سياسة حماية البيانات  
  
أو سياسات تصنيف المعلومات:  
4# ست  
  
من الضروري أن تقوم “جهة العمل" بتصنيف أصول معلوماتها للمساعدة في إدارتها وحمابتهاء وذلك من خلال النظر في مدى  
  
إمكانية أن يُلحق ضر ب “جهة العمل" ف حالة لنشر غير المقصود أوالتعديل أو الخسارة لهذه المعلومات. ويمكن القيام بذلك  
  
عن طريق تحديد ما ينيقي حمايته وما يمكن الاطلاع عليه ومن المصتّح له بذلك من الموظفين والعامة والأطراف الأخرى  
سس  
  
تصف سياسة تصنيف المعلومات المبادئا التي يجب اتباعها لحماية المعلومات, وذلك من خلال تحديد كيف ولمن يمكنك  
  
م هذه المعلومات بتصنيف معين من أجل الحفاظ على خصوصية وسلامة وتوفر أصول المعلومات ب “جه العمل”. ومن  
خلال إنشاء هذا النظام. ستحدد هذه السياسات متطلبات التعامل مع البياثات لتوفير أساسيات حمايتها في “جهة العمل \*  
  
سب  
  
ري هذه السياسة على جميع البيانات أو المعلومات الي يتم إنشاؤها أو جمعها أوتخزينها أو معالجتها في “جهة العمل"  
سوا كانت في شكل إلكتروني أوغي إلكتروني؛ وبصرف النظر عن مكان وجود هذه اليانات أونوع الجهاز المخزنة به؛ وبلتالي  
ينبتي أن يستخدمها جميع الموظفين. والأطراف الأخرى الي تتعامل مع البياتات الي تحتفظ بها “جهة العمل” أوتخصها.  
  
نيه  
  
يجب وضع جميع البيانات في “جهة العمل" في أحد التصنيفات التالية:  
  
المستوى الأول: سرية (مقيدة) تحرف البانات السرية على أنهاعالية الحساسية؛ وبسبب الكشف عنها أو فقداتها أو  
  
,اركيوة لشخص أوأكثر أوجهة العمل ويمكن أن تشمل ما يلي:  
  
\* البيانات الشخصية للموظفين أو العملاء في جهة العمل مثل هوبة المستخدم (0 566لا والضمان.  
الاجتماعي أو أرقام الهوبة الوه  
والسجلات الطبية.  
  
تدميرهاأ.  
  
وأرقام جواز السفر وأرقام بطافات الانتمان وأرقام رخصة القيادة  
  
\* بيانات المصادقة: مثل مفاتيح التشفير الخاصة؛ واسم المستخدم وكلمة المرور  
\* لسجلات العالية: مثل أرقام الحسابات المالية.  
\*» المواد التجارية: مثل الوثائق أو البيانات الي تكون ملكية فكرية فريدة أو محددة.

\* البيانات القانونية: بم في ذلك البيانات المصرح بها للجهات القانونية فقط.  
> المستوى الثاني: حساسة (داخلية) وهي البيانات ذات المخاطر المتخفضة ونشرها أو فقدها أو تدميرها لن يكون له  
تأثيركبير على الأشخاص أو جهة العملء ولكن لا بجوز نشرها خارج جهة العمل وغالباً تشتمل على ما بلي:  
‎٠‏ اليد الإلكتروني. معظم الوسائل يمكن حذفها أو ندرها دون أن تتسبب في أحرار (باستتناء اليد لإلكتروني.  
من الأشخاص الذين يتم تحديدهم في التصنيف السري. |  
\* الوثائق والملفات الي لا تتضمن بيانات سرية.  
\*» أي بانات مصنفة على أنها غير سرية. ويمكن أن تشمل معظم بيانات الأعمال» حيث أن معظم الملفات  
الي يتم إدرتها أو استخدامها يوم يمكن تصنيفها على أنها حساسة. ومن أمئلة هذه البيانات محاضر  
الاجتماعات وخطط العمل والتقارير الداخلية للمشاريع.  
المستوى الثالث: عامة (خبر مقيدة): وي البيانات التي يمكن الكشف عنها للعامة وتشمل البيانات والملفات التي لا  
تعر حرجة بالنسبة لاحتياجات وعمليات العمل, والتى يتم نشرها عمداً لاستخدامها حيث يكون تأثيرها محايداً أو  
إيجابياً على “جهة العمل”» مثل المواد التسويقية أو الإعلاتات.  
ك الاثقام: يجب أن يلم الشراء أومن يعمل مع "جهة العمل”  
  
ثانا؛ سياسة حماية البيانات.  
  
ل اسه  
البياات في أحد الأصول الرئيسية لدى “جهة العمل" اني تتطلب إجراءات ومسؤوليات لحمايتها. وني حمايةابانات  
المصتقة بشكل مختلف في التخزين والنقل والوصول وغير ذلك لضمان عدم كشفها أونشرها أو تعديلها  
  
سن  
تتناول سياسة حماية البانات, اليانات المخزئة |لإلكترونية أو السجلات الورقية] الي تحتفظ بها “جهة العمل"؛ وكذلك  
أشخاص الذين بستخدمونها والطرق التى يتبعونها ف التعامل بها والأجهزة المستخدمة لوصول إليهاء لضمان سرية البياثات؛  
والحفاظ على معابير الجودة في حماية البيانات.  
  
كما تقوم هذه السياسة بتحديد المتطلبات والمسؤوليات الأساسية للإدارة السليمة لأصول البيانات في “جهة العمل" وتحدد  
وسائل التحامل مع البياتات ونقلها داخل “جهة العمل.”  
  
سد

تسري هذه السياسة على جميع من يقوم بالأعمال من النظم والأشخاص وطرق العملء وبشمل ذلك جميع المدراء التنفيذيين  
واللجان والإدارات والشراء والموظفين والأطراف الأخرى الذين لديهم إمكانية الوصول إلى نظم البياات أوالبيانات.  
المستخدمة لأغراض “جهة العمل  
  
© نيه  
المسؤول عن البيانات.  
1 بجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته  
مع قيمة الأصول اللي سبتوى إدارتها وحمابتها.  
2 بجب عدم تكليف موظف مسؤول رسي للبيانات اي ليس لها تصنيف أمتي وتكون ذات قيمة عملية محدودة كما  
يجب التخلص من البيانات إذا لم يكن هناك حاجة قانونية أو تشغيلية لإيقائهاء وينبني تعيين المسؤولين المؤقتين  
لهذه البيانات داخل كل إدارة لضان إتمام عملية التخلص منها.  
3. يكو منشئ المستندات الجديدة الى لها استخدام داخلى محدد على المدى القصير هو المسؤول عنهاء وهذا يشمل  
الرسائل والخطط والجداول والتقريرء كما يجب إبلاغ جميع الموظفين بمسؤوليتهم عن الوثائق الي ينشئونها.  
4 يجب تعيين مسؤول موثوق وتحديد مسؤولياته بشكل واضح اتجاه أصول البيانات اللي بتم استخدامها في “جهة.  
العمل" على نطاق واسع. وينبني أن يملك هذا الشخص القدرة على التحكم في هذه البيانات.  
تخزين البيانات.  
1. يتم تخزين جميع لبيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتاطية منتظمة.  
2. يجب عدم السماح للموظقين للوصول إلى الببانات إلا بعد أعلامهم وموافقتهم على شروط الاطلاع على البيانات الي  
سيتعاملون معها.  
3 قواعد البيانات اللي تحتوي على بياذات شخصية يكون لها إجراءات محددة لإدارتها وتأمين السجلات والوثائق.  
الكشف عن البانات.  
1 في حالة مشاركة البيانات المقيدة مع “جهة عمل\* أخرى» يجب الحرص في الكشف عن هذه البيانات وأن يتم  
بطريقة آمنة.  
2 عندمايتم الإفصاح عن البيانات أو مشاركتهاء يجب أن يتم ذلك فقط وفقاً بروتوكول مشاركة البيانات الوا  
  
اتفاقية تبلدل البيانات.  
  
