي لم تعد مطلوبة أو التي لا قيمة لها في الوقت المناسب.

النطاق

تسري هذه السياسة على جميع السجلات التي يتم إنشاؤها في سياق عمل "جهة العمل"، بما في ذلك الوثائق الأصلية ونسخها، ويجب أن يمتثل جميع الموظفين لسياسات الاحتفاظ بالسجلات وإتلافها.

السياسة

1. **سجلات المحاسبة والمالية، وتشمل على:**
   - الوثائق المتعلقة بكشوف المرتبات وإجراءات المحاسبة ودفاتر الحسابات الدائنة والجداول الزمنية، ودفاتر الحسابات والفواتير وتقارير نفقات الموظفين. ويجب الاحتفاظ بها خمس سنوات على الأقل.
   - ينبغي الاحتفاظ بصفة دائمة بتقارير المراجعة السنوية والبيانات المالية، والاحتفاظ بالخطط السنوية والميزانيات للمدة اللازمة لتنفيذها والرجوع إليها عند الحاجة.
   - يجب الاحتفاظ بالعقود والمراسلات ذات الصلة بالعقود (بما في ذلك أي تعديلات على بنود العقد وجميع الوثائق الداعمة الأخرى)
   - سجلات "جهة العمل" (محاضر الاجتماعات، التكاليف الموقعة من الإدارة، أختام "جهة العمل"، أحكام التأسيس واللوائح، سجلات المساهمة والتقارير السنوية) والتراخيص والتصاريح ووثائق التأمين يجب أن تحتفظ بشكل دائم.
   - يجوز إتلاف المستندات المعتبرة في حكم المستندات ذات القيمة بعد اتخاذ الإجراءات اللازمة لتسجيل بياناتها أو ملخصها إذا مضى على استعمالها أو على إجراء آخر قيد فيها خمس سنوات إلا إذا كانت هذه المستندات محل فحص أو مراجعة أو كانت مطلوبة في دعوة قائمة أو كانت القوانين واللوائح أو تعليمات وزارة المالية تقرر الاحتفاظ بها لمدة أطول.
2. **الوثائق الإلكترونية:**

- المستندات الإلكترونية: وتشمل مكتبة برامج مايكروسوفت(Microsoft Office Suite) ، ملفات (PDF).والاحتفاظ يعتمد أيضا على موضوع السجلات وتصنيف بياناتها.
- البريد الإلكتروني: يعتمد الاحتفاظ برسائل البريد الإلكتروني على محتواها فلا ينبغي الاحتفاظ بجميعها، والبريد الإلكتروني الذي يتم حفظه يجب أن يكون مطبوعاً في نسخة ورقية وأن يُحتفظ به في الملف المناسب أو يتم تنزيله إلى ملف كمبيوتر ويتم الاحتفاظ به إلكترونيا أو على القرص كملف منفصل.
- ملفات صفحة ويب: في جميع الأجهزة في محيط العمل، يجب أن يتم جدولة متصفحات الإنترنت لحذف ملفات جمع البيانات مرة واحدة في الشهر.

3. **الملفات والمستندات القانونية :**

يتم الاحتفاظ بالأرشيف القانوني الخاص "بجهة العمل" بدون تحديد مدة على النحو التالي :

- ملفات الدعاوي القضائية وما يصدر فيها من أحكام ابتدائية ونهائية، وقرارات وأوامر المحاكم وكافة الملفات ذات الصلة.
- المذكرات والآراء القانونية الصادرة عن المكاتب القانونية .
- ملفات الموظفين وما يتضمنه من مستندات تخص حياتهم والوظيفية تحفظ بشكل دائم حتى بعد إنهاء علاقة الموظف "بجهة العمل"
- سجلات الإدارية الوظيفية (وتشمل سجلات الحضور والانصراف، استمارة الطلبات، سجل تغيرات العمل، أوراق إنهاء الخدمة، نتائج الاختبارات، سجلات التدريب) يتم الاحتفاظ بها وفق الحاجة إليها وللمدة اللازمة وفق تقديرات "جهة العمل"
- سجلات وأوراق امتحانات شغل الوظائف: تحتفظ "جهة العمل" بأوراق إجابة الامتحانات التحريرية والسجلات والقوائم وسائر الوثائق المتعلقة بالامتحانات التي تجريها لمدة سنتين تبدأ من تاريخ اعتماد نتيجة الامتحان.
- سجلات ومستندات تتمتع "جهة العمل" بسلطة تقديرية في تحديد المدة اللازمة للاحتفاظ بها وترتبط السلطة التقديرية باستمرار حاجة "جهة العمل" لها أو استخدامها والرجوع إليها **ومنها:**
  - ✓ التقارير الاستشارية.
  - ✓ دليل السياسات والإجراءات (الأصلي / النسخ)
  - ✓ التقارير السنوية.

4. **إجراءات أتلاف الوثائق:**

- يجب عدم إزالة أو أتلاف السجلات ألا أن كانت مصنفة بذلك أو عند انتهاء مدة الاحتفاظ بها.
- عند الاحتفاظ بالسجلات خلال الفترة المحددة لها في جداول الاحتفاظ، يتم إعدادها للإتلاف.
- الوثائق المالية يتم إتلافها والتخلص منها وفق الإجراءات المحددة بلائحة الميزانية والحسابات والمخازن:

- الوثائق المالية وسجلات المتعلقة بالموظفين يتم أتلافها بوسيلة تضمن إتلاف المستندات إتلافا كلياً
- يتم التخلص من البيانات الإلكترونية المحتفظ بها في الوسائط الأخرى عن طريق الإتلاف المادي لتلك الوسائط.
- يجب أن تتم عملية أتلاف السجلات بشكل آمن وكامل.
- يجب تسجيل عملية الإتلاف في وثيقة رسمية لأتلاف البيانات داخل "جهة العمل."

رابعاً: سياسة نشر البيانات

مقدمة

توضح هذه السياسة البيانات التي يمكن نشرها داخلياً وخارجياً والأساليب التي تنشر بها هذه البيانات، كما توضح النوع المحدد من البيانات التي سيتم الكشف عنها والتي لا يجوز الكشف عنها.

- بيانات لا يمكن الكشف عنها
  - ✓ البيانات الشخصية، وتشمل سجلات الموظفين والبيانات الطبية، وبيانات عن الراتب والمزايا.
  - ✓ البيانات المالية.
  - ✓ المسائل والإجراءات القانونية أو التأديبية أو محاضر التحقيق ويتم إعلان صاحب الشأن بالطرق الرسمية.
  - ✓ جميع البيانات السرية.
- البيانات التي يتعين الكشف عنها فيما يتعلق بارتباط مع جهات عمل الأخرى
  - ✓ ملخصات المشروع الأولية.
  - ✓ البيانات والمعلومات التي ترى "جهة العمل" ضرورة نشرها لاستخدامها أو لأخذ العلم بها.

الغرض

الغرض من هذه السياسة ضمان حماية البيانات الشخصية والبيانات السرية من الاستخدام غير المصرح به أو كشفها، وكذلك لتسهيل تحديد البيانات الجائز نشرها أو الكشف عنها. وقد وضعت هذه السياسة أيضا لحماية الملكية الفكرية لـ "جهة العمل."

النطاق

تسري هذه السياسة على جميع البيانات المنجزة والمتحصل عليها أو التي تم جمعها وتخزينها من قبل "جهة العمل."

السياسة

- البيانات المصنفة على أنها غير مقيدة يمكن أن تكون متاحة للعامة وجميع الموظفين وكذلك الأطراف الأخرى.

- البيانات التي تحتاج إلى الحماية يمكن الوصول إليها عن طريق الوصول المصرح به، مثل الموظفين أو الشركاء وفق مبدأ "الحاجة إلى المعرفة" لأغراض ذات صلة بالأعمال. وينبغي منح هذا التصريح لفترة محددة وتحددها الإدارة الأعلى مستوى.
- تقتصر البيانات السرية على مجموعة من الأشخاص في وظيفة معينة تتطلب طبيعة عملهم ضرورة الوصول إلى البيانات السرية التي تحتفظ بها "جهة العمل".
- البيانات المقيدة يتم الوصول إليها بموجب إجراءات رسمية ولأفراد متخصصين ومحددين على أساس الوظيفة.

خامساً: سياسة الوصول للبيانات

مقدمة

تحدد "جهة العمل" التصنيف الأمني لأصول البيانات ويوضح هذا التصنيف نوع البيانات التي يمكن عرضها أو الوصول إليها من قبل الموظفين أو الأطراف الأخرى. وكل مستوى من هذا التصنيف كالبيانات الحساسة أو البيانات السرية يتطلب تصريح مختلف من الإدارة العليا للوصول إليه.

الغرض

الغرض من هذه السياسة هو الحد من خطر ضياع البيانات أو الكشف عنها بشكل يؤثر على سلامة أو سرية أو وفرة أصول هذه البيانات، وذلك من خلال التحكم في الوصول إليها بتحديد من المصرح له بذلك ومن يستطيع استخدامها.

النطاق

تسري هذه السياسة على جميع البيانات من التقارير والمستندات والوثائق التي تم إصدارها أو جمعها من قبل "جهة العمل."

السياسة

- الأفراد المصرح لهم فقط يمكنهم الوصول إلى البيانات المتوفرة بشكل كامل .
- المستخدمين يُصرَح لهم الوصول للبيانات واستخدامها عند الطلب .
- المصرح لهم فقط من الموظفين أو المجموعات أو المنظمات يمكنهم الوصول للبيانات اللازمة لإجراء العمل فقط، كما أن قيمة الملكية الفكرية محمية عند استخدام هذه البيانات.

سادساً: سياسة الاستخدام المقبول:

مقدمة

الهدف من نشر سياسة الاستخدام المقبول لا يكمن في فرض قيود تتعارض مع ثقافة الانفتاح والثقة والشفافية داخل المؤسسات، وإنما تهدف إلى حماية **(جهة العمل)** وموظفيها وشركائها من حدوث أي أعمال غير قانونية أو ضارة من قبل الآخرين سواء كان ذلك بقصد او بدون قصد.

الأنظمة ذات العلاقة ب (Internet/Intranet/Extranet) بما في ذلك على سبيل المثال لا الحصر أجهزة الكمبيوتر والبرمجيات وأنظمة التشغيل ووسائط التخزين وحسابات الشبكات الموفرة للبريد الالكتروني ومتصفحات شبكة الانترنت وبروتوكول نقل الملفات. كل ما سبق هو ملك للمؤسسة. وهذه الأنظمة يجب أن يتم استخدامها لخدمة أغراض **(جهة العمل)** وفي مجال عملها واهتماماتها، وفي التعامل مع عملاءها وزبائنها في سياق العمليات الاعتيادية. (وفق سياسات الموارد البشرية بالمؤسسة)

نظام أمن وسلامة المعلومات الفعّال هو جهد جماعي يتطلب مشاركة ودعم كل موظفي **(جهة العمل)** كل من يتعامل مع المعلومات والأنظمة المتعلقة بها، وتقع على عاتق كل مستخدم للكمبيوتر مسؤولية معرفة هذه الإرشادات، وإجراء كل أنشطته وفقًا لها.

الغرض من السياسة

الغرض من وضع هذه السياسة هو تحديد ماهية الاستخدام المقبول لكل ما يتعلق بمعدات وأجهزة الكمبيوتر في **(جهة العمل).** وقد وُضعت هذه القواعد لحماية الموظف و(جهة العمل) على حد سواء، حيث أن الاستخدام غير المناسب لتلك المعدات والأجهزة قد يعرضهما لمخاطر كثيرة بما في ذلك هجمات البرمجيات الخبيثة وغيرها من التهديدات المحتملة المتعلقة بأنظمة وخدمات الشبكات وما يترتب عليها من أثار قانونية.

النطاق

تنطبق هذه السياسة على استخدام المعلومات والأجهزة الإلكترونية وأجهزة الكمبيوتر وموارد الشبكة اللازمة لإجراء أعمال **(جهة العمل)** أو ما يتعلق بالتعامل مع الشبكات الداخلية وأنظمة الأعمال، سواء كانت مملوكة أو مستأجرة من قبل **(جهة العمل)** أو الموظف أو طرف ثالث، ويتحمل الجميع مسؤولية تطبيق الممارسات الصحيحة فيما يتعلق بالاستخدام المناسب للمعلومات والأجهزة الإلكترونية وموارد الشبكة وفقًا لسياسات ومعايير) **(جهة العمل)**

السياسة

1. **الاستخدام العام والملكية**

- ✓ تمتلك **(جهة العمل)** البيانات المحفوظة على أجهزة الكمبيوتر والأجهزة الالكترونية الأخر ى، المملوكة أو المستأجرة من قبل المؤسسة، أو من طرف ثالث، ويجب التأكد من خلال الوسائل القانونية أو التقنية أن معلومات الملكية محمية وفقًا لمعيار حماية البيانات.
- ✓ تقع على عاتقك مسؤولية الإبلاغ عن سرقة أو فقدان أو كشف غير مصرح به عن معلومات الملكية المتعلقة بالمؤسسة.
- ✓ يسمح بالوصول ل إلى أو استخدام أو مشاركة معلومات الملكية فقط في حدود ما هو مصرح به وضروري للإيفاء بمتطلبات الوظيفة التي يتم التكليف بها.
- ✓ كل موظف مسؤول عن تطبيق معايير الاستخدام الأمن للأجهزة الإلكترونية في إطار الوظيفة، كل إدارة مسؤولة عن وضع مبادئ توجيهية بشأن الاستخدام الشخص ي الأمثل ل لأنظمة داخل المؤسسة، ويجب أن يسترشد الموظفون بسياسات الإدارة بشأن الاستخدام الشخص ي، واستشارة مشرفيهم أو مدراءهم.
- ✓ يجو ز للأفراد المصرح لهم مراقبة المعدات والنظم وحركة الشبكة في أي وقت لأغراض الأمان وصيانة الشبكة وذلك وفقًا **لسياسة المر قبة وسياسة التدقيق.**
- ✓ تحتفظ **(جهة العمل)** بحقها في التدقيق على الشبكات والأنظمة دوريًا لضمان الالتزام بهذه السياسة.

2. **معلومات الملكية**

- ✓ كل الأجهزة المحمولة وأجهزة الكمبيوتر المملوكة للمؤسسة والتي تتصل بشبكة الانترنت يجب أن تلتزم بسياسة **التحكم في الوصول.**
- ✓ يجب أن تتوافق كلمات المرور للأنظمة والمستخدم مع سياسة كلمة المرور، ويحظر منح إمكانية الوصول إلى شخص آخر عمداً أو عن طريق عدم تأمين الوصول.
- ✓ يجب تأمين جميع أجهزة الكمبيوتر باستخدام شاشة توقف محمية بكلمة مرور مع تعيين ميزة التنشيط التلقائي إلى 10 دقائق أو أقل، يجب عليك قفل الشاشة أو تسجيل الخروج عندما يكو ن الجهاز غير مراقب / غير مستخدم.
- ✓ النشر عن طريق الموظفين باستخدام البريد الالكتروني للمؤسسة يجب أن يتضمن إخلاء للمسؤولية بأن رأيهم لا يمثل رأي (جهة العمل) وإنما يعبر عن وجهة نظرهم الشخصية إلا فيما يتعلق بمهام العمل.

3. **الاستخدام غير المقبول**

بشكل عام يحظر ممارسة الأنشطة تالية الذكر، وقد يتم إعفاء الموظفين من هذه القيود أثناء القيام بمسؤولياتهم الوظيفية المصرح لهم بها (على سبيل المثال، قد يحتاج موظفو إدارة الأنظمة إلى تعطيل وصول الشبكة إلى المضيف، إذا كان ذلك المضيف يعرقل خدمات تؤثر على الإنتاج)

كما لا يسمح تحت أي ظرف من الظروف لأي موظف في (جهة العمل) بالتعاطي مع أي نشاط غير قانوني بموجب القانون المحلي أو الدولي أثناء استخدام موارد, (جهة العمل) والقوائم أدناه لم توضع بشكل موسع بأي حال من الأحوال، ولكنها محاولة لوضع إطار عام للأنشطة التي تندرج تحت فئة الاستخدامات الغير مقبولة.