3. بحظر الإفصاح عن البيانات المقيدة لأي “جهة عمل" خارجية بدون اتفاق مسبق.  
  
0 سياسة الاحتفاظ بالسجلات وإتلافها

\_  
  
تشمل السجلات جميع الوثائق والملفات التي ينتجها الموظفون في “جهة العمل ”» سواء كانت إلكترونية أو ورقية. وطرق  
  
الاحتفاظ با وأثلافها عتبر آم ثبت وهاماً في العديد من القواين التي يجب على معظم المؤسسات الامنثال لها.  
  
ن ت\_  
  
الفرض من هذه السياسة هوالتأكد من حمابة المجلات والوثا  
  
الرورية ل "جهة العمل" والحفاظ عليها وضمان التخلص  
  
من السجلات التي لم تعد مطلوبة أوالي لا قيمة لها في الوقت المتاسب.  
  
ع  
  
النطاق  
  
نري هذه السياسة على جميع السجلات الي يتم إنشاؤها في سياق عمل “جهة العمل" بما في ذلك الوثائق الأصلية  
ونسخهاء ويجب أن يمتتل جميع الموظفين لسياسات الاحتفاظ بالسجلات وإثلافها.  
  
4  
  
السياسة  
  
1 سجلات المحاسبة والمالية؛ وتشمل على:  
  
الوثائق المتعلقة بكشوف المرتبات وإجراءات المحاسبة ودفاتر الحسابات الدائتة والجداول الزمتية.  
ودفاتر الحسابات والفوتير وتقارير نفقات الموظفين. ويجب الاحتفاظ بها خمس ستوات على الأقل.  
ينبي الاحتفاظ بصفة دائمة بتقارير المراجعة السنوبة والبياتات 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)  
  
اسجلات "جهة العمل" (محاحر الاجتماعات, التكاليف الموقعة من الإد  
  
أختام “جهة العمل", أحكام  
التأسيس واللوائج. سجلات المساهمة والتقارير الستوية) والتراخيص والتصاريح ووثائق التأمين يجب أن  
تحتفظ بشكل دائم.  
  
يجوز إئلاف المستندات المعتيرة في حكم المستتدات ذات القيمة بعد اتخاذ الإجراءات اللازمة لتسجيل  
بياناتها أو ملخصها إذا مضى على استعمالها أو على إجراء آخر قيد فيها خمس سنوات إلاإذاكانت هذه  
المسنتدات محل فحص أو مراجعة أوكانت مطلوبة في دعوة قائمة أوكانت القواني واللوائح أو تعليمات.  
  
وزرة العالية تقرر الاحتفاظ بها لمدة أطول.  
  
2. الوثائق الإلكترونية:

‎٠‏ المستندات الإلكترونية: وتعمل مكتبة بامج مايكروسوفت (51:6 00660 :04161050 ؛ علفات  
.06 |والاحتفاظ يعتمد أيضا على موضوع السجلات وتصنيف بيناتا.  
\* البريد الإلكترو: يعتمد الاحتفاظ برسائل البريد الإلكتروني على محتواها فلا ينبتي الاحتفاظ بجميعهاء  
والبريد الإلكتروني الذي يتم حفظه يجب أن يكون مطبوعاً في نسخة ورقية وأن يُحتفظ به في الملف  
المتاسب أويتم تنزيله إلى ملف كمبيوتر وبتم الاحتفاظ به إلكترونيا أو على القرص كملف متفصل.  
‎٠»‏ ملفات صفحة وبب: في جميع الأجهزة في محيط العمل؛ يجب أن يتم جدولة متصفحات الإنترنت لحذف  
ملفات جمع البيانات مرة واحدة في الشهر.  
3. العلقات والمستتنات القانونية:  
يتم الاحتفاظ بالأرشيف القانوني الخاص \*بجهة العمل" بدون تحديد مدة على النحو اا  
\* ملفات الدعاوي القضاا  
  
‏وما يصدر فيها من أحكام ابتدائية ونهائية, وقرارات وأوامر المحاكم وكافة.  
الملقات ذات الصلة.  
  
‎٠»‏ المذكرات والآراء القانونية الصادرة عن المكاتب القانونية.  
  
‏\* ملفات الموظفين وما يتضمته من مسنندات تخص حياتهم والوظيفية تحفظ بشكل دائم حتى بعد إنهاء  
علاقة الموظف “بجهة العمل"  
  
‏» سجلات الإدارية الوظيفية (وتشمل سجلات الحضور والانصراف. استمارة الطليات 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 وساثر الوثالق المتعلقة بالامتحانات اللي تجربها لمدة سنتين تبدأ من تاريخ اعتماد  
تتيجة 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:  
التقاير الاستشارية.  
دليل السياسات والإجراءات [الأصلى / النسخ)  
التقازير السنوية.  
4. إجراءات أثلاف الوثائق:  
‎٠‏ يجب عدم إزلة أوأئلاف السجلات ألا أن كانت مصنفة بذلك أو عند انتهاء مدة الاحتفاظ بها.  
‎٠‏ عند الاحتفاظ بالسجلات خلال الفرة المحددة لها فى جداول الاحتفاظ» يتم إعدادها الإتلاف.  
  
‏\*» الوثالق المالية يتم إتلافها والتخلص متها وفق الإجراءات المحددة بلائحة الميرانية والحسابات والمخازن:

\*» الوثائق المالية وسجلات المتعلقة بالموظفين يتم أتلافها بوسيلة تضمن إتلاف المستندات إتلافاكياً  
  
‎٠‏ يتم التخلص من البيانات الإلكترونية المحتفظ بها في الوسائط الأخرى عن طريق الإتلاف المادي لتلك.  
الوسائط.  
  
‎٠‏ يجب أن تتم عملية أثلاف السجلات بشكل آمن وكامل.  
  
‎٠‏ يجب تسجيل عملية الإتلاف في وثيقة رسمية لأثلاف البيانات داخل “جهة العمل.”  
  
‏رابعاً؛ سياسة نش البيانات.  
ل ت\_  
توضح هذه السياسة البيانات الي يمكن نشرها داخلياً وخارجياً والأساليب الي تنشر بها هذه البيانات, كما توضح النوع المحدد  
من البيانات اللي سيتم الكشف عنها واي لا يجوز الكشف عنها.  
» بيانات لا يمكن الكشف عنها  
البيانات الشخصية؛ وتشمل سجلات الموظفين والبيانات الطبية, وبياتات عن الواتب والمزاي.  
  