4. أنشطة النظام والشبكة

الأنشطة التالية محظورة تمام اً، وبدون استثناءات:

- ✓ انتهاكات حقوق أي شخص أو شركة محمية بحقوق النشر أو السر التجاري أو براءة الاختراع أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة، بما في ذلك على سبيل المثال لا الحصر، تركيب أو توزيع " برامج ليست مرخصة بشكل مناسب للاستخدام من قبل (جهة العمل)
- ✓ النسخ غير المصرح به للمواد المحمية بموجب حقو ق الطبع والنشر، بما في ذلك على سبيل المثال لا الحصر، تحويل الصور الفوتوغرافية من المجلات أو الكتب أو غيرها من المصادر المحمية بحقو ق النشر إلى صور رقمية وتوزيعها، وأيضاً مواد الوسائط المتعددة المحمية بحقو ق النشر.. إلخ، وتثبيت أي برنامج محمي بموجب حقو ق النشر والتي لا تمتلك (جهة العمل) أو المستخدم له ترخيص بذلك.
- ✓ الموظفون المصرح لهم بالوصول إلى شبكة الانترنت يجب عليهم عدم استخدامها لتحميل برمجيات وألعاب، كما ينبغي عليهم عدم استغلالها في اللعب ضد خصوم على شبكة الانترنت.
- ✓ الوصول إلى البيانات أو الخادم أو الحساب (لأي غرض آخر غير القيام بأعمال تخص جهة العمل، حتى مع وجود تصريح بالدخول.
- ✓ انتهاك لقوانين مراقبة التصدير المحلية والدولية عند القيام بتصدير البرمجيات أو المعلومات التقنية أو برامج أو تقنيات التشفير، ويستوجب استشارة الإدارة المناسبة قبل تصدير أي مادة محل شك.
- ✓ استخدام أجهزة الكمبيوتر المملوكة للمؤسسة للانخراط بفاعلية في شراء أو نقل مواد تنتهك القانون.
- ✓ تقديم عروض احتيالية من المنتجات أو العناصر أو الخدمات موجهة من حساب) جهة العمل.
- ✓ التأثير على الخروقات الأمنية أو تعطيل اتصالات الشبكة، وتشمل الخروقات الأمنية، على سبيل المثال لا الحصر.

الوصول غير المصرح للبيانات أو الولوج إلى الخادم أو الحساب بدون تصريح رسمي إذا لم يكن ذلك من واجبات الوظيفة، أما تعطيل اتصالات الشبكة فيتضمن مثلاً، عملية مراقبه تدفق البيانات داخل الشبكة Network Sniffing، وعمليات حجب "الحرمان" من الخدمة)" Distributed Denial of Service "DDOS (، والتلاعب في الحزمة البيانات) Packet spoofing (ومعلومات التوجيه المزورة لأغراض خبيثة.

- ✓ عدم إجراء عملية فحص أمني للمنافذ ports إلا بعد إبلاغ مسبق للمسؤول ب (جهة العمل.)

- ✓ القيام بتنفيذ أي شكل من أشكال مراقبة الشبكة التي من شأنها اعتراض البيانات غير المخصصة لمضيف Host المستخدم، ما لم يكن هذا النشاط جزءًا من المهام أو الأعمال الروتينية للموظف.
- ✓ اجتياز عملية مصادقة المستخدم أو أمان أي مضيف أو شبكة أو حساب.
- ✓ استخدام تقنيات مصائد مخترقي الشبكات honeypots أو أي تقنيات مشابهة في شبكة (جهة العمل) دون إذن.
- ✓ التدخل في / أو رفض الخدمة لأي مستخدم غير مضيف Host الموظف) على سبيل المثال، هجمة رفض الخدمة denial of service attack
- ✓ استخدام أي برنامج/ نص / أمر، أو إرسال رسالة من أي نوع، بنية التدخل في / تعطيل جلسة عمل مستخدم ما بأي وسيلة، في الشبكة المحلية محلياً أو عبر (Internet/Intranet/Extranet)
- ✓ إفشاء معلومات عن/ قائمة بأسماء الموظفين إلى أي أطراف خارج (جهة العمل.)
- ✓ يجب تشفير الملفات التي تحتو ي على بيانات حساسة خاصة ب) جهة العمل (والتي يتم نقلها بأي شكل عبر الإنترنت، كما هو محدد في سياسة أمن البيانات الموجودة.

5. أنشطة البريد الإلكتروني والاتصالات

استخدام البريد الإلكتروني من أساسيات الوظائف اليومية، وعلى) جهة العمل) التأكد من أن الموظفين يفهمون حدود استخدام حسابات البريد الإلكتروني الخاصة بها، حيث يساعد الاستخدام المقبول للبريد الإلكتروني الموظفين على استخدام عناوين البريد الإلكتروني لـ(جهة العمل) بشكل صحيح كما هو محدد في سياسة استخدام البريد الالكتروني.

التواصل الاجتماعي والتدوين / النشر الالكتروني

- ✓ التدوين أو النشر الالكتروني من قبل الموظفين سواء كان ذلك باستخدام ممتلكات وأنظمة **(جهة العمل)** أو عبر أنظمة كمبيوتر خاصة يندرج أيضاً ضمن القيود المتعلقة بهذه السياسة، والاستخدام المحدود في مناسبات معينة لأنظمة **(جهة العمل)** للانخراط في التدوين مقبول، بشرط أن يكون بشكل محترف وأخلاقي ولا ينتهك سياسات (جهة **العمل)**، ولا يضر بمصالحها ولا يتداخل مع واجبات الوظيفة، والتدوين باستخدام أنظمة **(جهة العمل)** معرض للمراقبة.
- ✓ سياسة سرية المعلومات ب) جهة العمل (تنطبق أيضاً على التدوين، حيث يُحظر على الموظفين الكشف عن أي معلومات حساسة خاصة ب **(جهة العمل)**، وكذا الأسرار التجارية والمهنية أو أي مواد تحت مظلة سياسة سرية المعلومات عن الانخراط في عمليات التدوين أو النشر الالكتروني.

- ✓ يجب ألا ينخرط الموظفون في أي عملية تدوين أو نشر الكتروني يمكن أن تضر أو تشوه صورة وسمعة أو يمس كل ما يتعلق بالرضا عن مؤسسة ما، كما يُحظر على الموظفين نشر تعليقات تدل على تمييز، وإحراج، وإهانة، ومضايقة أو تبنى أي سلوك الكتروني من السلوكيات المحظورة.
- ✓ على الموظفين عدم نسب تصريحات شخصية أو آراء أو معتقدات لـ**(جهة العمل)** عند الانخراط في عمليات تدوين أو نشر الكتروني، وإذا قام موظف ما بالتعبير عن رأي ما أو معتقد خاص به فلا يمكنه بأي حال من الأحوال أن يتحدث بصفة موظف في) جهة العمل (أو ممثلاً لها صراحةً أو ضمنياً، كما يجب على الموظف أن يضع في الاعتبار المخاطرة التي تتضمنها عملية التدوين /النشر الالكتروني.
- ✓ وبغض النظر عن أهمية اتباع جميع القوانين المتعلقة بمناولة المواد الخاضعة لحقو ق النشر الخاضعة للرقابة والكشف عنها، كما لا يجو ز أيضًا استخدام العلامات التجارية والشعارات وأية ملكية فكرية أخر ى خاصة ب **(جهة العمل)** فيما يتعلق بأي نشاط تدوين أو نشر الكتروني.

سابعاً: سياسة كلمة السر/المرور

مقدمة

تعتبر كلمة المرور أو كلمة السر عنصرا مهم في مجال أمن المعلومات. فهي تستخدم كإثبات للهوية للموافقة على الوصول وذلك لحماية المستخدمين وحفظ خصوصيتهم، ولحماية البيانات والأنظمة والشبكات. على سبيل المثال يتم استخدامها لمصادقة مستخدمي أنظمة التشغيل والتطبيقات مثل البريد الإلكتروني والوصول عن بعد، كما تستخدم أيضا لحماية الملفات والمعلومات المخزنة الأخر ى. وفي ظل هذه الحاجة إلى كلمات المرور لأمو ر ذات أهمية عالية اقتض ى ذلك تركيب كلمات سر قوية ذات تشفير عالي، بحيث لا يمكن لأحد توقعها أو استنتاجها.

الغرض من السياسة

الغرض من هذه السياسة هو تحديد سياسات وإجراءات كلمة السر/المرور لتقديم أفضل مستو ى للخدمة مع أعلى درجات الحماية والخصوصية للمستخدمين.

النطاق

تسر ي هذه السياسة على جميع الموظفين في (جهة العمل) وتطبق على جميع كلمات المرور المستخدمة على كافة الأجهزة وملحقاتها والخدمات المرتبطة بها والأنظمة وفي جميع التطبيقات التي تعد جزءا من شبكة (جهة العمل) التي توفر الوصول إلى بيانات (جهة العمل) المملوكة.

السياسة

- ✓ فرض كلمة مرور قوية: يجب ان تكون كلمة المرور قوية ولا تتضمن في تركيبها الكلمات التي يسهل على الاخرين إيجادها.
  - يجب استخدام توليفة من الأحرف الكبيرة والصغيرة، مع أرقام، ورموز أو علامات الترقيم قدر الامكان عند اختيارك لكلمة السر/المرور.
  - لا يجب استخدام كلمات سر رائجة والتي يمكن التكهن بها بسهولة، كالأسماء وتاريخ الميلاد أو أرقام الهواتف.
  - يجب ان لا يقل عدد رموز كلمة السر/المرور عن 14 رمزا
  - لا يجب استعمال اسم المستخدم في كلمة السر.
  - لا يجب استخدام أرقام ا أو حروف متكررة مثل (3333 او AAAA)
  - في حالة اختيار كلمة تقليدية يفضل خلط حروفها بحيث لا تعطي معني متعارف عليه.
  - يفضل ان تكو ن كلمة المرور "جملة مرور" لا يفهمها الا المستخدم، مُكونة من تركيبة الاحرف والأرقام والرموز.
  - تطبيق ضوابط صارمة على كلمات المرور على مستو ى النظام وكلمة مرور الحسابات المشتركة.
- ✓ يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها.
  - يجب التعامل مع جميع كلمات المرور في (جهة العمل) على أنها بيانات سرية.
  - لا يحتفظ بكلمات المرور كنص عادي يمكن قراءته، وإنما يتم حفظ كلمات السر على شكل نص مشفر لا يمكن فكه او استخدامه من الشخص المخول.
  - يجب ألا يتم تخزين كلمات المرور على أنظمة الكمبيوتر في شكل غير محمي.
  - كلمات المرور للأنظمة) جذر النظام/مسؤول النظام Root/Administrator (يجب ان تخز ن باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.
  - يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وادخال البيانات في كل مرة من جديد.
- ✓ الحفاظ على سرية كلمات المرور: يجب عدم مشاركة أو كشف كلمة المرور مع أي شخص لأي سبب من الأسباب.

- يجب عدم أفشاء كلمة المرور وعدم كتابتها بطريقة صريحة مما يجعلها عرضة للاطلاع أو حتى التلميح عن تركيبتها، إلا في حالة الضرورة القصوى ويجب تغييرها بعد الكشف عنها
- يجب أخذ الحذر من الاشخاص المتطفلين عند طباعة لكلمة السر/المرور أثناء عملية الولوج.
- يمنع إرسال كلمة المرور عبر البريد الالكتروني أو من خلال اي وسيلة عبر الانترنت.
- يجب تغيير كلمات المرور إذا ظهر أي مؤشر على احتمال اختراق للنظام أو لكلمة المرور.
- يجب تغيير كلمات المرور المستخدمة للحسابات المشتركة على الفو ر في حالة اختراقها أو عندما يغادر مالكها (جهة العمل
- لا يجب استخدام نفس كلمة المرور لحسابات المسؤولين المتعددة.
- يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في (جهة العمل)
- يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والاجهزة داخل (جهة العمل) والحسابات والاجهزة الاخر ى خارجها.

✓ كلمات المرور الأولية (المؤقتة): يجب تغيير كلمات المرور الأولية للمستخدمين وفرض مدة انتهاء لصلاحيتها لإجبار المستخدم على تغييرها.

- على المستخدم تغيير كلمة المرور الأولية التي يستلمها من الجهة المختصة في أو ل استخدام له وقبل انتهاء وقت صلاحيتها؛ وذلك لضمان عدم تسريب كلمة السر لمستخدمين آخرين.
- يجب إعطاء كلمات المرور المؤقتة للمستخدمين بطريقة آمنة؛ ينبغي تجنب نقلها على ورقة مكشوفة (نص عادي) او عن طريق أطراف ثالثة أو رسائل البريد الإلكتروني غير المحمية (النص الواضح).
- وضع إجراءات للتحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة أو بديلة أو مؤقتة.
- يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقتة.

✓ يتطلب فحص كلمات المرور الجديدة في قوائم كلمات المرور شائعة الاستخدام أو المخترقة.

✓ يجب منع الولوج للأنظمة الداخلية والخاصة بعد 3 محاولات خاطئة خلال مدة زمنية لا تتجاوز 15 دقيقة. ويستمر المنع لمدة أقلها 30 دقيقة وأكثرها 3ساعات.

✓ يجب على المستخدم في حالة ان يشتبه او يلاحظ وجود مشكلة أمنية أو أن كلمة المرور الخاصة به قد تعرضت للاختراق الإبلاغ عن الحادث وتغيير جميع كلمات المرور.

✓ يجب أن يطلب من المستخدمين التوقيع على بيان للحفاظ على سرية كلمات المرور الشخصية؛ يمكن تضمين هذا البيان في شروط التوظيف.

✓ يجب ان يكون المستخدم على علم ودراية أنه المسؤول الوحيد عن حماية كلمة السر/المرور الخاصة به.

ثامناً: سياسة استعمال البريد الإلكتروني

مقدمة

يعتبر البريد الإلكتروني أداة اتصال أساسية في معظم مجالات الأعمال لسرعته وفعاليته العالية، ولأنه أصبح وسيلة معتمدة وتعبر عن الجهة المرسلة، أصبح من الضروري وضع سياسة استخدامه تفادياً للمشاكل التي قد تحدث بسبب سوء الاستخدام.

الغرض من السياسة

تحديد سياسات وإجراءات التعامل بالبريد الالكتروني من خلال البنية الأساسية لشبكة (جهة العمل) والتي يستهدف من خلالها حصول المستخدمين على أعلى درجات الحماية والتقليل من أضرار الاختراق وضمان استخدام مهني.

لنطاق

تسري هذه السياسة على جميع الموظفين الذين يمكنهم استخدام البريد الالكتروني في (جهة العمل) وجميع المصنعين والعملاء الذين يعملون باسم (جهة العمل)، وعلى نظام البريد الإلكتروني المستخدم داخل (جهة العمل).

السياسة

✓ حساب البريد الالكتروني

- يمنح كل موظف حساب بريد إلكتروني، ويجب أن يكو ن محدد بشكل فريد لكل مستخدم.
- عند إنشاء بريد إلكتروني جديد للمستخدم، يجب على المستخدم تغيير كلمة المرور ا لأولية الخاصة به في تسجيل الدخول التالي، حيث يجب تكوين النظام يفرض على المستخدمين تغيير كلمات المرور الأولية الخاصة بهم.
- يجب أن تكو ن كلمة مرور البريد الإلكتروني الخاصة بالمستخدم تتوافق مع سياسة كلمة المرور الصادرة عن (جهة العمل)
- يجب التحكم في حجم صندوق البريد من خلال تحديد سعة الحصة المخصصة، وكل مستخدم مسؤول إذا تجاوز السعة المحدودة، لذا يجب على المستخدم أرشفة الرسائل المهمة بشكل دوري وحذفها من البريد الوارد.

✓ استخدام البريد الالكتروني

يجب على جميع المستخدمين التقيد بما يلي عند استخدام البريد الإلكتروني الخاص بـ (جهة العمل)

- يجب أن يكو ن استخدام البريد الإلكتروني متوافقاً مع سياسات (جهة العمل) وإجراءاتها ومع القوانين المعمول بها والممارسات السليمة والامتثال للقوانين المعمول بها.
- يجب استخدام حسابات البريد الإلكتروني لـ (جهة العمل) لأعمال تتعلق بـ(جهة العمل)، حيث يستخدم لمساعدة الموظفين في تأدية وظائفهم.
- لا ينبغي استخدام البريد الإلكتروني المخصص للموظف لأغراض شخصية.
- يجب تأمين جميع بيانات (جهة العمل) الواردة في رسالة بريد إلكتروني أو مرفق طب قا لسياسة حماية البيانات.
- يجب توخي الحذر عند إرفاق المستندات أو الملفات بالبريد الإلكتروني، فقد تكو ن هذه المرفقات تابعة للآخرين، وإعادة توجيه هذه البيانات إلى مستلم آخر دو ن الحصو ل على إذن من المرسل قد يعتبر انتهاكاً لحقوق الطبع والنشر.
- يجب على جميع المستخدمين توخي الحذر عند فتح رسائل البريد الإلكتروني والمرفقات من مصادر غير معروفة.
- يجب على جميع المستخدمين ضمان أن يكو ن محتو ى البريد الإلكتروني دقيقا وواقعيا وموضوعيا، حيث يجب تجنب الآراء الشخصية حو ل الأفراد أو المؤسسات الأخرى.
- يجب أن يدرك المستخدمون أن رسائل البريد الإلكتروني قد تخضع للتدقيق للتأكد من أنها تلبي متطلبات هذه السياسة. ينطبق هذا على محتو ى الرسائل والمرفقات والعناوين ورسائل البريد الإلكتروني الشخصية.
- تعتبر جميع الرسائل المرسلة عبر نظام البريد الإلكتروني الخاص لـ(جهة العمل) ملكية خاصة بـ (جهة العمل) وتشمل رسائل البريد الإلكتروني الشخصية أيضا. يجب ألا يكو ن لدى المستخدم أي توقع للخصوصية في أي شيء يقوم بإنشائه أو تخزينه أو إرساله أو استلامه على نظام البريد الإلكتروني الخاص ب (جهة العمل).
- يمكن مراقبة الرسائل الإلكترونية دو ن إخطار مسبق إذا رأت (جهة العمل) ذلك ضروريا. إذا وجد دليل على أن الموظف لا يلتزم بالتوجيهات المنصوص عليها في هذه السياسة، تحتفظ (جهة العمل) بالحق في اتخاذ إجراءات تأديبييه وفق اللوائح المعمول بها.
- يجب انتقاء الألفاظ اللائقة وعدم كتابة أي لفظ مسيء او مهين للآخر.
- يجب على المستخدمين عدم الإفصاح عن كلمات المرور الخاصة بحساباتهم أو السماح لأي شخص آخر باستخدام حساباتهم، كما يجب عدم استخدام حساب مستخدم آخر.
- في الحالات التالية (الاستقالة، الفصل/الطرد، الإيقاف) سوف يتم أعلام الموظف بأنه سيتم قفل حساب بريده الالكتروني ومنحه فرصة محددة لنسخ وأرشفة محتويات بريده.