‏البياثات المال  
  
‏ّ  
‏المسائل والإجراءات القانونية أو التأديبية أو محاضر التحقيق ويتم إعلان صاحب الشأن بالطرق الرسمية.  
جميع البياثات السرية.  
\* البيانات الي يتعين الكشف عنها قيما يتعلق بارتباط مع جهات عمل الأخرى  
ملخصات المدروع الأولية.  
البيانات والمعلومات الي ترى “جهة العمل" ضرورة نشرها لاستخدامها أو لأخذ العلم بها.  
سن  
الغرض من هذه السياسة ضمان حماية البيانات الشخصية والبيانات السرية من الاستخدام غير المصرح به أو كشقهاء وكذلك  
التسهيل تحديد البيانات الجائز نشرها أو الكشف عنها. وقد وضعت هذه السياسة أيضا لحمابة الملكية الفكرية ل “جهة.  
الععلد\*  
  
‏سد  
  
‏تسري هذه السياسة على جميع البيانات المنجزة والمتحصل عليها أو لبي تم جمعها وتخزيتها من قبل ".  
  
‏نيه  
  
‏\* البيانات المصنفة على أنها غير مقيدة يمكن أن تكون متاحة للعامة وجميع الموظفين وكذلك الأطراف الأخرى.

+ البيانات الي تحتاج إلى الحماية يمكن الوصول إليها عن طريق الوصول المصرح به؛ مثل الموظفين أو الشراء وفق  
مب “الحاجة إلى المعرفة" لأغراض ذات صلة بالأعمال. وينبني منح هذا التصريح لغترة 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.  
  
خامسا: سياسة الوصول للبيانات.  
  
ل ت\_  
تحدد “جهة العمل" التصنيف الأمني لأصول البيانات ويوضح هذا التصنيف نوع البياثات اللي يمكن عرضها أو الوصول إليها  
من قبل الموظفين أو الأطراف الأخرى. وكل مستوى من هذا التصنيف كالبيانات الحساسة أوالبيانات السرية يتطلب تصريح  
مختلف من الإداة العليا للوصول إليه.  
  
سس  
  
الفرض من هذه السياسة هو الحد من خطر ضياع الباذات أو الكشف عنها بشكل يؤثر على سلامة أوسرية أو وفرة أصول هذه  
لبانات, وذلك من خلال التحكم في الوصول إليها بتحديد من المصرح له بذلك ومن بستطيع استخدامها.  
له سي  
  
تسري هذه السياسة على جميع البيانات من التقارير والمسنندات وا١‏  
  
ا  
  
‎٠‏ الأقراد المصرح لهم فقط يمكتهم الوصول إلى البيانات المتوفرة بشكل كامل.  
  
‎٠‏ المستخدمين يُصتح لهم الوصول للبيانات واستخدامها عند الطلب  
  
‎٠‏ المصرح لهم فقط من الموظفين أو المجموعات أو المنظمات يمكتهم الوصول للبيانات اللازمة لإجراء العمل فقط؛  
كما أن قيمة الملكية الفكرية محمية عند استخدام هذه البياتات.  
  
‏لق التي تم إصدارها أو جمعها من قبل  
  
‏سادسا؛ سياسة الاستخدام المقبول"  
  
‏ت\_

الهدف من نشر سياسة الاستخدام المقبول لا يكمن ف فرض قيود تتارض مع لقافة النفتاح والثقة والشغاقية داخل  
ؤسسات؛ وإنما تهدف إلى حمابة اجهة العمل) وموظفيها وشائها من حدوث أي أعمال غير قانوتية أوضارة من قبل  
الآخرين سواء كان ذلك بقصد او بدون قصل  
  
الأنظمة ذات العلاقة ب (:1018601/1016308:/5::/208) بع في ذلك على سبيل المثال لا الحصر أجهزة الكمبيوتر  
والبرمجيات وأنظمة التشغيل ووسائط التخزين وحسابات الشبكات الموفرة لبريد 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 واهتماماتهاء وق التعامل مع عملاءها وزيائنها قي سياق العمليات الاعتيادية. (وفق سياسات الموارد البشرية.  
بالمؤيسة)  
  
نظام أمن وسلامة المعلومات الفقال هو جهد جماعي يتطلب مشاركة ودعم كل موظفي (جهة العمل) كل من يتعامل مع  
المعلومات والأنظمة المتعلقة بهاء وتقع على عاتق كل مستخدم للكمبيوتر مسؤولية معرفة هذه الإرشادات؛ وإجراء كل أنشطته  
وفقالها  
  
صم نديمة  
الفرض من وضع هذه السياسة هو تحديد ماهية الاستخدام المقبول لكل ما بتعلق بمعدات وأجهزة الكمبيوتر في (جهة.  
العمل). وقد ؤضعت هذه القواعد لحماية الموظف و(جهة العمل) على حد سواء؛ حيث أن الاستخدام غير المناسب تتلك.  
الممدات والأجهزة قد يعرضهما لمخاطركثيرة بما في ذلك هجمات البومجيات الخبيثة وغيرها من التهديدات المحتملة.  
  
المتعلقة بأنظمة وخدمات الشبكات وما يترتب عليها من أثار قانوتية.  
  
ل سس  
تتطبق هذه السياسة على استخدام المعلومات والأجهزة الإلكترونية وأجهزة الكمبيوتر وموارد الشبكة اللازمة لإجراء أعمال  
(اجهة العمل) أوما يتعلق بالتعامل مع الشبكات الداخلية وأنظمة الأعمال» سواء كانت مملوكة أومستأجرة من قبل (جهة  
العمل) أو الموظف أو طرف ثالث, ويتحمل الجميع مسؤولية تطبيق الممارسات الصحيحة فيما يتعلق بالاستخدام المتاسب  
للمعلومات والأجهزة اللكترونية وموارد الشبكة وفقًا لسياسات ومعايير) (جهة العمل).  
  
نيه  
  
. الاستخدام العام والملكبة.

> تمتلك (جهة العمل) البيانات المحفوظة على أجهزة الكمبيوتر والأجهزة الالكترونية الأخرى؛ المملوكة أو  
المستاجرة من قبل المؤسسة, أومن طرف ثالث؛ ويجب التأكد من خلال الوسائل القانوتية أوالتقنية أن  
معلومات الملكية محمية وفقا لمعيار حماية البيانات.  
تقع على عاتقك مسؤولية اإبلاغ عن سرقة أو فقدان أوكشف غير مصرح به عن معلومات الملكية  
المتعلقة بالمؤسسة.  
يسمح بالوصول ل إلى أواستخدام أو مشاركة معلومات الملكية فقط في حدود ماهو مصح به وحروري  
للإيقاء بمتطلبات الوظيقة الي يتم التكليف بها.  
> كل موظف مسؤول عن تطبيق مايير الاستخدام الأمن للأجهزة لإلكترونية في إطار الوظيفة؛ كل إدارة  
مسؤولة عن وضع مبادئا توجيهية بشأن الاستخدام الشخص ي الأمثل ل لأنظمة داخل المؤسسة»  
ويجب أن يسترشد الموظفون بسياسات الإدارة بشأن الاستخدام الشخص ي؛ واستشارة مشرفيهم أو  
مدراءهم.  
يجوز للأفراد المصرح لهم مراقبة المعدات والنظم وحركة الشبكة في أي وقت لأغراض الأمان وصيانة.  
الشبكة وذلك وفقًا لسياسة المرقبة وسياسة التدقيق.  
تحتفظ (جهة العمل) بحقها في التدقيق على الشبكات والآد  
2 معلومات الملكية  
كل الأجهزة المحمولة وأجهزة الكمبيوتر المملوكة للمؤسسة واي تتصل بشبكة الانتنت يجب أن تلم  
'بسياسة التحكم في الوصول.  
يجب أن تتوافق كلمات المرور للأنظمة والمستخدم مع سياسة كلمة المرون ويحظر متح إمكانية الوصول  
إلى شخص آخر عمداً أوعن طريق عدم تأمين الوصول.  
يجب تأمين جميع أجهزة الكمبيوتر باستخدام شاشة توقف محمية بكلمة مرور مع تعيين ميزة التنشيط  
التلقان إلى 10 دقائق أواقل. يجب عليك قفل الشاشة أو تسجيل الخروج عندما يكون الجهاز غير  
مراقب / غير مستخدم.  
النشر عن طريق الموظفين باستخدام البريد الالكتروق للمؤسسة يجب أن بتضمن إخلاء للمسؤولية بأن.  
رأيهم ل يمثل رأي (جهة العمل) وإنم يعبر عن وجهة نظرهم الشخصية إلا فيما يتعلق بعهام العمل.  
3. الاستخدام غير المقبول  
بشكل عام يحظر ممارسة الأنشطة تالية الذكرء وقد يتم إعفاء الموظفين من هذه القيود أثتاء القيام بمسؤولياتهم  
الوظيفية المصرح لهم بها (على سبيل المثال» قد يحتاج موظفو إدارة الأنظمة إلى تعطيل وصول الشبكة إلى  
العضيف, إذاكان ذلك المضيف يعرقل خدمات تؤلر على الإنتاج)  
  
بة دورًا لضمان الالزام بهذه السياسة.

كما لا يسمح تحت أي ظرف من الظروف لذي موظف في (جهة العمل)بالتعاطي مع أي نشاط غير فانوق بموجب  
القانون المحلى أوالدوي أثناء استخدام موارد, (جهة العمل) والقوائم أدناه لم توضع بشكل موسع بأي حال من  
الأحوال: ولكنها محاولة لوضع إطار عام للأنشطة الي تندرج تحت فئة الاستخدامات الغير مقبولة.  
  
أنشطة النظام والشبكة.  
الأنشطة التالية محظورة تمام أ؛ ويدون استئناءات:  
اننهائات حقوق أي شخص أو دركة محمية بحقوق النشر أو السر التجاري أوبراءة الاختراع أوأي ملكية.  
فكرية أخرىء أو قوانين أو لوائج ممائلة؛ بم ني ذلك على سبيل المثال لا الحصره تركيب أوتوزيع " برامج  
ليست مرخصة بشكل متاسب للاستخدام من قبل (جهة العمل)  
النسخ غير المصرح به للمواد المحمية بموجب حقوق الطبع والنشر» بما في ذلك على سبيل المثال لا  
الحصر؛ تحويل الصور الفوتوغرافية من المجلات أوالكتب أوغيرها من المصادر المحمية بحقوق النشر  
إلى صور رقمية وتوزيعهاء وأيضاً مواد الوسائط المتعددة المحمية بحقو ق النشر.. إلخ؛ وتلبيت أي برنامج  
محمي بموجب حقوق النشر والني لا تمتلك (جهة العمل) أو المستخدم له ترخيص بذلك.  
> الموظفون المصرح لهم بالوصول إلى شبكة النترنت يجب عليهم عدم استخدامها لتحميل برمجيات  
والعابءكما ينبني عليهم عدم استغلالها في اللعب ضد خصوم على شبكة الانرنت.  
الوصول إلى البيانات أو الخادم أوالحساب [لأي غرض آخر غير القيام بأعمال تخص جهة العمل؛ حى مع  
وجود تصريح بالدخول.  
انتهاك لقواين مراقبة التصدير المحلية والدولية عند القيام بتصديرالبومجيات أو المعلومات التقنية أو  
برامج أوتقنيات التشفير ويستوجب استشارة اإدارة المناسبة قبل تصدير أي مادة محل شك.  
استخدام أجهزة الكمبيوتر المملوكة للمؤسسة للاتخراط بفاعلية في.  
تقديم عروض احتيالية من المنتجات أو المناصر 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  
الوظيقة, أما تعطيل اتصالات الشبكة فيتضمن مثلا. عملية مراقيه تدفق البياتات داخل الشبكة :14600016  
  
أو نقل مواد تنتهك القانون.  
  
5011508 وعمليات حجب "الحرمان" من الخدمة]” 0005" 580168 0 020121 015111010168 (. والتلاعب  
في الحزمة البيانات) 600006 020:01 (ومعلومات التوجيه المزورة لأغراض خبيثة.  
عدم إجراء عملية فحص أمني للمنافذ 00015 إلا بعد إبلاغ مسبق للمسؤول ب (جهة العمل.).

القيام بتنفيذ آي شكل من أشكل مراقية الشبكة التق من شأتها اعتراض البيانات غير المخصصة لمضيف  
6 المستخدم ما لم يكن هذا النشاط جزةا من المهام أو الأعمال الروتينية للموظف.  
  
اجتياز عملية مصادقة المستخدم أوأمان أي مضيف أوشبكة أوحساب.  
  
> استخدام تقنيات مصائد مخترق الشبكات 1006/0015 أو أي تقنيات مشابهة فى شبكة (جهة العمل  
دون إذن  
  
> التدخل في / أو رفض الخدمة لأي مستخدم غير مضيف 4055م الموظف) على سبيل المثال: هجمة رفض  
الخدية مزه 580162 )0 و0801  
  
استخدام أي برنامج/ نص / أمره أو إرسال رسالة من أي توع» بنية التدخل في / تعطيل جلسة عمل  
مستخدم ما بأي وسيلة, في الشبكة المحلية محلياً أو غبر (10166025/0172061/507206)  
  
إفشاء معلومات عن/ قائمة بأسماء الموظفين إلى أي أطراف خارج (جهة العمل.)  
  
يجب تشفير الملقات اللي تحتوي على بيانات حساسة خاصة ب) جهة العمل (والي يتم تقلهابأي شكل  
عبر الإنترنت, كما هو محدد في سياسة أمن لبيانات الموجودة.  
  
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 بهاء حيث يساعد الاستخدام المقبول لليويد  
الإلكتروني الموظفين على استخدام عناوينالبريد لإلكتروني لإجهة العمل) بشكل صحيح كما هو محدد في  
سياسة استخدام البريد الالكتروق.  
  