- يجب على من يتعرف على أو يلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفو ر بقسم أمن المعلومات في (جهة العمل) والابلاغ بشكل فوري.
- إرفاق كل رسالة بتوقيع نص ي في النهاية يحمل الاسم والوظيفة ورقم الهاتف والقسم التابع له واسم (جهة العمل)
- على المستخدم أخذ العلم والدراية أنه المسؤول الوحيد عما تحتويه الرسائل المرسلة من خلال حساب بريده الإلكتروني.
- يجب على المستخدمين ضمان إرسال رسائل البريد الإلكتروني إلى المستخدمين الذين يحتاجون إلى معرفة الأمر فقط.

✓ **الاستخدام الغير مقبول للبريد الالكتروني**

تعد الممارسات التالية غير مقبولة عند استخدام البريد الالكتروني الخاص ب (جهة العمل)

- استخدام نظام البريد الإلكتروني لـ(جهة العمل) لإنشاء أو توزيع أي رسائل مدمرة أو هجومية. يجب على الموظفين الذين يتلقون أي رسائل بريد إلكتروني بهذا المحتو ى من أي موظف ب (جهة العمل) إبلاغ الأمر إلى المسؤول على الفور.
- استخدام حساب البريد الإلكتروني لـ(جهة العمل) لتسجيل الدخول في أي من مواقع الشبكات الاجتماعية ما لم يكن ذلك لأغراض العمل، كما يجب الحصول على موافقة من الإدارة العليا لذلك.
- استخدام هوية مزيفة في رسائل البريد الإلكتروني الخاصة ب (جهة العمل).
- العبث بمحتو ي وعناوين الرسائل المعاد توجيهها أو مرفقاتها بدو ن توضيح ذلك بشكل صريح.
- إرسال رسائل بريد الكتروني غير مرغوب فيها بما في ذلك إرسال "بريد غير هام" JUKE MAIL، أو مواد إعلانية إلى أفراد لم يطلبوها تحديداً ك (رسائل البريد الالكتروني المزعج SPAM)
- استخدام غير مصرح به لمعلومات البريد الالكتروني أو تزويرها.
- إنشاء أو إجراء تحويل ل "سلسلة رسائل chain letters "، "بونز ي Ponzi " ، أو أي أشكال هرمية من أي نوع .
- استخدام رسائل بريد غير مرغوب بها داخل شبكات (جهة العمل) لمزودي خدمات آخرين نيابة عن أو للدعاية لأي خدمة مستخدمة من قبل (جهة العمل) أو متصلة عبر شبكتها.
- نشر الرسائل غير ذات العلاقة بالعمل أو ما شابه ذلك لعدد كبير من مجموعات الأخبار newsgroups أو ما يسمى ب (newsgroup spam)
- تغيير محتو ى و/أو عناوين البريد الإلكتروني للرسائل المعاد توجيهها أو مرفقاتها دو ن الحصو ل على موافقة.

تاسعاً: سياسة استخدام الانترنت

مقدمة

تعتبر الإنترنت أحد أكثر مصادر المعلومات استخداما، فهو يوفر موارد متعددة من البيانات والأفكار والأبحاث والأخبار، ويسهّل على المستخدمين الحصول على المعلومات والبيانات لتشجيعهم على إجراء الأبحاث وتبادل المنافع.

الوصول إلى الإنترنت من قبل الموظفين بشكل يتعارض مع احتياجات العمل قد يؤدي إلى إساءة استخدام الموارد، وهذا قد يعرض (جهة العمل) لمخاطر يجب معالجتها لحماية أصول المعلومات الخاصة ب (جهة العمل). بالإضافة إلى ذلك قد تواجه (جهة العمل) خطر تشويه السمعة و/او التعرض لمشاكل قانونية من خلال أنواع أخرى من سوء الاستخدام. يساعد اتباع سياسة استخدام الإنترنت في حماية كلاً من الموظف والمؤسسة من تبعات سوء استخدام الإنترنت.

الغرض

تهدف هذه السياسة الى تحقيق الاستخدام الآمن للإنترنت وذلك بتزويد الموظفين بالقواعد والمبادئ التوجيهية حول الاستخدام الملائم لمعدات وشبكة (جهة العمل) والاتصال بالإنترنت لضمان استخدام الموظفين للإنترنت بطريقة آمنة وأكثر فاعلية.

النطاق

تنطبق هذه السياسة على جميع مستخدمي الإنترنت) الموظفين وجميع الأطراف الثالثة (الذين يتصلون بالأنترنت من خلال أجهزة الكمبيوتر أو الشبكات الخاصة بـ(جهة العمل) والخدمات المرتبطة بها.

السياسة

✓ **استخدام الموارد**

- يتم الموافقة على الوصول إلى الإنترنت فقط إذا تم تحديده ضمن احتياجات العمل. يتم منح خدمات الإنترنت على أساس مسؤوليات الوظيفة الحالية للموظف.
- ستقوم إدارات (جهة العمل) بمراجعة متطلبات وصول المستخدمين إلى الإنترنت بشكل دوري لضمان استمرار احتياجهم للإنترنت.
- يصرح لمستخدمي الانترنت في (جهة العمل) باستخدامها لأغراض تخص العمل وبطريقة لا تخالف الأنظمة واللوائح المعمول بها في (جهة العمل)، أو بما يؤدي إلى الإضرار بها او بسمعتها.
- لا تكفل (جهة العمل) دقة المعلومات التي يتم الحصو ل عليها عن طريق الإنترنت، ذلك يقع على عاتق مصدر ومنتج هذه المعلومات.

- تحتفظ (جهة العمل) بحق فرض السعة المسموح بها لاستعمال الاتصال بالإنترنت حسب ما تراه الجهة الفنية المختصة وبما يتناسب مع متطلبات كل إدارة.

✓ **الاستخدام المسموح**

- التواصل بين الموظفين وغير الموظفين لأغراض العمل.
- ما يقوم به فنيي دعم تكنولوجيا المعلومات من تنزيل لتحديثات البرامج والتصحيحات.
- استعراض مواقع الويب للبائعين المحتملين للحصو ل على معلومات عن المنتجات.
- مراجعة المعلومات التنظيمية أو البيانات الفنية.
- إجراء الابحاث

✓ **الاستخدام الشخصي**

- قد يُعد استخدام اجهزة كمبيوتر (جهة العمل) للوصول إلى الإنترنت لأغراض شخصية، دو ن موافقة مدير المستخدم وقسم تكنولوجيا المعلومات، سببا لاتخاذ إجراءات تأديبييه حسب اللوائح المعمول بها.
- يجب أن يكو ن جميع مستخدمي الإنترنت مدركين أن شبكة (جهة العمل) تقوم بإنشاء سجل تدقيق يبين طلب الخدمة، سواء في العناوين الداخلية أو الخارجة، حيث يتم مراجعتها هذه السجلات بشكل دوري.
- المستخدمون الذين يختارون تخزين أو نقل المعلومات الشخصية مثل المفاتيح الخاصة أو أرقام بطاقات الائتمان أو الشهادات أو الاستفادة من "محافظ" الإنترنت يقومون بذلك على مسؤوليتهم الخاصة. (جهة العمل) ليست مسؤولة عن أي فقدان للمعلومات، مثل المعلومات المخزنة في المحفظة، أو أي ما قد ينتج من خسائر لاحقة للممتلكات الشخصية.
- المستخدم مسؤول مسؤولية كاملة عن أجهزة الكمبيوتر الخاصة به واستخدامها، وعليه أن يكو ن على دراية بأمن وحفظ موارد تكنولوجيا المعلومات.
- يجب على المستخدمين الذين يتعرفون على أو يلاحظون وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفو ر بالقسم المختص في(جهة العمل) والابلاغ بشكل فوري.

✓ **الاستخدام المحظور**

- يمنع منعا باتا استخدام الانترنت أو استغلالها بطريقة تعرض شبكة (جهة العمل) للخطر، أو فتح ثغرات أمنية في الشبكة أو نشر برمجيات ضارة أو غير مشروعة.

- لا يجو ز انتحال شخصية الاخرين أو جهاز آخر.
- يمنع استخدام اسم (جهة العمل) أو أي من أقسامها أو أي من موظفيها دو ن إذن كتابي رسمي.
- يمنع العبث بالمعلومات الخاصة بموظفين آخرين أو بجهات أخر ى أو الاطلاع عليها بشكل غير قانوني.
- يمنع نشر المعلومات الخاصة بـ (جهة العمل) أو الخاصة بالآخرين دو ن إذن صريح بذلك.
- يمنع محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية بدو ن تصريح رسمي من الجهة المعنية.
- لا يجو ز الإخلال بأي من حقو ق النشر أو التأليف، أو حقو ق الملكية الفكرية لأي بيانات، تطبيقات، برامج أو معلومات.
- يمنع مراقبة الاتصالات الإلكترونية للمستخدمين الآخرين لغرض التجسس وانتهاك الخصوصية.
- لا يجو ز استخدام الانترنت بشكل يؤثر سلبا على المستخدمين الآخرين، أو على أداء الأجهزة والشبكات.
- يمنع استخدام الانترنت لأي أغراض غير قانونية أو غير شرعية. ومن الأمثلة على ذلك إرسال مواد عنيفة أو تهديدية أو خداعية أو إباحية أو فاحشة أو غير قانونية أو غير شرعية والذي يمكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج، أو مضايقة لأي شخص أو جهة أو أمنها السيبرانية.
- يمنع إهدار الموارد المعلوماتية، أو إحداث أي تغيير في الموارد المعلوماتية دو ن امتلاك صلاحية تخو ل ذلك.
- يمنع إنشاء موقع الكتروني أو حساب على مواقع التواصل الاجتماعي يمثل (جهة العمل) ، أو إدارتها أو أي جزء منها دو ن إذن كتابي رسمي من صاحب الصلاحية.
- عدم استخدام قنوات اتصال بالموارد المعلوماتية الأخر ى أو الارتباط بها إلا من خلال القنوات المتاحة والمصرح بها رسميا من (جهة العمل)
- يمنع استخدام الموارد المعلوماتية بشكل يؤدي إلى إهدار وقت الموظف.
- يجب عدم استخدام الاتصال بالإنترنت الخاص بـ (جهة العمل) لأغراض تجارية أو سياسية، أو بهدف تحقيق ربح شخص ي أو تجار ي أو تسويقي.
- يمنع إنشاء نسخ الكترونية غير مصرح بها من المستندات والوثائق التي تخص (جهة العمل) وإداراتها او لأي مواد محمية بحقو ق نشر لغرض نشرها أو إرسالها عبر شبكة (جهة العمل)

عاشراً: سياسة أمان محطات العمل (الكمبيوتر وملحقاته)

مقدمة

تستخدم أجهزة الكمبيوتر وملحقاتها) طابعات، ماسحات ضوئية، أجهزة كمبيوتر محمولة، الخ (في أداء العمل يومي ا بطريقة معقولة ومتناسبة مع أهداف واستراتيجيات (جهة العمل)، ولتقديم أفضل مستو ى للخدمة مع أعلى درجات الحماية والخصوصية للمستخدمين، وضعت "سياسة محطات العمل" لضمان استخدام مهني لمحطات العمل.

الغرض من السياسة

تهدف هذه السياسة لحماية المستخدم ومحطات العمل من المخاطر المحتملة وذلك بتحديد سياسات وإجراءات استخدام اجهزة الكمبيوتر وملحقاتها في (جهة العمل)

النطاق

تسري هذه السياسة على جميع الموظفين والمستخدمين الذين يستعملون أجهزة الكمبيوتر وملحقاتها والخدمات المرتبطة بها.

السياسة

- ✓ يسمح للمستخدم باستعمال أجهزة الكمبيوتر المخصصة له، أو التي المصرح له باستعمالها. ولا يجو ز استخدام أجهزة الآخرين، أو محاولة الدخول عليها.
- ✓ تقع المسؤولية الكاملة على المستخدم للاستخدام الملائم لجميع الموارد المخصصة له بما فيها من اجهزة الكمبيوتر وملحقاتها أو برمجيات الأجهزة.
- ✓ لا يسمح للمستخدمين بالوصول إلى الشبكة باستخدام الحواسيب الشخصية واللوحية والهواتف الذكية. الا بتصريح من الادارة الفنية المختصة.
- ✓ يجب عدم محاولة الوصول إلى أجزاء ممنوعة الوصول من الشبكة، مثل نظام التشغيل الرئيس ي، برامج الأمان وغيرها دو ن الموافقة من الادارة المختصة.
- ✓ يجب عدم وضع أو تنصيب أو استخدام أي برامج أو أدوات أو أجهزة قد تؤدي إلى أو تساعد على تلف البرامج أو الأجهزة أو مكونات النظام.
- ✓ يمنع تثبيت أو استخدام الأدوات التي عادة ما تستخدم لمهاجمة أنظمة الأمن أو اختراق أنظمة الكمبيوتر أو الشبكات الأخر ى (مثل كاشفات كلمات السر أو ماسحات الشبكة... إلخ)
- ✓ يجب احترام الخصوصية الشخصية وحقو ق الآخرين وعدم الحصو ل على بيانات تخص مستخدم آخر، إضافة إلى البرامج أو الملفات الأخر ى من دو ن إذن مسبق.
- ✓ يطلب موافقة خاصة من قسم تقنية المعلومات قبل تنصيب أي برامج أو تركيب أجهزة خاصة على أنظمة (جهة العمل)

- ✓ أجهزة الكمبيوتر تعتبر اعارة من (جهة العمل) لذا فهي للاستخدام الرسمي لـ (جهة العمل) فقط ولا يجوز استخدامها من قبل أفراد الأسرة أو الأصدقاء تحت أي ظرف من الظروف.
- ✓ عند إرجاع جهاز الكمبيوتر، تحتفظ إدارة تقنية المعلومات بالحق في تنظيف القرص الثابت من أي بيانات وإعادة تثبيت كافة البرامج المبدئية. المستخدم مسؤول عن أي بيانات يتركها على الكمبيوتر المحمول عند إعادتها إلى (جهة العمل)
- ✓ تحتفظ إدارة تكنولوجيا المعلومات بحقها في استرجاع جميع المعدات التي تم اعارتها للمستخدمين من أجل إجراء تحديثات وتحسينات للبرامج، و / أو استبدال أو تحديث الأجهزة في أي وقت.
- ✓ لا يقوم موظفو ادارة تقنية المعلومات بالدخول (login) للأجهزة الشخصية لأعمال الصيانة الا بعد اخذ الاذن من صاحب العلاقة مباشرة.
- ✓ اجهزة الكمبيوتر وملحقاتها موجودة لخدمة الموظفين والمستخدمين لأداء الأعمال بطريقة أفضل، وعليه فإنه ليس من الممكن استغلالها لأغراض شخصية.
- ✓ توفر (جهة العمل) مجموعة واسعة من الطابعات المتصلة بالشبكة للمساعدة في اداء اعمال (جهة العمل)، كما يُسمح بطابعات سطح المكتب الفردية، وسيتم دعمها من قبل قسم تقنية المعلومات.
- ✓ يحظر على موظفي (جهة العمل) شراء معدات الشبكات الخاصة بهم، بما في ذلك على سبيل المثال لا الحصر: بطاقات الشبكة المحلية والبطاقات اللاسلكية وأجهزة التوجيه والمبدلات وتوصيل كابلات الشبكة والطابعات الجاهزة للربط بالشبكة.
- ✓ يعتبر استقرار الشبكة أم را بالغ الأهمية في بيئة (جهة العمل)، وقد تؤدي إضافة معدات الشبكة غير المصرح بها لشبكة (جهة العمل) إلى حدوث مشكلات يصعب تشخيصها.
- ✓ عند استعمال الكمبيوتر يجب أن يكون الدخول باستخدام اسم المستخدم وكلمة المرور الخاص به، وعند ترك الجهاز ولو لفترة وجيزة يجب قفل شاشة الجهاز بكلمة المرور.
- ✓ لا يجب تخزين أي وثائق أو ملفات لا علاقة لها بالعمل في المساحات المخصصة للموظفين على الخادم المخصص لذلك.
- ✓ مسؤولية المستخدم أن يتعلم كيفية استعمال جهاز الكمبيوتر وملحقاته بشكل سليم، وإذا شعر أنه بحاجة إلى التدريب، فعليه التوجه وطلب المساعدة من المعنيين في القسم المختص.
- ✓ لا يسمح لأي شخص من خارج (جهة العمل) باستخدام حواسيب (جهة العمل) إلا بإذن كتابي رسمي.
- ✓ يجب على المستخدم عدم ابطال عمل برامج مكافحة الفيروسات والبرامج الخبيثة على اجهزة كمبيوتر (جهة العمل)، كما يجب ان يتم فحص وسائل تخزين البيانات (مثل الأقراص المضغوطة أو محركات الأقراص الثابتة أو ذاكرة الفلاش) قبل فتح أي ملف أو برنامج.