للا تال الاجساي والدوين / للد رلالكتوني  
  
> التدوين أو النشر الالكتروني من قبل الموظفين سواء كان ذلك باستخدام ممتلكات وأنظمة (جهة العمل) أو  
عبر أتظمة كمبيوتر خاصة يندرج أيضاً ضمن القيود المتعلقة بهذه السياسة؛ والاستخدام المحدود في  
  
ة (جهة العمل) الانخراط في التدوين مقبول بشرط أن يكون بشكل محترف وأخلاقي  
ولا بنتهك سياسات (جهة العمل)؛ ولا يضر بمصالحها ولا بتداخل مع واجبات الوظيفة, والتدوين  
باستخدام أنظمة (جهة العمل معرض للمراقبة.  
  
سياسة سرية المعلومات ب) جهة العمل (تنطبق أيضا على التدوين, حيث يُحظر على الموظفين الكشف  
عن أي معلومات حساسة خاصة ب (جهة العمل)؛ وكذاالأمرار التجارية والمهنية أوأي مواد تحت مظلة.  
سياسة سرية المعلومات عن الاتخراط في عمليات التدوين أو النشر الالكتروني.  
  
مناسيات معينة لأه

بيجب ألا ينخرط الموظفون في أي عملية تدوين أو نشر الكتروني يمكن أن تضر أو تشوه صورة وسمعة أو  
يمس كل ما بتعلق بالرضا عن مؤسسة ماء كا يُحظر على الموظفين نشر تعليقات تدل على تميين وإحراج»  
وإهانة؛ ومضايقة أ تبن أي سلوك الكتروني من السلوكيات المحظورة.  
  
على الموظفين عدم نسب تصريحات شخصية أو آراء أو معتقدات لإجهة العمل) عند الاتخراط 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 سملا لها صراحة أوضمتيا. كما يجب على الموظف  
أن يضع في الاعتبار المخاطرة الي تتضمنها عملية التدوين /النشرالالكتروي.  
  
وبغض النظر عن أهمية اتباع جميع القواتين المتعلقة بمناولة المواد الخاضعة لحقوق الندر الخاضعة.  
للرقابة والكشف عنهاء كما لا يجو ز أيضًا استخدام العلامات التجارية والشعارات وآية ملكية فكرية أخرى  
خاصة ب (جهة العمل) فيما يتعلق بأي نشاط تدوين أو نشر الكتروني.  
  
سابعاً: سياسة كلمة السر/المروز  
  
ت\_  
  
تعتبر كلمة المرور أوكلمة السر عنصرا مهم في مجال أمن المعلومات. في تستخدم كإثيات للهوية للموافقة على الوصول وذلك  
الحماية المستخدمين وحفظ خصوصيتهم؛ ولحماية البيانات والأنظمة والشبكات. على سبيل المثال يتم استخدامها لمصادقة.  
مستخدي أنظمة التشغيل والتطبيقات مثل البريد الإلكتروني والوصول عن بعد؛ كما تستخدم أيضا لحمابة الملقات.  
والمعلومات المخزثة الأخرى. وفي ظل هذه الحاجة إلى كلمات المرور لأمو ر ذات أهمية عالية اقتض ى ذلك تركيب كلمات  
سر قوية ذات تشفير عاليء بحيث لا يمكن لأحد توقعها أو اسننتاجها.  
  
©#ه | سمننية  
الفرض من هذه السياسة هو تحديد سياسات وإجراءات كلمة السرلمرور لتقديم أفضل مستوى للخدمة مع أعلى درجات  
الحماية والخصوصية للمستخدين.  
  
ل سس

قسري هذه السياسة على جميع الموظفين في (جهة العمل) وتطبق على جميع كلمات المرور المستخدمة على كافة الأجهزة.  
وملحقاتها والخدمات المرتبطة بها والأنظمة وفى جميع التطبيقات الي تعد جزءا من شبكة (جهة العمل) ال توقر الوصول  
إلى بيانات (جهة العمل) المملوكة.  
  
# انيه  
  
فرض كلمة مرور قوية: بجب ان تكون كلمة المرور قوية ولا تتضمن في تركييها الكلمات الت يسهل على  
الاخرين إيجاده.  
» يجب استخدام توليقة من الأحرف الكبيرة والصغيرة؛ مع أرقام؛ ورموز أو علامات التوقيم قدر  
الامكان عند اختيارك لكلمة السر/المرور  
‎٠»‏ لايجب استخدام كلمات سر رائجة ولتق يمكن التكهن بها بسهولة كالأسماء وتاريخ الميلاد أو  
أرقام الهواتف.  
‎٠‏ يجب ان لا يقل عدد رمو زكمة السر/المرور عن 14 رمز  
\* لايجب استعمال اسم المستخدم ف ككمة الس  
\* لايجب استخدام أرفام | أوحروف متكررة مثل (3333 اوشظهم)  
» في حالة اختباكمة تقليدية يقضل خلط حروفها بحيث لا تعطي معي متعارف عليه.  
» يفضل ان تكون كلمة المرور "جملة مرور" لا يفهمها الا المستخدم؛ ُكونة من تركيبة الاحرف  
والأرقم والرموز  
‎٠‏ تطبيق ضوابط صارمة على كلمات المرور على مستوى النظام وكلمة مرور الحسابات المشتركة.  
يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها.  
» يجب التعامل مع جميع كلمات المرور فق (جهة العمل) على أنها بيانات سرية.  
» لا يحتفظ بكلمات المرو ركتص عادي يمكن فراءته؛ وإنم يتم حفظ كلمات السر على شكل تص  
مشفرلا يمكن فكه ا استخدامه من الشخص المخول.  
\* يجب آلا يتم تخزين كلمات المرور على أنظمة الكمبيوتر في شكل غير محي.  
\* كلمات المرور للأنظمة] جذر النظام/مسؤول النظام 0001/80011015112106 (يجب ان تخزن.  
باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.  
‎٠‏ يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وادخال البيانات في كل مرة من  
الحفاظ على سرية كلمات المرور: يجب عدم مشاركة أوكشف كلمة المرور مع أي شخص لأي سبب من  
الأسبابد

يجب عدم أفشاء كلمة المرور وعدم كتابتها بطريقة صريحة مما يجعلها عرضة للاطلاع أوحتى  
التلميح عن تركبيتهاء لاني حالة الضرورة القصوى ويجب تغيرها بعد الكشف عنها  
  
يجب أخذ الحذر من الاشخاص المتطفلين عند طباعة لكلمة السر/المرور أثناء عملية الولوج.  
يمتع إرسال كلمة المرور عبر البريد الالكتروني أو من خلال اي وسيلة عبر الانترنت.  
  
يجب تغي ركلمات المرور إذا ظهر أي مؤشر على احتمال اختراق للتظام أو لكلمة المرون  
  
يجب تغي ركلمات المرور المستخدمة للحسابات المشتركة على الفور في حالة اختراقها أ عندما  
يفاد مالكها إجهة العمل  
  
لايجب استخدام تقس كلمة المرور لحسابات المسؤولين المتعددة.  
  
يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في  
إجهة العمل  
  
يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والاجهزة داخل (جهة العمل  
والحسابات والاجهزة الاخرى خارجها.  
  
كلمات المرور الأولية [المؤقتة: بجب تغيي ركلمات المرور الأولية للمستخدمين وقرض مدة انتهاء  
لصلاحيتها لإجبار المستخدم على تغيرها.  
  
0  
  
على المستخدم تغي ركلمة المرو الأولية التي يستلمها من الجهة المختصة في أول استخدام له  
وقبل انتهاء وقت صلاحينها؛ وذلك لضمان عدم تسريب كلمة الس لمستخدمين آخرين.  
  
يجب إعطاء كلمات المرور المؤفتة للمستخدمين بطريقة آمنة؛ ينبني تجنب نقلها على ورفة  
مكشوفة (نص عادي) او عن طريق أطراف ثالثة أو رسائل بريد الإلكتروتي غير المحمية [النص  
الواضح).  
  
وضع إجراءات للتحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة أو بديلة أو مؤقتة.  
يجب على المستخدمين الإفرار باستلام كلمات المرور المؤفتة.  
  
يتطلب فحص كلمات المرور الجديدة في قوائم كلمات المرور شائعة الاستخدام أو المخترقة.  
يجب متع الولوج للأنظمة الداخلية والخاصة بعد 3 محاولات خاطئة خلال مدة زمتية لا تتجاوز 15  
  
دقيقة. ويستمر المتع لمدة أقلها 30 ‎٠‏  
  
وأكثرها قساعات.  
  
يجب على المستخدم في حالة ان يشتبه او بلاحظ وجود مشكلة أمنية أوأن 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.

امن سياسة استعمال الويد الإكتروني  
  
\_  
  
يعتب البريد الإلكتروق أداة اتصال أساسية في معظم مجالات الأعمال لسرعته وفعاليته العالية, ولأنه أصبح وسيلة معتمدة  
وتعبر عن الجهة المرسلة؛ أصبح من الضروري وضع سياسة استخدامه تقادياً للمشائل الى قد تحدث بسبب سوه الاستخدام.  
  
ل لض منائيلة  
تحديد سياسات وإجراءات التعامل بريد الالكترو من خلال البنية الأساسية لشبكة جهة العمل) وال يستهدف من  
خلالها حصول المستخدمين على أعلى درجات الحماية ولتقليل من أخرار الاختراق وضمان استخدام مهن  
  
سي  
  
تسري هذه السياسة على جميع الموظقين الذين يمكنهم استخدام البريد الالكتروي في (جهة العمل) وجميع المصنعين  
والعملاء الذين يعملون باسم (جهة العمل)ء وعلى نظام ابريدالإلكتروني المستخدم داخل (جهة العمل).  
  
ب ا  
حساب البريد الالكتروني  
  
\* يمتح كل موظف حساب بريد إلكتروني» ويجب أن يكون محدد بشكل فريد لكل مستخدم.  
  
\* عند إنشاء بريد إلكتروتي جديد للمستخدم, يجب على المستخدم تغييركلمة المرورا لأولية  
الخاصة به في تسجيل الدخول التالي. حيث يجب تكوين النظام يفرض على المستخدمين تغير  
كلمات المرور الأولية الخاصة بهم.  
  
\* بجب أن تكون كلمة مرور البريد لإلكتروني الخاصة بالمستخدم تتوافق مع سياسة كلمة المرور  
الصادرة عن (جهة العمل  
  
\* بيجب 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 اليد الواريد  
  
استخدام بريد الالكتروني  
يجب على جميع المستخدمين التقيدبما بلي عند استخدام اليد لإكتروني الخاص ب [.

يجب أن يكون استخدام البريد الإلكتروني متوافقاً مع سياسات (جهة العمل) وإجراءاتها ومع  
القوانين المحمول بها والممارسات السليمة والامتثال للقواتين المعمول بها.  
  
يجب استخدام حسابات البريد الإلكتروني ل (جهة العمل) لأعمال تتعلق ب(جهة العمل)ء حيث  
يستخدم لمساعدة الموظفين في نادية وظائفهم.  
  
ل ينبني استخدام البريد لإلكتروني 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 أوالملقات بالبريد الإلكتروني؛ فقد تكون هته  
المرفقات تابعة للآخرين. وإعادة توجيه هذه البيانات إلى مستلم آخردون الحصول على إذن  
من المرسل قد يعت انتهاا لحقوق الطبع والنشر  
  
يجب على جميع المستخدمين توعي الحذر عند فتح رسائل البريد الإلكترون والمرفقات من  
مصادر غير معروفة.  
  
يجب على جميع المستخدمين ضمان أن يكون محتوى البريد الإلكترو دقيقا وواقعيا  
وموضوعياء حيث يجب تجنب الآراء الشخصية حول الأفراد أو المؤسسات الأخرى.  
  
يجب أن يدرك المستخدمون أن رساثل اليد الإلكتروني قد تخضع للتدقيق للتأكد من أنها تبي  
متطليات هذه السياسة. يتطبق هذا على محتوى الرسائل والمرفقات والعناوين ورسائل ريد  
الإلكتروني الشخصية.  
  
تعتبر جميع الرسائل المرسلة عير نظام لبريد الإلكتروني الخاص لإجهة العمل) ملكية خاصة +  
(جهة العمل) وتشمل رسائل البريد الإلكتروي الشخصية أيضا. يجب آلا يكون 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 مراقية الرسائل الإلكتروتية دون إخطار مسبق إذارأت (جهة العمل) ذلك ضرورا. ذا وج  
دليل على أن الموظف لا يلترم بالتوجيهات المنصوص عليها في هذه السياسة؛ تحتفظ (جهة.  
العمل) بالحق في اتخاذ إجراءات تأديبييه وفق اللوائج المحمول بها.  
  
يجب انتقاءالألفاظ اللائقة وعدم كتابة أي لفظ مسيء او مهين للآخر.  
  
يجب على المستخدمين عدم الإفصاح عن كلمات المرور الخاصة بحساباتهم أوالسماح لذي  
شخص آخر باستخدام حساباتهم؛ ها يجب عدم استخدام حساب مستخدم آخر  
  
في الحالات التالية [الاستقالة, الفصل/الطرد الإيقاف) سوف يتم أعلام الموظف بأنه سيتم فقل  
  
حساب بريده الالكتروني ومنحه فرصة محددة لنسخ وأرشفة محتويات بريده.

يجب على من يتحرف على أو بلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها الاتصال على الفور  
بقسم أمن المعلومات في (جهة العمل) والابلاغ بشكل فوري.  
  
إرفاف كل رسالة بتوقيع نص ي في التهاية بحمل الاسم والوظيفة ورقم الهاتف والقسم التابع له.  
  
واسم (جهة العمل  
  
على المستخدم آخذ العلم والدراية أنه المسؤول الوحيد عما تحتويه الوسائل المرسلة من خلال  
  
حساب بريد الإلكتروني.  
  
يجب على المستخدمين ضمان إرسال رسائل البريد الإلكترون إلى المستخدمين الذين يحتاجون  
  
إلى معرفة الأمر فقط.  
  
الاستخدام الغير مقبول اليد لالكتروق  
تعد الممارسات التلية غير مقبولة عند استخدام بريد الالكترو الخاص ب (جهة العمل  
  
استخدام نظام لبريد الإلكتروني لإجهة العمل) لإنشاء أو توزيع أي رسائل مدمرة أو هجومية.  
يجب على الموظفين الذين يتلقون أي رسائل بريد إلكتروي بهذا المحتوى من أي موظف ب  
(جهة العمل) إبلاغ الأمر إلى المسؤول على الغو  
  
استخدام حساب البريد الإلكتروق لإجهة العمل) لتسجيل الدخول في أي من مواقع الشبكات  
الاجتماعية مالم يكن ذلك لأغراض العمل كما يجب الحصول على موافقة من الإدارة العليا  
ذلك  
  
استخدام هوية مزيفة في رسائل البريد الإلكتروني الخاصة ب (جهة العمل).  
  