- ✓ يحظر على المستخدمين نسخ أية مواد أو برامج من اجهزة الكمبيوتر الخاصة بـ (جهة العمل) لتوزيعها خارجها دو ن موافقة خطية وصريحة.

الحادي عشر: سياسة مضاد الفيروسات

مقدمة

العتاد البرمجي والمادي الذي يكونان معاً الشبكة الداخلية يعد مورداً أساسياً لعمل ل (**جهة العمل**)، فهي تعين الموظفين على إجراء أعمالهم اليومية والتي لن يتمكنوا من تنفيذها من دون وجود هذه الأنظمة. تشكل الفيروسات خطراً كبيراً على هذه الأنظمة، إذا يمكنها التسبب في اضطراب عملها وقد تسفر إلى فقد المعلومات أو تخريبها وفسادها مما يؤدي إلى ضرر بإنتاجية (**جهة العمل**)،

الغرض

صممت هذه الوثيقة للإرشاد والتوجيه نحو العمل على التقليص من خطر الإصابة بالفيروسات وإلى ما يجب اتخاذه في حالة مواجهتها.

نطاق الاختصاص

تنطبق هذه السياسة على:

- كل الموظفين طالما كانوا يستخدمون معدات (جهة **العمل**)، للدخول على شبكة (جهة **العمل**)، من أي مكان، ومن أي كمبيوتر وعبر أي وصلة انترنت.
- الأشخاص الآخرين العاملين للمؤسسة والافراد والجهات المنخرطين في أي عمل ما معها والمستعملين لمعدات وشبكات (**جهة العمل**).
- أياً أحد أعطي له الحق في الدخول على شبكة (جهة **العمل**)،

السياسة

✓ **مسؤوليات المستخدم**

- يجب أن يستعمل فقط برنامج مضاد الفيروسات المعتمد لدى (**جهة العمل**)، والذي يجب أن يكون متوفراً من خلال موقع التحميل الخاص بـ(جهة العمل) مثلاً: يجب تحميل وتنصيب الإصدار الحالي، كما يجب تحميل وتنصيب آخر التحديثات للبرنامج فور توفرها.
- يمنع فتح أي ملف أو ماكرو مرفق برسالة بريد الكتروني من مصدر غير معروف أو مشبوه أو غير موثوق به. يجب حذف هذه الملحقات على الفور ومن ثم تأكيد الحذف بتفريغ سلة المهملات.
- يجب مسح الرسائل المزعجة (Spam) (والرسائل المتسلسلة) Chain) وغيرها من رسائل البريد الغير مرغوب بها وعدم إعادة إرسالها للغير.
- يمنع تحميل الملفات من مصادر غير معروفة أو مشبوهة.

- يجب تجنب المشاركة المباشرة على قرص التخزين بصلاحيات القراءة والكتابة مالم يكن هناك حاجة ضرورية لذلك وتلبية لمتطلبات العمل التي لا يمكن تحقيقها بطريقة أخرى.
- يجب إجراء كشف عن الفيروسات لأي وسيط تخزين متنقل قبل استخدامه.
- يتوجب حفظ نسخ احتياطية للبيانات الحساسة وإعدادات النظام بشكل دوري وتخزينها في مكان آمن.
- يحظر على المستخدمين الخوض في إي نشاط يستهدف به صناعة و/أو توزيع البرامج الخبيثة) مثل الفيروسات والديدان واحصنة طروادة ورسائل البريد الالكتروني المفخخة . . .إلخ (داخل شبكة أو أنظمة (**جهة العمل**).
- يتوجب على المستخدمين إعلام فريق تقنية المعلومات ب (جهة العمل) في حالة اكتشاف وجود فيروس بأنظمتهم.
- أنظمة تقنية المعلومات المصابة ببرنامج خبيث أو فيروس ولم يتمكن مضاد الفيروسات من معالجتها يجب فصلها وعزلها من شبكة (جهة العمل) إلى أن تصبح خالية من العدوى.
- إذا اكتشف المستخدم أن نظامه مصاب بعدوى ما فيجب عليه القيام بالتالي:
  - إبلاغ فريق تقنية المعلومات ب(جهة العمل) على الفور.
    1. إطفاء الجهاز.
    2. ضمان ألا يستعمل الجهاز موظفين آخرين.
    3. أن يكون مستعداً لاطلاع فريق تقنية المعلومات على أي إجراء قام به قد يكون سبب العدوى.

✓ **مسؤوليات فريق تقنية المعلومات ب (جهة العمل)،**

- يجب توفير برنامج مضاد الفيروسات وتجهيزه لجميع الموظفين من قبل فريق تقنية المعلومات، وهم فقط من يحق لهم تنصيب وضبط البرنامج على أنظمة المستخدمين ومخدمات الشبكة الخاصة ب (جهة العمل)
- يجب توزيع ونشر تحديثات برنامج مضاد الفيروسات عبر شبكة (**جهة العمل**) بشكل آلي فور وصولها من الشركة المصنعة ويجب ضبط البرنامج ليتحقق من وجود التحديثات كل 60 دقيقة.
- تعريفات الفيروسات والبرامج الخبيثة يجب نشرها عبر شبكة (جهة العمل) بشكل آلي فور وصولها من الشركة المصنعة ويجب ضبط البرنامج ليتحقق من وجود التحديثات كل 10 دقائق، كما يجب ربط جميع نسخ البرنامج الموجودة بالأنظمة بمخدم تحميل تعريفات ثانوي بحيث إذا لم يسجل الجهاز دخوله بشبكة (جهة العمل) يمكنه تحميل التعريفات من المخدم الثانوي.
- يجب ضبط برنامج مضاد الفيروسات للقيام بمسح في الوقت الحقيقي (Real Time Scanning) وإجراء مسوحات دورية مجدولة زمنياً.

- يجب تفعيل ميزة المسح التلقائي عند الدخول (On-access Scanning) في مضاد الفيروسات لوسائط التخزين المحمولة.
- مخدم مضاد الفيروسات يجب مراقبته بشكل يومي من قبل عضو معين من فريق تقنية المعلومات بـ(جهة العمل) ومتابعة ما يصدره من تنبيهات وإنذارات، وكما يجب إحالة إي مشكلة لا يمكن حلها عن بعد عبر واجهة الإدارة المركزية للخادم إلى مكتب دعم تقنية المعلومات والذي بدورهم يعتبرونها حادثة ويقومون بتكليف أحد الاخصائيين للتحقيق في الأمر.
- إذا أصيب عدد من الأجهزة (ثلاثة أو أكثر) ببرنامج خبيث في نفس الوقت فيتوجب إصدار تقرير فني حول أسباب العدوى وإحالته إلى مسؤولي الأمن السيبرانية بالإدارة العليا.
- يتوجب إصدار تقرير نصف سنوي بخصوص مدى التزام الجميع بتطبيق السياسة وإحالته لمسؤولي الأمن السيبراني بالإدارة العليا ومدير فرع بـ(جهة العمل) إن وجد وإلى فريق التخطيط الاستراتيجي لتقنية المعلومات في موعد محدد.
- يجب وضع آلية لمنع التلاعب بإعدادات وضبط برنامج مضاد الفيروسات من قبل المستخدمين.
- في حالة اشتباه المستخدم في وجود فيروس بجهازه وقام بالتبليغ عنه لمكتب دعم تقنية المعلومات، فعلى فريق تقنية المعلومات القيام بالتالي:
  1. الكشف على الجهاز وأي وسائط تخزين ملحقه به.
  2. إعادة ضبط الجهاز في حالة كانت الإصابة حرجة برمجية الفدية الخبيثة مثلاً.
  3. الكشف على أي خادم قد يكون اتصل به الجهاز المصاب.
  4. محاولة معرفة مصدر العدوى.
  5. ضمان توثيق الحادثة.

سياسات حماية الشبكات

أولاً: سياسة جهاز التوجيه ومبدل (router and Switch) الشبكة

نظرة عامة

لا توجد الية معينة لحماية الشبكة, لأن أي نظام أمني يمكن أن يتعرض للتخريب والاختراق, إن لم يكن من الخارج ,فإنه المؤكد أن من الداخل, في نهاية المطاف لتأمين شبكة يجب تنفيذ طبقات مختلفة من الأمن, بحيث يجب على المهاجم

اختراق نظامين أو أكثر للوصول إلى الأصول الهامة, الخطوة الأولى في تطبيقات السياسات هي تحديد السياسيات التي سيتم تنفيذها, وغالباً ما تقيد التدابير الأمنية الأفراد في ممارساتهم التشغيلية, مما يردي إلى تعزير اللوائح الأمنية ,لذا, تحكم سياسات الشبكة, كيفية تنفيذ الشبكة وتهيئتها لتبسيط عمل الموظف في الظروف العادية ,وكذلك إرشادات كيفية التفاعل أو التعامل أثناء حدوث الحوادث في هذا السياق , يشرح القسم التالي فرض مقاييس السياسات لكل مصطلح أو مبدأ من الشبكة لحماية المعلومات والنظم.

سياسات جهاز التوجيه ومبدل (Router and Switch) الشبكة

المقدمة

توفر أجهزة التوجيه ومبدلات الشبكة وظائف أمان مهمة داخل الشبكة إذا ما تم تهيئتها بشكل صحيح، فهما ضمن العديد من الأجهزة والبرامج المتوفرة والتي تساعد في إدارة وحماية الشبكة الخاصة من الشبكة العامة، تحدد سياسة أمن الموجه ومبدل الشبكة متطلبات التهيئة لتلبية معايير الأمان ومتطلبات إدارة التغيير والمتطلبات التشغيلية.

الغرض:

هذه الوثيقة مصممة لحماية معدات وبيانات (جهة العمل) وشركائها التجاريين أو أي بيانات مملكة أو تحت تصرف (جهة العمل) من خلال تحديد الحد الأدنى لمعايير التكوين والضبط لجميع أجهزة التوجيه والمبدلات التي تتصل بشبكة (جهة العمل)

النطاق:

يجب على جميع الموظفين والمتعاقدين والمستشارين والعاملين المؤقتين وغيرهم ممن يستخدمون أجهزة الشبكة مثل الموجه و/ أو المبدل الالتزام بهذه السياسة، كما تخضع لهذه السياسة جميع أجهزة التوجيه والمبدلات المتصلة بالشبكة

السياسة:

✓ يجب أن يستوفي كل جهاز توجيه / مبدل معايير التهيئة التالية:

- لا يتم تكوين أي حسابات مستخدمين محليين على جهاز التوجيه و/ أو التبديل نفسه، بل يجب ان تستخدم أجهزة التوجيه والمبدلات خادم AAA مخصص لهذا الغرض مثل (TACACS+) للقيام بجميع مصادقات المستخدمين.
- يجب استخدام كلمة السر (Enable Secret) بدلاً من تمكين كلمة المرور (Enable password)
- يجب الحفاظ على كلمة السر (enable Secret) مشفرة ومؤمنة على جهاز التوجيه أو المبدل

- يجب تعطيل الخدمات أو الميزات التالية:

1. البث الموجه عبر بروتوكول الانترنيت (IP directed broadcasts) يمكن تفعيل البث الموجه نحو بروتوكول الانترنيت عند الرغبة في تنفيذ خدمات الإدارة عن بعد مثل النسخ الاحتياطية على الأجهزة المضيفة في شبكة فرعية ليس لها اتصال مباشر بالأنترنيت
2. الحزم الواردة لجهاز التوجيه/التبديل والقادمة من مصادر ذات عناوين غير صالحة مصل عناوين RCF1918
3. خدمات TCP الصغيرة (TCP small services)
4. خدمات UDP الصغيرة (UDP small services)
5. جميع خدمات الويب التي تعمل على جهاز التوجيه
6. التكوين التلقائي (Auto configuration)
7. بروتوكول استكشاف الأجهزة للطبقة الثانية مثل (LLDP&CDP) وبرتوكولات الاكتشاف الأخرى.

- يجب عدم سماح ما يلي على واجهة منافذ أجهزة التوجيه/ التبديل:

1. نيابة عن (وكيل) بروتوكول حل العناوين (Proxy-ARP)
2. رسائل (ICMP) الغير قابلة للوصول
3. التبديل السريع (Fast switching) والتبديل الذاتي (autonomous switching)
4. التخزين المؤقت للمسار متهدد البث (Multicast)
5. بروتوكول عمليات الصيانة (MOP)

- يجب ضبط الخدمات التالية:

1. تشفير كلمة المرور
2. مزامنة الوقت (NTP) يجب مزامنة جميع ساعات الشبكة من مصدر زمن مشترك

- جميع تحديثات التوجيه (Routing) يجب أن تتم باستخدام تحديثات التوجيه الامن.

- استخدام نصوص SNMP الموحدة ل (جهة العمل) يجب إزالة النصوص الافتراضية، مثل العامة أو الخاصة (Public & Private) يجب تهيئة SNMP لاستخدام النسخة الأكثر أماناً من البرتوكول المدعومة من كلال الطرفين , الجهاز وأنظمة الإدارة.

- يجب استخدام قوائم التحكم في الوصول (Access control lists) للحد من مصدر ونوع حركة المرور التي يمكن ان تصل للجهاز نفسه.

- يجب أن يحتوي كل جهاز توجيه (routing) على اشعار تنبيه يظهر في نافذة أو أوار الدخول للنظام يحوي عل معلومات تفيد بأن الدخول هنا مسموح به للمستخدمين المصرح لهم بذلك فقط لا غير. البيان التالي يجب أن يظهر عند استخدام أي شكل من أشكال تسجيل الدخول سواء كانت محلية او عند بعد.
" يحظر الدخول لهذا الجهاز لغير المصرح لهم.
يجب أن يكون لديك إذن صريح للدخول الى هذا الجهاز او ضبطه. أي إجراء أو تغيير تقوم به يكون عرضة للتوثيق والحفظ إذا ما ارتكبت أي مخالفات للسياسات المعتمدة، فسوف تتعرض لاتخاذ إجراءات عقابية صارمة ضدك حسب اللوائح المعمول بها. ليس لك أي حق في الخصوصية على هذا الجهاز استخدامك لهذا النظام يعد موافقة تلقائية على مراقبة ما تقوم به "

- لا يجوز أبداً استخدام بروتوكول Telnet عبر أي شبكة لغدارة جهاز توجيه، مالم يكن هناك نفق آمن يحمي مسار الاتصال بالكامل، الإصدار من بروتوكول (SSH) هو بروتوكول الإدارة المفضل

- ينبغي وضع أجهزة التوجيه والمبدلات في مكان يقتصر فيه الدخول على الأشخاص المرخص لهم

- يجب أن يقوم المبدل بتعطيل منفذ أو مجموعة من المنافذ في حالة ظهر بها عناوين أجهزة (MAC) جديدة او غير مسجلة مسبقاً على المنفذ ذا كانت هذه الميزة متاحة.

- يجب ان يقوم المبدل بتوليد رسائل (SNMP TRAP) إذا وقع الاتصال وتم إعادة توليده في حال توافرت هذه الميزة

- يجب ان تستخدم بروتوكولات التوجيه الديناميكية المصادقة عند إرسال تحديثات التوجيه على الأجهزة المجاورة (يجب تمكين ميزة تحويل كلمة المرور بدالة الاختزال (Hashing) في نص المصادقة عند دعمها.