العيث بمحتوي وعناوين الرسائل المعاد توجيهها أو مرفقاتها بدون توضيح ذلك بشكل صريح.  
إرسال رسائل بريد الكتروني غير مرغوب فيها بما في ذلك إرسال "بريد غير هام" .ااه1را )الال أو  
مواد إعلانية إلى أفراد لم يطلبوها تحديداً ك (رسائل البريد الالكتروني المزعج 588011)  
  
استخدام غير مصرح به لمعلومات البريد الالكتروي أو تزوريها.  
  
إنشاه أو إجراء تحويل ل "سلسلة رسائل 1861865 910"  
هرمية من أي نوع  
  
استخدام رسائل بريد غير مرغوب بها داخل شبكات (جهة العمل) لمزودي خدمات آخرين نيابة  
عن أو للدعاية لذي خدمة مستخدمة من قبل (جهة العمل) أو متصلة عبر شبكتها.  
  
نشر الرسائل غير ذات العلاقة بالعمل أوما شابه ذلك لعدد كبير من مجموعات الأخبار  
  
"بونزي 0002 "  
  
1605820105 أوما بس ب (50301 000/5810108)  
تغيير محتوى و|أو عناوين البيد الإلكتروني للرسائل المعاد توجيهها أو مرفقاتها دون الحصول  
  
على موافقة.

قاسم سياسة استخدام الاترنت  
ل ت\_  
  
تعر الإترنت أحد أكثر مصادر المعلومات استخداماء فهو يوفر موارد متعددة من لبيانات والأفكار والأبحاث والأخبار ويسهّل  
على المستخدمين الحصول على المعلومات والبيانات لتشجيعهم على إجراء الأبحاث وتبادل المنافع.  
  
الوصول إلى النترنث من قبل الموظفين بشكل يتعارض مع احتياجات العمل قد يؤدي إلى إساءة استخدام الموارده وهذا قد  
بعرض (جهة العمل) لمخاطر بجب معالجتها لحماية أصول المعلومات الخاصة ب (جهة العمل). بالإضافة إلى ذلك قد تواجه.  
(جهة العمل) خطر تشويه السمعة وااو التعرض لمشائل قانونية من خلال أنواع أخرى من سوء الاستخدام. يساعد اتباع  
  
سياسة استخدام الإنترنت في حماية كل من الموظف والمؤسسة من تبعات سوه استخدام الإتوذت.  
  
ل سنس  
تهدف هذه السياسة الى تحقيق الاستخدام اآمن للإنترنث وذلك بتزويد الموظفين بالقواعد والمبادالتوجيهية حول  
الاستخدام اعلالم لمعدات وشبكة (جهة العمل والاتصال بلإنرنت لضمان استخدام الموظفين للإنترنت بطريقة آمنة وأكثر  
  
فاعلية.  
  
سين  
  
تتطبق هذه السياسة على جميع مستخدي الإنترتت) الموظفين وجميع الأطراف الثالثة [الذين يتصلون بالترنت من خلال  
الكتبيوتر أو الشبكات الخاصة بإجهة العمل) والخدمات المرتبطة با.  
#ه ضيه  
استخدام الموايد  
‎٠‏ يتم الموافقة على الوصول إلى الإنترنت فقط إذا تم تحديده ضمن احتياجات العمل يتم منج  
  
اخدمات الإنترنت على أساس مسؤوليات الوظيفة الحالية للموظف.  
  
أجهزة  
  
» ستقوم إدارات (جهة العمل) بمراجعة متطلبات وصول المستخدمين إل الإترنت بشكل دوري  
الضمان استمرار احتياجهم للإنتونت.  
  
‎٠‏ بصح لمستخدي الانتنت في (جهة العمل) باستخدامها لأغراض تخص العمل وبطريقة لا  
تخالف النظمة واللوائج المعمول بها في (جهة العمل). أوبما يؤدي إلى الإضرار بها أو بسمعتها.  
  
‎٠‏ لاتكقل [جهة العمل) دقة المعلومات الي يتم الحصول عليها عن طريق الإنرنت, ذلك بقع على  
عاتق مصدر ومنتج هذه المعلومات.

\* تحتفظ (جهة العمل) بحق فرض السعة المسموح بها لاستحمال الاتصال بلإنترنت حسب ماتراة  
  
الجهة الفنية المختصة ويما بتناسب مع متطلبات كل إدارة.  
  
الاستخدام السموح  
\* التواصل بين الموظفين وغير الموظفين لأغراض العمل.  
\* ما بقوم به قبي دعم تكنولوجيا المعلومات من تتزيل لتحديئات الامج والتصحيحات.  
\*» استعراض مواقع الويب للبائمين المحتملين للحصول على معلومات عن المنتجات.  
\* مراجعة المعلومات التنظيمية أوالبياتات الفنية.  
  
‎٠‏ إجراء الابحاث  
  
‏الاستخدام الشخمي  
  
‏\* قد يعد استخدام اجهزة كمبيوتر (جهة العمل) للوصول إلى الإنترنت لأغراض شخصية؛ دون  
موافقة مدير المستخدم وقسم تكنولوجيا المعلومات؛ سبي لاتخاذ إجراءات تأديبييه حسب  
اللوائج المحمول بها.  
  
‎٠‏ يجب أن يكون جميع مستخدي الإنترنت مدركين أن شبكة [جهة العمل) تقوم بإنشاء سجل  
تدفيق ببين طلب الخدمة؛ سواء في العناوين الداخلية أو الخارجة, حيث يتم مراجعتها هذه  
السجلات بشكل دوري.  
  
‏» المستخدمون الذين يختارون تخزين أونقل المعلومات الشخصية مثل المفاتيح الخاصة أوأرقام  
بطاقات الانتمان أو الشهادات أو الاستقادة من "محافظ" الإنترنت يقومون بذلك على  
مسؤوليتهم الخاصة. (جهة العمل) ليست مسؤولة عن أي فقدان للمعلومات؛ مثل المعلومات  
المخزنة في المحفظة؛ أوآي ما قد ينتج من خسائر لاحقة للممتلكات الشخصية.  
  
‏\* المستخدم مسؤول مسؤولية كاملة عن أجهزة الكمبيوتر الخاصة به واستخدامهاء وعليه أن يكون.  
على دراية بأمن وحفظ موارد تكتولوجيا المعلومات.  
  
‏\* بيجب على المستخدمين الذين يتعرفون على أو يلاحظون وجود مشكلة أمنية فعلية أو مشتيه بهاء  
الاتصال على الفور بالقسم المختص في(جهة العمل) والابلاغ بشكل فوري.  
  
‏الاستخدام المحظور  
بمتع من بانا استخدام الانترنت أو استغلالها بطريقة تعرض شبكة (جهة العمل) للخطره أوفتح  
  
‏ثغرات أمنية في الشبكة أونشر برمجيات ضارة أوغير مشروعة.