- من خلال المعيار المعتمد لدى (جهة العمل) يتم تحديد فئة من الأجهزة تعتبر ذات وضع حساس نظراً لطبيعة عملها، وبذلك فإنها تحتاج إلى خدمات وضبط إضافي والذي يجب أن يشمل:

    1. متابعة مراقبة لقوائم التحكم في الوصول لبرتوكول الانترنيت (IP Access List Accounting)

    2. تسجيل وتوثيق أحدا الجهاز (Device Logging)

3. يجب إسقاط الحزم الواردة للموجه التي يكون مصدرها من عناوين غير صالحة، مثل عناوين RCF1918 أو تلك التي يمكن استخدامها لخداع (Spoof) حركة مرور الشبكة

- يجب توثيق عمليات ضبط الشبكة والتغيرات التي تتم عليها بشكل منتظم وذلك لفهم بنيتها يجب أن يتضمن مستند توثيق الشبكات ما يلي:

1. رسم تخطيطي للشبكة
2. ضوابط النظام (system Configuration)
3. قواعد الجدار الناري
4. عناوين برتوكولات الأنترنيت (IP addresses)
5. قوائم التحكم في الوصول

ثانياً: سياسة الاتصالات اللاسلكية:

المقدمة

مع الانتشار المتسارع للهواتف الذكية والأجهزة اللوحية، فإن الاتصال اللاسلكي أصبح واسع الانتشار وهو ما أصبح أمراً مسلماً به ولا تخلو من أي مؤسسة، يمكن الضبط اللاسلكي الغير الآمن توفير باب مفتوح وسهل للمخترقين والقراصنة.
نعد سياسات الاتصالات اللاسلكية ضرورية لأمن الكمبيوتر نظراً لوجود طلب متزايد على المعدات اللاسلكية في كل (جهة عمل) اليوم. قد تحدد سياسة الاتصال اللاسلكي انه لا يجب استخدام أي معدات لاسلكية لذلك لن يكون عملياً وواقعياً لأن ذلك قد يؤدي للجوء بعض الإدارات على انتهاك لهذه السياسة، لذلك كان من الأفضل تحديد الشروط وتحديد المعدات المعتمدة للاستخدام اللاسلكي لتقليل مخاطر الأمان المرتبطة باللاسلكي الذي لابد منه.

الغرض:

الغرض من هذه السياسة هو تامين وحماية أصول المعلومات التي تملكها (جهة العمل). تمنح (جهة العمل) الوصول الى هذه المواد كامتياز ويجب أن تدار هذه الموارد بطريقة مسؤولة للحفاظ على سرية ونزاهة وتوافر جميع الأصول المعلوماتية.
كما تحدد هذه السياسة الشروط التي يجب ان تستوفيها أجهزة البنية التحتية اللاسلكية للاتصال بشبكة (جهة

العمل)

بحيث لا تتم الموافقة إلا على أجهزة البنية التحتية اللاسلكية التي تفي بالمعايير المحددة في هذه السياسة أو تلك التي تم منحها استثناء من قبل إدارة امن المعلومات للاتصال بشبكة (جهة العمل).

النطاق:

تنطبق هذه السياسة على جميع أجهزة البنية التحتية اللاسلكية المتصلة بشبكة (جهة العمل) أو تكون موجودة ضمن (جهة العمل) والتي توفر اتصالاً لاسلكياً بأجهزة طرفية، بما في ذلك على سبيل المثال، أجهزة الكمبيوتر المحمولة وأجهزة سطح المكتب والهواتف الوية والأجهزة اللوحية. وبشكل في ذلك أي شكل من أشكال أجهزة الاتصال اللاسلكي القادر على نقل حزم البيانات، لذلك يجب ان يلتزم بهذه السياسة جميع الموظفين والاستشاريين والعاملين المؤقتين وغيرهم في (جهة العمل)، كما تشمل جميع الموظفين التابعين لأطراف ثالثة والموكل لها إدارة أجهزة البنية التحتية اللاسلكية بالنيابة عن (جهة العمل)

السياسة:

- ✓ جميع أجهزة البنية التحتية اللاسلكية الموجودة في موقع (جهة العمل) والمتصلة بشبكتها، أو التي توفر الوصول إلى معلومات مصنفة على أنها سرية يجب عليها ما يلي:
  - الالتزام بالمعايير المحددة في معيار الاتصالات اللاسلكية
  - استخدام برتوكولات المصادقة والبنية التحتية المعتمدة من قبل (جهة عمل)
  - استخدام برتوكولات التشفير المعتمدة لدى (جهة العمل)
  - الحفاظ على العناوين المادية للأجهزة (MAC) التي يمكن تسجيلها وتتبعها.
- ✓ للحد من احتمال إساءة استخدام الشبكة اللاسلكية
  - بنبعي ان تكون هنالك مصادقة سليمة للمستخدم مع الاستبدال المناسب لآلية WEP وتتبع الشذوذ (Anomaly tracking) على الشبكة المحلية اللاسلكية
  - في نفس الوقت، القائمة التالية تحوي على عدداً من الأحداث المشبوهة التي قد تقع داخل الشكة المحلية اللاسلكية والتي ينبغي دائما أن تأخذ في عين الاعتبار عند ضبط أنظمة كشف المتسلل:

1. إطارات الإرشاد (Beacon Frames) القادمة من نقطة وصول لاسلكية لم يطلب منها ذلك (unsolicited)
2. فيضان الأطر غير المصادق عليها هجوم (MITM)
3. اطر بيانات تحوي عنوان MAC مكرر.
4. تغيير عنوان MAC بشكل عشوائي

- ✓ بروتكولات التشفير اللاسلكية:

يفضل استخدام بروتوكول حماية الوصول للواي فاي الإصدار 2 (WAP2) كبرتوكول تشفير للشبكات اللاسلكية بدلاً من بروتوكول حماية الوصول للواي فاي الإصدار الأول (WAP) وبرتوكول الخصوصية المكافئة للشبكات السلكية (WEP) وذلك لأنه يوفر خوارزمية أمان أقوى وتشفيراً متقدماً كما يتحقق من صحة الرسالة وتكاملها.

- ✓ يجب توثيق عمليات ضبط الشبكة والتغييرات التي تتم عليها بشكل منتظم وذلك لفهم بنيتها، يجب أن يتضمن مستند توثيق الشبكات ما يلي:

1. رسم تخطيطي للشبكة
2. ضوابط النظام (system Configuration)
3. قواعد الجدار الناري
4. عناوين برتوكولات الأنترنيت (IP addresses)
5. قوائم التحكم في الوصول

ثالثاً: سياسة الشبكة الافتراضية الخاصة (VPN)

المقدمة:

الشبكة الخاصة الظاهرية (VPN) هي شبكة اتصال خاصة وآمنة توفر طريقة ملائمة للوصول الة موارد الشبكة الداخلية عن بعد، عبر الشبكة العامة (الانترنيت)، حيث توفر VPN وصولاً آمناً من خلال توفير وسيلة لحماية البيانات أثناء انتقالها عبر شبكة غير موثوق بها.

الغرض:

تهدف هذه لسياسة إلى توفير إرشادات خاصة باتصالات الوصول عن بعد عبر IPsec أ, شبكة L2TP الخاصة الافتراضية (VPN إلى شبكة (جهة العمل).

النطاق:

تنطبق هذه السياسة على جميع موظفي (جهة العمل) والمقاولين والمستشارين والموظفين المؤقتين وغيرهم من العمال بما في ذلك جميع الموظفين المنتسبين إلى أطراف ثالثة المستخدمين لشبكات VPN ليتمكنوا من الدخول إلى الشبكة (جهة العمل).

تنطبق هذه السياسة على تطبيقات VPN التي يتم توجيهها للمرور عبر مركز IPsec (IPsec Concentrator)

السياسة:

- ✓ تقع على عاتق الموظفين الذي لديهم امتيازات استخدام الشبكة الافتراضية الخاصة VPN ضمان عدم السماح للمستخدمين غير المصرح لهم بالوصول إلى الشبكات الداخلية ل (جهة العمل) عبر وصلات ال (VPN) الخاصة بهم.
- ✓ يجب التحكم في استخدام الشبكة الافتراضية الخاصة VPN باستخدام مصادقة بكلمة المرور لمرة واحد (One time Password) كجهاز إشارة السماح (Token Device) أو نظام المفتاح العام / الخاص مع اختيار عبارة مرور قوية (Passphrase)
- ✓ عندما يكون الاتصال بشبكة (جهة العمل) نشطاً، فإن آلية الشبكات الافتراضية الخاصة (VPN) يجب ان تقوم بإجبار كل حركة المرور من وإلى الكمبيوتر عبر نفق VPN بينما يقوم بطرح وتجاهل أي حركة بيانات أخرى.
- ✓ تقاسم أو ازدواج الاتصال عبر نفق التشفير (Dual Split Tunneling) غير مسموح، إذ لا يسمح بحصول أكثر من اتصال شبكي واحد فقط في نفس الوقت،

  تقاسم أو ازدواج الاتصال عبر نفق التشفير يسمح بوجود اتصالين نشطين متزامنين في نفس الوقت, احدهما لشبكة آمنة عبر (VPN) والثاني لشبكة غير آمنة، هذا الوضع يشكل ثغرة تسهل الاتصال المباشر من الانترنيت الغير آمن إلى الشبكة المؤمنة باتصال بتقنية الـ (VPN)
- ✓ بوابات الشبكات الافتراضية الخاصة (VPN gateways) يتم اعدادها وإدارتها من قبل موظفي القسم الخاص بعمليات الشبكة لـ(جهة العمل)

- ✓ يتوجب على كل الأجهزة التي تتصل بالشبكة الداخلية لـ(جهة العمل) باستخدام (VPN) أو غيرها من التقنيات ان تستخدم برامج مضاد للفيروسات محدثة ومطابقة للمعايير من قبل (جهة العمل)، بما في ذلك الحواسيب الشخصية.
- ✓ يجب فصل مستخدمي VPN تلقائياً عن شبكة (جهة العمل) بعد ثلاثين دقيقة من عدم النشاط. ويج على المستخدم تسجيل الدخول مرة أخرى لإعادة الاتصال بالشبكة.
  " يمنع استخدام Pings او عمليات شبكة مصطنعة أخرى للحفاظ على الاتصال مفتوحاً"
- ✓ يجب ضبط جهاز (VPN concentrator) بتحديد وقت أي اتصال بحيث لا يتجاوز الأربع وعشرين ساعة
- ✓ يجب على مستخدمي أجهزة الكمبيوتر التي ليست من الأجهزة التي تملكها (جهة العمل) تهيئة الأجهزة بحيث تتوافق مع سياسات الشبكة وسياسات الربط بتقنية الشبكة الافتراضية الخاصة (VPN)لـ (جهة العمل).
- ✓ باستخدام تكنولوجيا VPN مع الأجهزة الشخصية، يجب أن يعي المستخدمون أن اجهزتهم أصبحت امتداداً فعلياً وجزء من شبكة (جهة العمل)، وبالتالي فهي تخضع لنفس القواعد واللوائح التي تنطبق على المعدات التي تستخدمها جهة العمل.
- ✓ يجب توثيق عمليات ضبط الشبكة والتغييرات التي تتم عليها بشكل منتظم وذلك لفهم بنيتها، يجب أن يتضمن مستند توثيق الشبكات ما يلي:

1. رسم تخطيطي للشبكة
2. ضوابط النظام (system Configuration)
3. قواعد الجدار الناري
4. عناوين برتوكولات الأنترنيت (IP addresses)
5. قوائم التحكم في الوصول

رابعاً: سياسة جدار الحماية/الناري (firewall)

مقدمة:

الاتصال بشبكة مفتوحة وغير آمنة مثل الانترنيت يؤدي الى احتمالية فتح مدخلاً كبيراً للهجمات السيبرانية على الشبكة الداخلية لـ(جهة العمل). أحد أفضل الطرق للدفاع ضد هذه الهجمات هي استخدام الجدران النارية عند نقطة الاتصال بشبكة الانترنيت، حيث أنه من الضروري حماية الشبكات الخاصة الداخلية ومرافق الاتصالات الخاصة ب (جهة العمل)

الغرض:

يتم تعريف جدران الحماية (الجدار الناري) على أنها أنظمة أمان تتحكم وتقيد اتصال الشبكة وخدماتها، جدران الحماية تنشئ نقطة تحكم يمكن عبرها فرض عناصر التحكم بالوصول. بسعة هذا المستند إلى مساعدة (جهة العمل) في فهم قدرات تقنيات جدار الحماية وسياسات الجدار الناري.

النطاق:

تحدد هذه السياسة القواعد الأساسية المتعلقة بإدارة وصيانة الجدران النارية، وتنطبق على جميع الجدران النارية التي تملكها أو تؤجرها أو تتحكم بها (جهة العمل)

السياسة:

✓ مراجعة مجموعة القواعد للتأكد من اتباعها للترتيب كالتالي:

- مرشحات مكافحة الانتحال (حجب العناوين الخاصرة والعناوين الداخلية التي تظهر من الخارج)
- قواعد تصريح المستخدم (على سبيل المثال السماح ب HTTP إلى خادم الويب العام)
- قواعد تصريح الإدارة (مثل رسائل تنبيه (SNMP traps) لخادم إدارة الشبكة)
- الرفض والتنبيه (تنبيه مسؤولي الأنظمة حول حركة المرور المشبوهة)
- الرفض والتوثيق (حفظ سجل حركة المرور للتحليل)

✓ جدار الحماية القائم على التطبيق:

- في حالة الدخول على خادم مخصص، يجب وضع جدار ناري برمجي يعمل بالنيابة (وكيل) (Applications Proxy Firewall) ما بين المستخدم المتصل عن بعد والخادم المخصص ولذلك لإخفاء هوية الخادم.
- التأكد من مراقبة المسؤولين لأية محاولات لانتهاك سياسة الأمن باستخدام سجلات التدقيق التي تم انشاؤها بواسطة جدار الحماية على مستوى التطبيق.
- ضمان أن هنالك آلية لتحديث وسد ثغرات الجدار الناري على مستوى التطبيقات والتحقق بأنها محدثة لسد آخر الثغرات.
- تأكد من وجود عملية لتحديث البرنامج بأحدث بصمات الهجوم.
- في حال تنزيل التواقيع من موقع الموردين والشركات المصنعة، يجب التأكد من انها من موقع موثوق.

- في حال إرسال البصمات بالبريد الالكتروني إلى مسؤول النظام يجب التأكد من استخدام التوقيعات الرقمية للتحقق من المورد وان المعلومات المنقولة لم يتم تغييرها أثناء النقل.
- يجب حظر الأوامر التالية لـ (SMTP) في جدار الحماية على مستوى التطبيق:
  1. EXPN (التوسيع - expand)
  2. VRFY (تحقق - verify)
  3. DEBUG
  4. WIZARD
- يجب حظر الامر التالي لFTP :
  1. PUT
- مراجعة وحظر العناوين (URL's) والتأكد بانها ملائمة، فعلة سبيل المثال، يجب حظر أي عنوان URL لمواقع المخترقين.
- التأكد من أن المستخدمين المخولين هم فقط من يتم التصديق عليهم بواسطة جدار الحماية على مستوى التطبيق.

✓ تفحص بحالة الاتصال (Stateful inspection)

- مراجعة جداول الحالة (State Tables) للتأكد من إعداد القواعد المناسبة من حيث عناوين المصدر والوجهة ومنافذ المصدر والوجهة والمهلة
- تأكد من أن المهلة مناسبة حتى لا تعطي المتسلل الكثير من الوقع لشن هجوم ناجح

بالنسبة لعناوين URL

- في حال استخدام خادم نصفية عناوين URL، تأكد من تحديده بشكل مناسب في برنامج جدار الحماية. (إذا كان خادم التصفية من خارج (جهة العمل)، فتأكد من أنه من مصدر موثوق به)
- إذا كان الترشيح على عناوين MACمسموح به فيجب مراجعة المرشحات للتأكد من انها مقتصرة على عناوين MAC المناسبة لـ (جهة العمل)

✓ تسجيل الأحداث:

- تأكد من تفعيل خاصية تسجيل الاحداث وان يتم مراجعة السجلات لتحديد أي أنماط محتملة قد نشير الى وجود هجوم.
- سجلات إدارة جدار حماية الشبكة (الأنشطة الإدارية) وسجلات الأحداث (نشاط حركة المرور) يجب ان:
  1. يتم تخزينها على وحدة تخزين بديلة (ليس على نفس الجهاز)
  2. تتم مراجعتها يومياً على الأقل، مع الاحتفاظ بالسجلات لمدة تسعين يوماً

- ✓ التصحيحيات والتحديثات:
  - تأكد من اختبار وتثبيت أحدث التصحيحات والتحديثات المتعلقة بجدار الحماية الخاصة بك
  - إذا تم تنزيل التصحيحات والتحديثات تلقائياً من مواقع الويب الخاصة بالموردين، فتأكد من استلام التحديث من موقع موثوق به
  - في حال إرسال التصحيحات والتحديثات بالبريد الالكتروني غلة مدير النظام، تأكد من استخدام التوقيعات الرقمية للتحقق من المورد (Vendor) والتأكد من عدم تعديل المعلومات في الطريق
- ✓ تقييم / اختبار الضعف
  - يجب التحقق ما إذا كان هناك إجراء لاختبار المنافذ المفتوحة باستخدام (NMAP)، وما إذا كانت المنافذ غير الضرورية مغلقة.
  - التأكد من وجود إجراء لاختبار القواعد عند تأسيسها او تغييرها حتى لا يؤدي إلى رفض الخدمة او السماح باستمرار وجود نقاط ضعف دون أن يتم اكتشافها.
- ✓ الالتزام بسياسة الأمن:
  - تأكد من أن القواعد تتوافق مع سياسة أمن (جهة العمل)
- ✓ تأكد من أن العناوين التالية الخاصة، (RCF 1918) المنتحلة والعشوائية محظورة:
  - عناوين خاصة (RCF1918)

    10 0 0 0 - 10 255 255 255

    172 16 0 0 - 172 31 255 255

    192 168 0 0 - 192 168 255 255
  - عناوين محجوزة

    240 0 0 0
  - عناوين غير قانونية

    0 0 0 0
  - UDP echo
  - بث ICMP (RFC 2644)
- ✓ الوصول عن بعد
  - في حالة استخدام الوصول عن بعد، تأكد من استخدام برتوكول SSH (المنفذ 22) بدلاً من Telnet

- ✓ نقل الملفات

- إذا كان بروتوكول FTP مطلوباً، فتأكد من وضع الخادم، الذي يدعم FTP، في شبكة فرعية مختلفة عن تلك المخصصة للشبكة المحمية الداخلية

✓ حركة البريد الالكتروني

- التحقق من البرتوكول المستخدم للبريد والتأكد من وجود قاعدة لحظر حركة البريد الوارد باستثناء تلك القاصدة حادم البريد الداخلي.

✓ حظر حركة ICMP غير المرغب فيها (ICMP 8,11,3)

- تأكد من وجود قاعدة تمنع طلبات ورسائل ارتداد ICMP
- تأكد من وجود قاعدة تمنع ارسال رسائل تجاوزت الوقت (Time Exceeded) ورسائل الإبلاغ عن عدم القدرة على وصول الهدف (Unreachable)

✓ الخوادم الحرجة والحساسة (Critical Servers)

- التأكد من وجود قعدة تمنع حركة المرور الموجهة إلى عناوين داخلية حرجة وحساسة من مصادر خارجية. يجب أن تستند هذه القاعدة إلى المتطلبات التنظيمية، نظراً لأن بعض (جهات العمل) قد تسمح بتوجيه حركة المرور عبر تطبيق ويب وعب المنطقة المجردة من السلاح (DMZ)

✓ جدران الحماية الشخصية:

- تأكد من حصول مستخدمي الكمبيوتر المحمول على التدريب المناسب فيما يتعلق بالتهديدات وأنواع العناصر المحظورة بواسطة جدار الحماية والمبادئ التوجيهية لتشيل جدا الحماية الشخصي. خذا العنصر ضروري، حيث تعتمد الجدران النارية الشخصية أحياناً على مكالبة المستخدم بالرد على الهجمات، على سبيل المثال، ما إذا كنت تريد قبول/ رفض طلب من عنوان معين
- قم بمراجعة إعدادات الحماية الخاصة بجدار الحماية الشخصي للتأكد من أنه يقيد الوصول إلى منافذ معينة، ويحمي من الهجمات المعروفة، وأن هنالك تنبيهات كافين لتسجيل الدخول وتنبيهات للمستخدم في حالة حدوث اختراق.
- تأكد من وجود إجراء لتحديث البرنامج لأية هجمات جديدة أصبحت معروفة. ويمكن بدلاً من ذلك الاعتماد على ما توفره معظم الأدوات المشابهة من خيارات تحميل التحديثات التلقائية عبر الانترنيت، في مثل هذه الحالات، يجب التأكد من تلقي التحديثات من مواقع موثوق بها.

✓ جدران الحماية الموزعة

- التأكد من توزيع سياسة الأمن باستمرار على جميع الأجهزة المضيفة، خاصة عند وجود تغيرات في السياسة.

- التأكد من وجود ضوابط كافية لضمان سلامة السياسة أثناء النقل، على سبيل المثال،IPsec لتشفير السياسة عند النقل.
- تأكد من وجود ضوابط كافية لمصادقة المضيف المناسب

مرة أخرى يمكن استخدام IPsec للمصادقة مع شهادات التشفير

✓ استمرار توافر جدران الحماية:

- تأكد من وجد جدار حماية بديل على جدار الحماية الأساسي (Hot standby For The Primary Firewall)

✓ يجب توثيق عمليات ضبط الشبكة والتغييرات التي تتم عليها بشكل منتظم وذلك لفهم بنيتها، يجب أن يتضمن مستند توثيق الشبكات ما يلي:

1. رسم تخطيطي للشبكة
2. ضوابط النظام (system Configuration)
3. قواعد الجدار الناري
4. عناوين برتوكولات الأنترنيت (IP addresses)
5. قوائم التحكم في الوصول

سياسة الأطراف الثالثة

أولاً: سياسة الوصول للأطراف الثالثة

مقدمة

تعمل سياسة الوصول للأطراف الثالثة على بيان الإجراءات التي تحكم وصول أطراف ثالثة إلى شبكة (جهة العمل) وتطبيقاتها.

وتتمثل الأطراف الثالثة في الجهات الخارجة عن (جهة العمل) من مؤسسات أو أفراد.

تغطي السياسة الجوانب التالية للتعاملات مع الطرف الثالث:

- تقييم مخاطر الطرف الثالث.
- الاتفاقيات والعقود.
- توفير خدمات للشبكة.
- صلاحيات الوصول والاتصال للأنظمة والشبكات.
- أمن الوصول من قبل الاطراف الثالثة.

الغرض من السياسة

الغرض من هذه السياسة هو تحديد السياسات والمعايير لجميع الأطراف الثالثة التي تسعى للوصول إلى شبكة (جهة العمل) لغرض التعامل المشترك مع الأعمال المتعلقة بـ (جهة العمل)، وقد تم تصميم هذه السياسة للحد من التعرض المحتمل للمخاطر المرتبطة بوصول الطرف الثالث لـ (جهة العمل).

النطاق

تنطبق هذه السياسة على الموظفين في (جهة العمل) المختصين بتوفير وصول الأطراف الثالثة إلى شبكة (جهة العمل) أو الأجهزة الملحقة بها، وكذلك على جميع الأطراف الثالثة سواء كانوا أفراد ا أو شركات أو مؤسسات أو متعاقدين أو استشاريين أو متخصصين.

السياسة

- ✓ يجب التوقيع على اتفاقية عدم الإفصاح عند التعاقد مع الطرف الثالث، وتحديد دور ومسؤوليات الطرف الثالث بوضوح في هذه الاتفاقية.
  - لن يُمنح الطرف الثالث إمكانية الوصول إلى مرافق شبكة (جهة العمل) إلا بعد توقيع عقد رسمي يحدد الشروط والضوابط التي يجب على الأطراف الثالثة الالتزام بها لضمان الوصول الأمن إلى مرافق شبكة (جهة العمل) من قبل الأطراف الثالثة.
  - تتطلب جميع طلبات الاتصال الجديدة بين ا لأطراف الثالثة و(جهة العمل) موافقة الطرف الثالث وممثل (جهة العمل) على الاتفاقية والتوقيع عليها.
- ✓ المتطلبات ا لأولية (قبل الاتفاق): ستخضع عملية منح الوصول لمعدات تقنية المعلومات للمراجعة والتصديق من القسم المختص بذلك (قسم أمن المعلومات)
  - تجري المراجعة الأمنية للتأكد من أن أي توصيل يتطابق مع متطلبات العمل بأفضل طريقة ممكنة، وأنه يتبع مبدأ "أقل صلاحيات وصول".
  - يجب على جميع الأطراف الثالثة الالتزام بمتطلبات أمن المعلومات والتي تضمن الحد الأدنى من مستوى الأمان الذي تطلبه (جهة العمل) من قبل الطرف الثالث، والتي يتحدد من خلالها ما الذي يجب على (جهة العمل) تنفيذه والحفاظ عليه من تدابير أمنية تخص جميع جوانب أمن المعلومات وجميع عمليات الدعم المرتبطة بها.

- يجب على جميع الأطراف الثالثة التأكد من أنها لا تنتهك أياً من لوائح نظام إدارة أمن المعلومات في أي وقت أثناء تعاقدها مع (جهة العمل)

✓ إنشاء الاتصال:

- يجب أن يستند كل اتصال قائم على مبدأ "أقل صلاحيات الوصول" وفقاً لمتطلبات العمل والمراجعة الأمنية المعتمدة.

✓ تعديل أو تغيير الاتصال والوصول:

- يجب أن تتم التغييرات في الاتصال أو الوصول بناء على ما تقتضيه مصلحة العمل وأن تخضع للمراجعة الأمنية، كما يجب تنفيذ التغييرات من خلال عملية إدارة التغيير بـ (جهة العمل)

✓ وصول الطرف الثالث المسموح به:

- يسمح للطرف الثالث الوصول إلى أنظمة أو شبكة (جهة العمل) للأغراض المتفق عليها في العقد، ويشمل ذلك الشركاء لـ(جهة العمل) غير الموظفين مباشرة ولديهم وصول مباشر أو عن بعد إلى أنظمة وشبكة (جهة العمل).
- يجب السماح للطرف الثالث بالوصول إلى المرافق والخدمات والبيانات التي تكون مطلوبة لتنفيذ المهام المحددة في العقد فقط، وعلى النحو الذي تم توضيحه للمسؤولين على هذه المرافق والبيانات ضمن طلب الوصول الأصلي.

✓ الأجهزة والمعدات (محطات العمل) الخاصة بالطرف الثالث:

عندما تستخدم الأطراف الثالثة أجهزة الكمبيوتر الشخص ي / أجهزة الكمبيوتر المحمولة أو أي أجهزة غير مملوكة لـ(جهة العمل) للوصول إلى الموارد الموجودة على شبكة وأنظمة (جهة العمل)، يجب أن تضمن الأطراف الثالثة ما يلي:

- يجب أن تكون أنظمة التشغيل محدثة بشكل كامل مع أحدث التصحيحات.
- يجب تنصيب برامج مكافحة الفيروسات وبرمجيات التجسس والبرمجيات الضارة وبآخر التحديثات.

✓ وصول الأطراف الثالثة عن بعد:

- يتم تحديد مسؤوليات إدارة أمن وصول الطرف الثالث بوضوح لكل من (جهة العمل) والطرف الثالث، كما يجب توفير مستوى مناسب من الإدارة والدعم الفني من قبل الطرفين لضمان تحقيق الامتثال لهذه السياسة.
- يجب تعيين المناصب التالية لكل اتصال بين الأطراف:

1. مسؤول الخدمة أو من له الصلاحية ليكون مسؤولًا عن السماح بدخول الطرف الثالث من خلال تفويض الاتصال في تصريح كتابي.

2. المسؤول عن النظام والذي يتحمل المسؤولية الكاملة عن كل اتصال من ا لأطراف الثالثة وذلك للتأكد من تطبيق الأطراف للسياسات والمعايير لهذا الاتصال. كما أنه المسؤول عن تأكيد ما إذا كان مسموحا للطرف الثالث بالدخول إلى أنظمة المؤسسة، وكما له أن يحظر دخول الطرف الثالث إلى بعض الأنظمة الحساسة.

- ✓ الإبلاغ عن الحوادث: يجب أن تقوم ا لأطراف الثالثة بإبلاغ الإدارة عن أي حادثة تؤثر على أمن المعلومات والخصوصية، وعلى جميع نقاط الضعف الأمنية المشتبه بها أو ما قد يشكل تهديد ا لأصول تقنية المعلومات في (جهة العمل).
- ✓ إنهاء الوصول:
  - عندما انتهاء الحاجة إلى الوصول يجب أن يقوم المسؤول عن الاتصال داخل (جهة العمل) بإنهاء الوصول.
  - يجب أن يقوم المسؤولون عن كل اتصال بمراجعة هذه الاتصالات سنويا للتحقق من وجود حاجة لاستمرارها، وأن نوع الوصول الحالي يلبي متطلبات الاتصال المرجوة.
  - يتم على الفور إنهاء جميع الاتصالات التي لم يعد لها فائدة أو حاجة في تنفيذ أعمال (جهة العمل).
  - في حالة تم تعريفهم داخل نظام (جهة العمل)، يجب أن يكون لدى جميع الأطراف الثالثة والمستخدمين الخارجيين تاريخ صلاحية لحساباتهم.

القواعد الارشادية لاتفاقية عدم الإفصاح:

مقدمة

عندما تقوم (جهة العمل) بالدخول في مشاركة عمل مع طرف ثالث يجب توقيع اتفاقية عدم الافصاح، حيث تكون هناك الحاجة لفهم وتقييم إجراءات العمل لكل منهما.

الغرض

الغرض من هذه القواعد هو ضمان عملية توقيع اتفاقية عدم الافصاح لـ (جهة العمل) من قبل جميع الاطراف الثالثة الذين لديهم إمكانية الوصول إلى البيانات السرية لـ (جهة العمل) والاحتفاظ بها بشكل ملائم وموثوق.

النطاق:

تسري هذه القواعد الارشادية على (جهة العمل) وعلى جميع ا لأطراف الثالثة سواء كانوا أفراد أو شركات أو مؤسسات أو متعاقدين أو استشاريين أو متخصصين.

القواعد الإرشادية:

- ✓ يجب على جميع الأطراف الثالثة توقيع اتفاقية عدم الإفصاح كخطوة أولى في بداية عملهم مع (جهة العمل)، مع اقرارهم بفهم هذه السياسة والتزامهم بها.
- ✓ يجب على الطرف الثالث الممنوح له حق الوصول المباشر أو غير المباشر إلى البيانات أو المعلومات التي تملكها (جهة العمل) عدم الافصاح عن هذه المعلومات أو نشرها.
- ✓ تلتزم (جهة العمل) بضمان الخدمات السرية لجميع الأطراف الثالثة. فالسرية هي بين الأطراف الثالثة و (جهة العمل) وليس للموظفين الذين يقدمون خدمات معينة.
- ✓ الوثائق التي تحتو ي على معلومات شخصية بما في ذلك على سبيل المثال لا الحصر الأسماء أو العناوين أو أرقام الهاتف أو السجلات الطبية أو السجلات المالية لموظفي (جهة العمل) يجب أن تكو ن خاضعة لرقابة دقيقة ويجب عدم الإفصاح عنها أو الكشف عنها لأي أشخاص أو مصادر غير مصرح لهم بذلك.
- ✓ يجب أن تحتو ي اتفاقية عدم الإفصاح على الأقل على الآتي:
  - أسماء الأطراف المتعاقدة.
  - أي من الأطراف المتعاقدة ملزم بحماية سرية المعلومات المكشوف عنها، سواء كان الطرف المستقبل أو الطرف المفصح عنها أو كليهما (أحادي أو ثنائي)، كما يمكن أن يكو ن لاتفاقية عدم الإفصاح أكثر من طرفين، وفي هذه الحالة يجب تحديد الأطراف الملزمة بذلك.
  - تحديد ماهي المعلومات السرية في الاتفاقية.
  - مدة الالتزام بالاتفاقية بالسنوات.
  - مدة وشروط الحفاظ على سرية المعلومات بالسنوات.
  - المعلومات التي سيتم استبعادها من الاتفاقية، كالمعلومات التي تم معرفتها مسبق ا أو التي تتواجد ومتاحة للعموم، أو التي يُطّلع عليها لاحق ا من أطراف أخرى.
  - الشروط والقيود المتعلقة بطرق نقل المعلومات السرية.
  - الإجراءات التي ينبغي اتخاذها على المعلومات السرية عند نهاية الاتفاقية.
  - مسؤوليات استلام والتعامل مع المعلومات السرية:
    1. استخدام المعلومات للأغراض المتفق عليها فقط.
    2. الكشف عنها فقط للأشخاص الذين يحتاجون إلى معرفة المعلومات لأداء الاغراض المتفق عليها.

3. استخدام الجهود المناسبة (بدل العناية اللازمة أو الجهود المعقولة) للحفاظ على أمان المعلومات. غالباً ما يتم تعريف الجهود المعقولة على أنها معيار لرعاية المعلومات السرية لا تقل صرامة عن تلك التي يستخدمها المستلم للحفاظ على أمان معلوماته الخاصة.
4. التأكد من أن الاشخاص الذين تم الكشف لهم عن المعلومات يلتزمون بشروط تقييد الاستخدام وتقييد الإفصاح، وضمان حماية المعلومات.

- نوع الإفصاح المسموح به – المعلومات اللازمة للوصول للهدف المطلوب في إطار القانون.
- يجب أن يختار الطرفان القانون والقضاء المختص الذي يحكم تنفيذ الاتفاقية.

سياسة النسخ الاحتياطي

مقدمة

تفشل الأنظمة واجهزة الكمبيوتر بشكل مفاجئ وقد تفقد السجلات الحيوية والنظم ومنتجات العمل بشكل لا رجعة فيه إذا تم تخزينها فقط على تلك ا لأنظمة وأجهزة الكمبيوتر، وقد يسبب هذا الفقد نقص الإنتاجية وزيادة التكلفة، لذا وجب النسخ الاحتياطي للبيانات وهو عملية نسخ وتخزين واستعادة لبيانات الكمبيوتر والتي يمكن أن تكو ن في أي صورة ما.

يعمل النسخ الاحتياطي على ما يلي:

- ✓ توفير تخزين آمن لأصول البيانات الهامة لسير العمل في (جهة العمل)
- ✓ منع فقدان البيانات في حالة الحذف العرض ي أو تلف البيانات أو فشل النظام أو حدوث الكوارث.
- ✓ السماح باستعادة البيانات المؤرشفة في الوقت المناسب في حالة حدوث كارثة أو فشل في النظام.

الغرض من السياسة

الغرض من هذه السياسة هو توفير إطار متسق لتطبيقه على عملية النسخ الاحتياطي، بحيث تعطي هذه السياسة معلومات محددة للمساعدة في منع حدوث فقد في بيانات (جهة العمل) بضمان توفر نسخ احتياطية ومفيدة عند الحاجة إليها - سواء كان ذلك لمجرد استرداد ملف معين أو عند الحاجة إلى استرداد كامل لأنظمة التشغيل.

النطاق

تنطبق هذه السياسة على جميع البيانات المخزنة على أنظمة (جهة العمل) وعلى جميع أجهزة الكمبيوتر، سواء أجهزة الكمبيوتر المحمولة وأجهزة سطح المكتب، وعلى جميع الخوادم التي تملكها (جهة العمل) وأي أجهزة إلكترونية أخر ى تخزن البيانات.

السياسة

- ✓ تحديد البيانات الهامة

- يجب ان تحدد (جهة العمل) البيانات الأكثر أهمية لها وذلك من خلال عملية تصنيف البيانات ومن خلال مراجعة أصو ل المعلومات، حيث يجب تحديد البيانات الهامة والحرجة بحيث يمكن منحها أولوية أعلى أثناء عملية النسخ الاحتياطي.
- البيانات التي يتم نسخها احتياطياً

سيتم الاحتفاظ بنسخة احتياطية من:

1. جميع البيانات التي تقرر أنها هامة وحساسة لأعمال (جهة العمل) و/أو وظيفة الموظف.
2. جميع المعلومات المخزنة على خادم الملفات التابعة لـ (جهة العمل). وتقع على عاتق المستخدم ضمان نقل أي بيانات ذات أهمية إلى خادم الملفات.
3. جميع البيانات المخزنة على خوادم الشبكة، والتي قد تتضمن خوادم الويب وخوادم قواعد البيانات ووحدات التحكم في النطاق والجدران النارية وخوادم الوصول عن بعد.

✓ تخزين النسخ الاحتياطي

- عند التخزين في موقع (جهة العمل) يجب ان تخزن وسائط النسخ الاحتياطي في حاوية مقاومة للحريق في منطقة مؤمنة بضوابط تحكم بالدخول.
- يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع (جهة العمل)، بمسافة
- مناسبة وذلك للحماية من الحرائق أو الفيضانات أو الكوارث الإقليمية أو الكبيرة الأخر ى، للابتعاد عن أي ضر ر في حالة حدوث كارثة في الموقع الرئيسي.
- عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع يجب ضمان - وبشكل معقول- عدم تعرضها للكوارث كالسرقة أو النار كما يجب اختيار أماكن تخزين تستخدم أساليب حماية من الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي.
- يسمح بالنسخ الاحتياطي عبر الإنترنت إذا كانت الخدمة تلبي المعايير المحددة هنا.

✓ تكرار النسخ الاحتياطي

- يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.
- الآلية التي يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح، يتعين على (جهة العمل) جدولة مواعيد مناسبة لعملية النسخ الاحتياطي متسقة مع طبيعة عمل المؤسسة؛ بحيث يمكن استعادة بيانات كافية لاستمرار العمل في حالة وقوع حادث مفاجئ، ولكي يمكن تجنب عبء لا لزوم له على المستخدمين والشبكة ومسؤول النسخ الاحتياطي.

- يجب تذكير جميع الموظفين بأن ك لا منهم مسؤول بصورة شخصية عن البيانات الموجودة على أجهزة

كمبيوتر سطح المكتب أو الكمبيوتر المحمول التي في عهدتهم، ويقع على عاتقهم مسؤولية تخزين جميع البيانات المهمة الموجودة لديهم على وسائط النسخ الاحتياطي المستخدمة في (جهة العمل).

- يجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين نسخ احتياطية لها.
- يجب اختبار وتوثيق إجراءات استعادة البيانات، كما يجب أن تحدد الوثائق من هو المسؤول عن عملية

استعادة البيانات وكيف يتم تنفيذها وتحت أي ظروف يجب تنفيذها والمدة التي تستغرقها كامل العملية بد أ من الطلب وانتهاء إلى استعادة البيانات، من المهم للغاية أن تكو ن الإجراءات واضحة وموجزة بحيث لا تكون مربكة ويساء تفسيرها في وقت الأزمات من قبل القراء بخلاف مسؤول النسخ الاحتياطي.

✓ لاحتفاظ بالنسخ الاحتياطي

- يجب أن تحدد (جهة العمل) الوقت اللازم للاحتفاظ بالنسخ الاحتياطي، وما عدد النسخ المخزنة من البيانات المنسوخة احتياطيا الكافية للحد من المخاطر بكفاءة مع الحفاظ على البيانات المطلوبة.
- يجب الاحتفاظ بنسخ احتياطية وفقا لجدو ل الحفظ والتخلص من النسخ الاحتياطي، يحدد الجدو ل حالة البيانات فيما إذا كان يمكن التخلص منها أو إعادة تدويرها أو إبقاؤها في مخز ن الأرشيف.

✓ النسخ المخزنة

- النسخ المخزنة يجب ان تخزن مع وصف قصير يتضمن المعلومات التالية:

تاريخ النسخ الاحتياطي / اسم المورد / نوع طريقة النسخ الاحتياطي) كامل / تزايدي)

- يجب الاحتفاظ بسجل للحركات المادية والالكترونية لجميع النسخ الاحتياطية، يجب أن تشير الحركة المادية والالكترونية للنسخ الاحتياطية إلى:
  1. النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين.
  2. أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخر.

✓ يجب توفير النسخ المخزنة فور ورود طلب معتمد، يجب أن تتم الموافقة على طلب البيانات المخزنة من قبل شخص مخول له، يقوم بترشيحه مدير الإدارة المختصة، كما يجب أن تتضمن طلبات البيانات المخزنة ما يلي:

- تعبئة نموذج يوضح تفاصيل الطلب، بما في ذلك النسخة المطلوبة وأين ومتى يرغب مقدم الطلب في استلامها والغرض من طلب النسخة.
- الإقرار بأن النسخة الاحتياطية سيتم إرجاعها أو إتلافها فور الانتهاء من استخدامها.
- تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.

✓ يجب توفير مستو ى حماية مناسب للمعلومات المخزنة في موقع التخزين الاحتياطي وفق ا للمعايير المطبقة

في الموقع الرئيس ي، كما ينبغي ان تمتد الضوابط المطبقة على وسائط النسخ الاحتياطي في الموقع الرئيس ي لتشمل موقع التخزين الاحتياطي.

✓ اختبار عملية استعادة البيانات

- يجب أن يتم فحص والقيام بإجراءات استعادة النسخ الاحتياطية بشكل منتظم لضمان فعاليتها وللتحقق من إمكانية استكمال اجراءات عملية الاستعادة في الوقت المحدد والإبلاغ عن قدرتها على استعادة البيانات.

يجب اختبار وسائط النسخ الاحتياطي بانتظام لضمان الاعتماد عليها للاستخدام الطارئ عند الضرورة.

يجب اختبار استعادة النسخ الاحتياطي عند إجراء أي تغيير قد يؤثر على نظام النسخ الاحتياطي.

سيتم مراجعة معلومات سجل الأحداث الناتجة من كل مهمة نسخ احتياطي يوميا للأغراض التالية:

1. للتحقق من الأخطاء وتصحيحها.
2. لمراقبة مدة عملية النسخ الاحتياطي.
3. لتحسين أداء النسخ الاحتياطي حيثما أمكن ذلك.

✓ وسائط النسخ الاحتياطي

- يجب حماية وسائط النسخ الاحتياطي من الوصول غير المصرح به أو سوء الاستخدام أو العبث بها، بما في ذلك الحماية الكافية لتجنب أي ضر ر مادي ينشأ أثناء عملية نقلها أو تخزينها. لذا يجب على جميع الموظفين المسؤولين عن معالجة النسخ الاحتياطي للبيانات الآتي:
  1. أثبات هوية ذو صلة
  2. إذن تخويل ذو صلة
- عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أو الحساسة، ينبغي مراعاة ما يلي:
  1. استخدام أماكن تخزين (حاويات) آمنة.
  2. التسليم باليد.
  3. في الحالات الحرجة يتم تقسيم ما سيتم تسليمه إلى أجزاء يرسل كل جزء عبر ط ريق مختلفة عن غيره.

- يجب تدمير جميع وسائط النسخ الاحتياطية بشكل مناسب، يتم تدمير الوسائط والتخلص منها كما هو موضح أدناه:
    1. يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.
    2. يجب ان لا تحتوي الوسائط على نسخ احتياطية يمكن إعادة استخدامها (فعالة.)
    3. يجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو استرجاعها من قبل طرف غير مصرح له.
    4. يجب العمل على أن تتلف وسائط النسخ الاحتياطي ماديا بحيث لا يمكن استعادة محتوياتها قبل التخلص منها.
- أنواع معينة من وسائط النسخ الاحتياطي لها عمر وظيفي محدود، إذ أنه بعد مدة معينة من الخدمة لن يكون بالإمكان اعتبار هذه الوسائط موثوقا بها. عند وضع وسائط النسخ الاحتياطي في الخدمة يجب تسجيل التاريخ عليها، ليتم إيقافها عن الخدمة بعد أن يتجاوز وقت استخدامها مواصفات المصنع.

سياسة الأمان المادي

مقدمة

الأمان المادي هو مجموعة من الإجراءات الأمنية التي يتم تبنيها لضمان عدم وصول غير المصرح لهم إلى المواد والمعدات الخاصة بمركز البيانات، إذ يمكن أن تتألف إجراءات الأمان المادي من طيف واسع من الطرق لردع وإحباط الدخلاء بما في ذلك اللجوء لطرق تعتمد على التقنية، وسياسة الأمان المادي المطبقة بشكل جيد يمكنها حماية موارد ومعدات مركز البيانات من السرقة والعبث والكوارث الطبيعية والتخريب والهجمات السيبرانية وغيرها من الأفعال المؤذية، على كل الأشخاص أن يكونوا على وعي كامل بمحتويات هذه السياسة الأمنية وأن يتقيدوا بالأجزاء التي تشمل مجال عملهم.

الغرض

يعد تعيين وفرض الضوابط المادية والبيئية المطلوبة لحماية الأصول والأنظمة المعلوماتية من الدخول الغير مص رح به وصونها من المخاطر البيئية أمراً لا غنى عنه، وهذه السياسة تحدد متطلبات حماية مراكز البيانات من التهديدات المادية والبيئية لضمان سرية وتكامل وتوافر البيانات التي تحويها هذه المراكز.

النطاق

تصف هذه السياسة متطلبات الأمان المادي لمراكز البيانات التابع لـ(جهة العمل)، بما في ذلك مكاتب مركز عمليات الشبكة (Network Operations Center, NOC) وكل ما يتواجد بها، والسياسة تغطي العديد من المتطلبات الخاصة بالأشخاص والممتلكات، فهي تشمل كل العاملين والمتعاقدين ومهندس ي الخدمات وكل من يمثل (جهة العمل)والذين بدورهم يتوقع أن يمتثلوا ويتقيدوا بهذه المتطلبات.

السياسة

✓ بند العقار

- مخاطر الكوارث الطبيعية

يجب أن يتم اختيار موقع مركز البيانات بحيث تكون احتمالية حدوث الكوارث الطبيعية عند مستويات مقبولة، الكوارث الطبيعية تشمل على سبيل المثال لا الحصر، العواصف الرعدية والامطار الغزيرة والعواصف الرملية والفيضانات.

- مخاطر الكوارث من صنع الإنسان

يجب أن يتم اختيار موقع مركز البيانات بحيث تكون احتمالية حدوث الكوارث من صنع الإنسان أقل ما يمكن، الكوارث من صنع الإنسان تشمل على سبيل المثال لا الحصر، تحطم الطائرات وأعمال الشغب والتفجيرات والاشتباكات المسلحة والحرائق، يجب ألا يكون الموقع بجانب المطارات أو السجون أو الثكنات العسكرية أو الطر ق السريعة أو الملاعب الرياضية أو مسارات الاستعراضات.

- البنية التحتية

يجب أن يعتمد مركز البيانات على المنشآت المزودة للطاقة الكهربائية بنسبة لا تقل عن 9.99%، ولا بد أن يتم تزويد الكهرباء للموقع من محطتين (أو أكثر) فرعيتين منفصلتين ويفضل أن تتصل كل منهما بمحطات توليد منفصلة، ويجب أن يتوفر بالموقع مصدرين للمياه، كما لا بد من توفير أكثر من مزود خدمة واحد للاتصال بالشبكة.

- تفرد الغرض

يجب ألا يتشارك مركز البيانات نفس المساحة مع المكاتب الأخر ى وخاصة تلك المملوكة لمؤسسة أخرى، وفي حال الاضطرار إلى ذلك فيجب ألا يكون لهذه المكاتب جدران ملاصقة لمركز البيانات.

- محيط الموقع:

يجب أن تتواجد حراسة عند كل نقطة دخول لمركز البيانات، وهو المكان الذي يجب أن يتم ضبط دخول العاملين بمركز البيانات عبره باستخدام طريقة موثوقة للمصادقة الآلية، كما يجب ألا يتواجد أي شيء يمكن أن يعيق الرؤية من خلال كاميرات المراقبة أو من قبل حراس الدوريات في المساحات المحيطة بالمبنى والتي بد ورها يجب أن تكون مضاءة بشكل جيد، ويجب ألا يكون هناك أي لوحات أو علامات إرشادية تبين أن المكان يخص مركز البيانات أو هوية (جهة العمل) المالكة.

- المراقبة:

يجب تركيب كاميرات مراقبة (CCTV cameras) خارج مركز البيانات لمراقبة الأماكن المجاورة، كما يجب تسيير دوريات منتظمة من قبل الحراس داخل محيط (جهة العمل). وفي حالة وجود موقف للمركبات يجب أن يتم منح إذن خاص بدخوله للسيارات المملوكة للعاملين في (جهة العمل) والمتعاقدين والحراس وأطقم النظافة، وكل من عدا ذلك يجب أن يستعملوا موقف الزوار فقط، بينما المركبات التي لا تلتزم بذلك يجب سحبها خارج (جهة العمل) فور اكتشافها.

- موضع نوافذ غرف الخوادم:

يجب ألا تحتوي غرف الخوادم على نوافذ مطلة على الخارج، فهذه النوافذ تشكل خطراً بسبب إمكانية استغلالها للتنصت عن بعد ولما تسببه من دخول لحرارة زائدة للغرفة، لذا يجب أن تكون هذه الغرف في المنطقة الداخلية للمبنى بعيداً عن الجدران الخارجية، وإذا كان لا بد أن تتواجد هذه الغرف قرب حواف المبنى فيجب أن يكون هناك عازل مادي خارج جدار الغرفة يحول دون الوصول المباشر لجدران غرفة الخوادم.

- نقاط الدخول:

يجب أن تتواجد طريقة للمصادقة التلقائية عند كل نقاط الدخول بـ (جهة العمل)، كما يجب توثيق دخول المواد والمعدات وكل الأشياء التي يصطحبها الأفراد الداخلين لـ (جهة العمل) من قبل عناصر الحراسة، كما يجب متابعتها عند المغادرة مع تحديد الزمن وهوية الشخص، ولذلك يجب أن يتوفر بمقر الحراسة إمكانية الوصول لقاعدة بيانات شارات (Badges) المصادقة والتي يجب أن تحتوي على صورة لحامل الشارة، كما يجب أن تحتوي الشارة ذاتها على صورة لحاملها.

- غرف الخوادم:

1. الدخول

يجب وضع لافتات توضح أن هذه الغرف هي مناطق محظورة الدخول لغير المصرح لهم، كما يجب أن تحوي على حظر الطعام والشراب والتدخين بداخلها، ويجب أن تحتوي أبواب الغ رف على آلية للمصادقة التلقائية ،كما يجب أن تكون هذه الأبواب مقاومة للحريق، ويجب أن يكون هناك بابين فقط للغرفة، فنظراً لعدم وجود نوافذ فإن الاقتصار على باب واحد يعد تصميماً مخالفاً لمعظم ضوابط الحماية من الحرائق المعمول بها دولياً، كما يجب السماح بالدخول لغرف الخوادم فقط لمن يقوم بصيانة الحواسيب أو البنية التحتية للغرف، كما يجب أن يقتصر الدخول أثناء العطل على حالات الطوارئ فقط لا غير.

2. البنية التحتية

يجب أن تخضع غرف الخوادم للمتابعة بكاميرات المراقبة، كما يجب توفير مصادر بديلة احتياطية للطاقة وللتبريد والاتصال بالشبكة عند كل غرفة، ويجب أن تزود الغرف بأرضية مرتفعة (Raised Floor) بحوالي 46 سنتيمتر من أجل السماح بسريان الهواء وإدارة الكوابل، بالإضافة إلى وجوب أن تزود الغرف بآلية لفلترة الهواء، كذلك يجب أن يكون سقف الغرف عالياً ليسمح بتبديد الحرارة.

3. البيئة

درجة الحرارة في كل غرفة يجب أن يحافظ عليها ما بين 12 و24 درجة مئوية، كما يجب أن تبقى الرطوبة ما بين 20% و80%، ويتوجب مراقبة درجة الحرارة والرطوبة باستخدام حساسات تركب داخل الغرف وأن توثق قراءاتهما وترسل إلى مركز عمليات الشبكة (NOC)

4. الوقاية من الحرائق

يجب تزويد كل غرفة بعامل غمر شامل (Total Flooding Agent Solution)، كما يجب وضع أسطوانات إطفاء حريق مناسبة في كل غرفة، يفضل عدم استخدام أنظمة أنابيب رش لإطفاء الحرائق في غرف الخوادم.

- ✓ المر افق
  - أنظمة التبريد

يجب تركيب نظام تبريد بديل بالمنشأة، كما يجب عزل الوحدات الخارجية لنظام التبريد عن موقف المركبات الخاص بمركز البيانات.

- الطاقة

يتوجب أن تحتوي غرف الخوادم على مصدر طاقة مبني على البطاريات لديه سعة كافية لتشغيل الأجهزة إلى حين الانتقال إلى تشغيل مولدات الطاقة المعتمدة على الوقود التقليدي (بالديزل مثلاً)، في حالة عدم وجود مولد احتياطي للكهرباء فيجب أن تكون سعة البطاريات كافية للتشغيل لمدة 24 ساعة، كما يجب أن يتوفر وقود للمولد كافي لتشغيله لمدة 24 ساعة مخزنة في الموقع وأن يكون هناك تعاقد مسبق على تزويد المركز بوقود كافي للتشغيل لمدة أسبوع عند الحاجة لذلك.

- القمامة

يجب أن يتم مراقبة حاويات قمامة المنشأة بكاميرات الدوائر المغلقة، ويجب فرم وإتلاف كل المستندات التي تحتوي على معلومات حساسة بحيث لا يمكن استرجاعها قبل أن يتم التخلص منها.

- مركز عمليات الشبكة (NOC)

يجب توفير أنظمة مراقبة للحريق والطاقة والطقس ودرجة الحرارة والرطوبة بمركز عمليات الشبكة (NOC)، كما يجب أن يكون هناك طرق بديلة احتياطية ليتواصل المركز مع العالم الخارجي، كما يجب تواجد أطقم (الموظفين المختصين) في المركز

على مدار 24 ساعة طول أيام الأسبوع، ويوصي أن يقوم موظفي المركز بمتابعة وكالات الأنباء للاطلاع على أي أحداث قد يكون لها تأثير على أمان مركز البيانات.

- ✓ التعافي من الكوارث
  - خطة التعافي من الكوارث

يجب أن يكون لمركز البيانات خطة للتعافي من الكوارث، على أن تتناول إجابة على الأسئلة التالية: ما الذي يمكن اعتباره كارثة؟ من الذي يتم تنبيهه بحدوث الكارثة وكيف يتم ذلك؟ من الذي يجري تقييماً للأضرار ويقرر ماهي الموارد الاحتياطية التي يجب استخدامها؟ أين تقع المواقع الاحتياطية وما الذي يتم القيام به للحفاظ عليها وما هو الجدول الزمني الخاص بذلك؟ كم م ره وتحت أي ظروف يتم تحديث الخطة؟ إذا كانت المؤسسة لا تملك مركز البيانات، ما طول الزمن الذي يكون فيه مركز البيانات المتعاقد معه خارج الخدمة إلى حين عودته للعمل؟ يتوجب حفظ وتحديث قائمة بالأشخاص والمؤسسات التي يجب تبليغهم من قبل طاقم مركز عمليات الشبكة بما في ذلك أرقام المكتب والمنزل والنقال ومعرفات التواصل الفوري إن أمكن.

- التخزين الاحتياطي خارج الموقع

يجب إجراء نسخ احتياطي للبيانات الحساسة بشكل دوري وحفظها خارج موقع مركز البيانات، ويتوجب إصدار وتنفيذ سياسة نسخ احتياطي تحدد الخطوات الواجب اتباعها لاستعادة النسخ الاحتياطية وتحتوي جدولاً زمنيا لإجراء بروفات اختبار جاهزية خطوات النسخ الاحتياطي.

- ✓ بند ما يخص البشر
  - الغير عاملين بمركز البيانات

1. الحراس

كل الحراس يجب أن يتم التحقق من سوابقهم الجنائية قبل توظيفهم وتكرار ذلك بشكل دوري، ويجب تعريفهم على الغرض من سياسة الأمان المادي وتدريبهم على كيفية الفرض الدقيق لهذه السياسة.

2. أطقم النظافة

يجب أن يعمل أفراد النظافة في مجموعات لا تقل عن شخصين، ويجب حصر عمل طاقم النظافة على المكاتب ومركز عمليات الشبكة، في حال استدعى الأمر تواجدهم داخل غرفة الخوادم يتوجب أن يصحبهم أحد موظفي (NOC)

3. مهندسي الصيانة

يجب توثيق زمن دخول وخروج مهندس ي الصيانة للمنشأة عند مدخل المبنى، كما يجب على موظفي مركز عمليات الشبكة توثيق عملية تبادل شارات الدخول لمهندس ي الصيانة عندما يدخلون غرفة الخوادم.

4. الزوار

يجب أن يرافق الزوار الشخص الذي يزورونه طول المدة التي يقضونها بالمركز، كما يجب عدم السماح بدخول الزوار لغرفة الخوادم بدون موافقة كتابية من إدارة مركز البيانات، كما يجب على كل الزوار توقيع اتفاقية عدم افصاح قبل دخول غرف الخوادم.

5. المستخدمين

- التوعية

يجب أن يكون المستخدمين على وعي بخطر تسرب البيانات أو المعلومات بطرق احتيالية (Shoulder Surfing) وغيرها من طرق الهندسة الاجتماعية، كما يجب تدريبهم على الاحتراس من الدخلاء، ويجب أن يدربوا على تأمين حواسيبهم المكتبية والمحمولة داخل وخارج المركز والوعي بما يحيط بهم وإجراءات الطوارئ التي عليهم اتباعها عند الحاجة.

- السياسة

يجب أن يوقع كافة المستخدمين داخل مركز البيانات اتفاقية عدم افصاح، كما يجب عليهم توقيع سياسة الأمان المادي التي يقوم حراس الأمن بفرضها.

✓ التعافي من الكوارث

- الهيكل التنظيمي

يجب أن اعتماد هيكل تنظيمي مكتوب يبين مهام كل وظيفة ومسؤولياتها، ويحتوي على معلومات عن المهام الأخرى التي تم تدريب الموظف على أدائها غير تلك التي ضمن مهام وظيفته الحالية.

- توثيق مهام العمل

يجب عدم الاقتصار على توثيق ما يعرفه الموظفين حالياً على الأنظمة الموجودة، كل الأعمال الجديدة والتغييرات التي تطرأ على الأنظمة يجب أن توثق أيضاً.

- التدريب على مهام الزملاء

يجب تدريب موظفي مركز البيانات على عدد من مهام زملائهم، وهو الأمر الذي يساهم في تنفيذ بعض المهام الضرورية والحرجة عند حدوث أزمة ما، كما يضمن إنجاز العمل عند حدوث ض رف طاري لأحد الموظفين مما يسهل عملية إحلال موظف مكان الأخر.

- معلومات التواصل

يجب حفظ وتحديث بيانات التواصل الخاصة بكل موظفي مركز البيانات

- العمل عن بعد

يجب على موظفي مركز البيانات التدرب على العمل عن بعد بشكل دوري، إذ أن ذلك سيسهل إمكانية استمرار تشغيل المركز في حالة استعص ى الوصول والتواجد بالمركز لسبب ما.

سياسة تصنيف البيانات:

مقدمة:

هدفها تصنيف البيانات ع مستويات وتحديد اجراءات الحماية لكل مستوى. وتامين الحماية اللازمة للمعلومات وعدم تمكين الوصول إليها وتسريبها من غير ذوي الصلاحية، وحمايتها من أيّ محاولة تهديد خارجي،

ويشمل هذا المصطلح العديد من الأدوات والطرق والإجراءات اللازمة والواجب توفرها لتمكين الحماية من المخاطر التي من المحتمل قد تحدث من الداخل او الخارج للمنظمة,

يعتبر هذا النوع من السياسات ضرورة وشرطاً أساسياً هادف لتمكين المستخدم من فرض سيطرته على المعلومات بشكل كامل، كذلك من منع الآخرين الغير مصرح لهم من الاطلاع عليها أو إجراء أي تغيير عليها دون إذن مسبق،

أمن المعلومات هي عبارة عن سلسلة من العمليات والطرق والإجراءات يتمّ تطبيقها من قبل بعض القطاعات ومنظّمات التأمين لفرض أقوى طرق الحماية والتحكم على المعلومات الخاصة بها وعلى أنظمتها, ووسائطها لمنع تمكين الوصول إليها لغير المصرّح لهم.

تمتاز حماية المعلومات بأنها عملية وإجراءات مستمرة، أي إنها تتطلب بالضرورة إلى العمل بشكل دائم في مواكبة كل ما هو جديد ومتطور من تقنيات الامن وأساليبها في حماية ما تملكه المنظمة من معلومات حساسة، كما يجب الاستمرارية بشكل دائم بفرض الرقابة على المخاطر وافتراضها،

والسعي بشكل دوري لإيجاد حلول وابتكارات دائمة، لذلك لا يمن إطلاق النظام المعلوماتي الأمني الحقيقي على نظام أيّ من المؤسسات إلا في حال كان عملي ومحققا للاستمرارية في المواكبة للعمليات الأمنية والتقنية المتعلقة في امن وحفظ سرية المعلومات سعيا للوصول إلى أقل احتمالية من المخاطر التي من الممكن تواجه المعلومات الخاصة بها.

منع تسريب البيانات خارج المنظمة (Data Leakage Prevention -DLP)

المعلومات السرية والمهمة تشكل هاجس لدى الكثير من المسؤولين في المنظمات للبيانات التي تمتلكها إلى خارج نطاق المنظمة, ووصولها لأشخاص غير مصرح لهم الاطلاع على البيانات، خسائر كبيرة تنج عن تسرب البيانات للمنظمات هذا

سوف نركز من خلال السياسيات المتبعة على أحد مفاهيم واستراتيجيات امن المعلومات

منع تسريب البيانات أو ما يسمى (Data Leakage prevention DLP) ويطلق عليه أحياناً

(Data Loss Prevention) وكلاهما يحملان نفس المعنى من حيث المفهوم , ولكن يطل

في حال فقدان (Loss) يكون التسريب بشكل متعمد

في حال تسرب (Leakage) يكون بشكل غير متعمد ,

بالإضافة إلى أن هناك مسميات عديدة ومفاهيم متعلقة بهذا المفهوم ومنبثقة من DLP

- information leak prevention (ILP)
- Information leak detection and prevention (ILDP)
- content monitoring and filtering (CMF)
- information protection and control (IPC)
- Finger printing
- Data security and protection

(Data Leakage Prevention DLP) يمكن تعريفها على انها استراتيجية أمنية شاملة للحفاظ على البيانات المهمة من الأشخاص الغير مصرح لهم بالاطلاع عليها ومنع تداولها خارج نطاق المنظمة باختلاف أنواع البيانات وحالة ومكان هذه البيانات سواء كانت مخزنة على وحدات التخزين (In-rest) أو أجهزة المستخدمين والخوادم (In -Use) أو متنقلة من خلال الشبكة (In-motion)

اهم العوامل في حماية البيانات تكمن من خلال إن بناء استراتيجية شاملة للحفاظ على البيا نات من تداولها خارج نطاق المنظمة. يعتمد بشكل أساسي على تصنيف هذه البيانات Data Classification كذلك (Keywords policies)فتطبيق سياسات تصنيف البيانات من قبل المنظمات من حيث سرية البيانات وأهميتها ويساعد كثيراً

عند فرض القيود التقنية والحلول الأمنية المناسبة لحماية البيانات, وكمثال على تصنيف البيانات في المنظمات (عام، هام، سري، سري للغاية) فجميع البيانات بشكل عام متفاوتة الأهمية بحسب تصنيفها

هناك طرق كثيرة لتسريب البيانات منها

1. الحديث بصوت عالي في الأماكن العامة على ما تحتويه بيانات المنظمة
2. سياسة المكتب النظيف تنص على عدم ترك ملفات بالمكتب من غير توقير حماية من السرقة clean desk policy
3. ترك الأجهزة بدون تسجيل خروج أو قفل للشاشة او عدم حماية الملفات
4. الهندسة الاجتماعية وخداع الموظفين من خلال طرق الاحتيال لاستخراج المعلومات المهمة والسرية من الموظفين
5. نسخ البيانات على أجهزة التخزين المختلفة منها (USB,HD) ونقلها خارج المنظمة
6. طباعة الملفات المهمة عن طريق الأشخاص الغير مصرح لهم وعدم اتلافها أو إخراجها خارج المنظمة
7. استخدام الكاميرا المدمجة مع أجهزة الهواتف المحمولة لالتقاط صور للبيانات المهمة ويمكن من حمايتها عند تبني (Data Leakage Prevention or Watermark)
8. إرسال البيانات المهمة إلى خارج المنظمة بدون تصريح عبر البريد الإلكتروني
9. ضعف أنظمة تحكم الوصول Access Controlللتطبيقات وقواعد البيانات والتي عن طريقها يتم الوصول للبيانات المهمة
10. وصول وتمكن المخترقين من عالم الإنترنت إلى الشبكة الداخلية للمنظمة عبر الخدمات الإلكترونية المقدمة من خلال الانترنت او التصيد الالكتروني من خلال البريد

كثير من الشركات التقنية والبرمجية طرحت عدة أنظمة مخصصة لاستراتيجيات (Data Leakage Prevention DLP) وهنا سوف نكتب بشكل عام عن أبرز النقاط التي يركز عليها الكثير من المهتمين بهذا الجانب والأنظمة المخصصة لذلك والتي تشمل عدة جوانب منها التقنية والإدارية والمادية الفيزيائية وهي كالاتي:

1. أولا اهم خطوة قبل البدء في حماية البيانات يجب على المسؤولين في أي منظمة تصنيف البيانات حسب أهميتها وسريتها وذلك لاتخاذ الحماية والإجراءات المناسبة لكل تصنيف
2. بناء السياسات والبرامج الأمنية المتعلقة في بيانات المنظمة وإطلاع جميع موظفي المنظمة عليها وحثهم على التعهد على اتباعها
3. إيجاد إجراءات أمنية وتقنية للحفاظ على سرية البيانات تُتبع عند التخلص منها سواء كانت هذه البيانات تقنية أو ورقية
4. تثقيف وتوعية موظفي المنظمة بشكل دوري تجاه المخاطر التقنية المختلفة ك Phishing Email ، Malicious URLوالتي قد تساهم في تسريب البيانات خارج المنظمة
5. إيجاد أنظمة التحكم بالوصول Access Control داخل المنظمة سواء كانت على البيانات أو التطبيقات وحتى المباني لدى المنظمة يجب أن تكون متواجدة وفعالة بالقدر الذي يحمي البيانات من الوصول الغير مصرح له
6. التأكد من ان الصلاحيات الممنوحة لمستخدمي أنظمة المنظمة وتطبيقاتها تستند على وفق الحاجة Least Privileges

7. عدم السماح استخدام اجهزة المستخدمين وتعطيل أو مراقبة الأجهزة التي قد تساهم في تسريب البيانات مثل USB, CD/DVD

أنواع البيانات المستهدفة

1. البيانات عند تخزينها DATA IN REST

البيانات عند تخزينها تشير إلى البيانات المخزنة الأرشفة هذه المعلومات تكون ذات أهمية بالنسبة للشركات والحكومات ,بشكل عام بسبب زيادة احتمالية تعرضها للاختراق ق او التسرب من قبل طرف غير مصرح به عندما لا يتم استخدامها ,بشكل دوري حماية هذه المعلومات يتضمن عدة طرق مثل التحكم بالوصول، تشفير البيانات وسياسات تطبق لحفظ البيانات.

2. البيانات عند استخدامها

DATA IN USE البيانات في حال تم استخدامها تشير إلى البيانات التي يقوم المستخدم بالتعامل معها حاليا أنظمة منع فقد البيانات تقوم بحماية هذه البيانات عن طريق مراقبة وتتبعها والتدقيق عليها وتحديد إذا كان هناك اي نشاطات غير مصرح بها مثل التقاط صورة للشاشة، النسخ واللصق وغيرها من محاولات نقل بيانات حساسة سواء كانت عن عمد أم بدونه.

3. البيانات عند انتقالها DATA IN MOTION

البيانات عند انتقالها هي البيانات التي من خلا ل شبكة الاتصال حتى تصل الى جهة النهاية شبكات الاتصال قد تكون داخلية أو خارجية نظم منع تقل البيانات تحمي هذه البيانات حيث تراقب الحساسة منها والتأكد عدم تسريب البيانات بشكل غير مصرح به حتى تعبر الشبكة عبر قنوات الاتصال.