\* لا يجوز انتحال شخصية الاخرين أوجهاز آخر.  
  
‎٠‏ بمتع استخدام اسم (جهة العمل) أوأي من أقسامها أوأي من موظفيها دون إذن كتابي رسي.  
  
‏\* يمتع العيث بالمعلومات الخاصة بموظفين آخرين أو بجهات أخرى أوالاطلاع عليها بشكل غير  
قانوني.  
  
‏\* بمتع نشر المعلومات الخاصة ب (جهة العمل) أو الخاصة بالآخرين دون إذن صريح بذلك.  
  
‏\* بمتع محاولة فك تشغير بيانات الآخرين في الأنظمة المعلوماتية بدون تصريح رسي من الجهة.  
المعنية.  
  
‏\* لا يجوز الإخلال بأي من حقوق النشر أو التأليف» أوحقوق الملكية الفكرية لذي بيانات»  
تطبيقات, برامج أومعلومات.  
  
‏\* بمتع مراقبة الاتصالات الإلكتروتية للمستخدمين الآخرين لغرض النجسس وانتهاك الخصوصية.  
  
‏\* لا يجوز استخدام الانترنت بشكل يؤثر سلبا على المستخدمين الآخرين» أو على أذاء الأجهزة  
والشبكات.  
  
‎٠‏ بمتع استخدام النترنت لذي أغراض غير فانونية أ غير شرعية. ومن الأمئلة على ذلك إيسال مواد  
عنيقة أوتهديدية أو خداعية أوإباحية أو فاحشة أوغير قانونية أوغير شرعية والذي يمكن أن  
ايتسبب في أي تهديد أوتخريب؛ أوإزعاج» أو مضابقة لأي شخص أوجهة أوأمتها السيوانية.  
  
‏\* بمتع إهدار الموارد المعلوماتية, أو إحداث أي تغير في الموارد المعلوماتية دون امتلاك صلاحية.  
تخول ذلك.  
  
‎٠‏ بمتع إنشاء موقع الكتروني أو حساب على موافع التواصل الاجتماي يمثل (جهة العمل) + أو  
إدارتا أوأي جزء منهادون إذن كنلي رسي من صاحب الصلاحية.  
  
‏\* عدم استخدام قنوات اتصال بالموارد المعلوماتية الأخرى أو الارتباط بها إلا من خلال القنوات  
المتاحة والمصرح بها رسميا من [جهة العمل)  
  
‎٠‏ يمتع استخدام الموارد المعلوماتية بشكل يؤدي إل إهدار وقث الموظف.  
  
‏\* يجب عدم استخدام الاتصال بالإنترتت الخاص ب إجهة العمل) لأغراض تجارية أوسياسية. أو  
بهدف تحقيق ريح شخص ي أوتجاري أوتسوبني.  
  
‎٠‏ يمتع إنشاء نسخ الكترونية غير مصرح بها من المسنتدات والوثئق التي تخص (جهة العمل)  
وإدااتها اولذي مواد محمية بحقوق نشر لغرض نشرها أو إرسالها عبر شبكة (جهة العمل).  
  
‏عاهر؟ سياسة أمان محطات العمل [الكمبيوتر وملحقاته)

ت\_  
  
تستخدم أجهزة الكمبيوتر وملحقاتها) طابعات, ماسحات ضولية؛ أجهزة كمبيوتر محمولة؛ الخ ( أداء العمل يوي ‎١‏  
  
بطريقة معقولة ومتناسبة مع أهداف واستراتيجيات (جهة العمل). ولتقديم أفضل مستوى للخدمة مع أعلى درجات  
  
الحماية والخصوصية للمستخدمين. وضعت "سياسة محطات العمل" لضمان استخدام مهن لمحطات العمل.  
ل رض تناسيمة  
  
تهدق هذه السياسة لحماية المستخدم ومحطات العمل من المخاطر المحتملة وآلك بتحديد سياسات وإجراءات  
  
استخدام اجهزة الكمبيوتر وملحقاتها ني (جهة العمل  
  
سين  
  
تسري هذه السياسة على جميع الموظفين والمستخدمين الذين يستحملون أجهزة الكمبيوتر وملحقاتها والخدمات  
المرتبطة بها  
  
ا  
  
> يسم للمستخدم باستعمال أجهزة الكمبيوترا١‏  
استخدام أجهزة الآخرين, أومحاولة الدخول عليها.  
  
> تقع المسؤولية الكاملة على المستخدم للاستخدام الملائم لجميع الموارد المخصصة له بما فيها من اجهزة  
الكمبيوتر وملحقاتها أو برمجيات الأجهزة.  
  
لايسمج للمستخدمين بالوصول إلى الشبكة باستخدام الحواسيب الشخصية واللوحية والهواتف الذكية. الا  
بتصريح من الادارة الفنية المختصة.  
  
بجب عدم محاولة الوصول إلى أجزاء ممتوعة الوصول من الشبكة؛ مثل نظام التشغيل الرئيس ي؛ برامج  
الآمان وغيرها دون الموافقة من الادارة المختصة.  
  
أوالي المصرح له باستعمالها. ولا يجوز  
  
بجب عدم وضع أوتنصيب أو استخدام أي برامج أوأدوات أو أجهزة قد تؤدي إلى أو تساعد على تلف البرامج  
أو الأجهزة أو مكونات النظام.  
  
يمتع تلبيت أواستخدام الأدوات الي عادة ما تستخدم لمهاجمة أنظمة الأمن أو اختراق أنظمة الكمبيوترأو  
الشبكات الأخرى (مثل كاشفات كلمات الس أو ماسحات الشبكة.. إلغ)  
  
يجب احترام الخصوصية الشخصية وحقوق الآخرين وعدم الحصول على بيانات تخص مستخدم آخره  
إضافة إل البرامج أو الملفات الأخرى من دون إذن مسبق.  
  
بطلب موافقة خاصة من قسم تقنية المعلومات قبل تنصيب أي برامج أوتركيب أجهزة خاصة على أنظمة.  
(جهة العمل

أجهزة الكمبيوتر تعتبر اعارة من (جهة العمل) لذا في للاستخدام الرسمى ل (جهة العمل) فقط ولا يجوز  
استخدامها من قبل أفرادالأسرة أو الأصدفاء تحت أي ظرف من الظروف.  
  
عند إرجاع جهاز الكمبيوتر. تحتفظ إدارة تقنية المعلومات بالحق في تنظيف القرص الثابت من أي بيانات.  
وإعادة تثبيت كافة ابرامج المبدثية. المستخدم مسؤول عن أي بيانات يتركها على الكمبيوتر المحمول عند  
إعادتها إلى (جهة العمل  
  
تحتفظ إدارة تكولوجيا المعلومات بحفها في استرجاع جميع المعدات الي تم اعارتها للمستخدمين من أجل  
إجراء تحدينات وتحسينات للبرامج, و / أواستبدال أو تحديث الأجهزة في أي وقت.  
  
لا بقوم موظفوادارة تقنية المعلومات بالدخول (080 للأجهزة الشخصية لأعمال الصيان الا بعد اخذ الاذن.  
من صاحب العلاقة مباشرة.  
  
اجهزة الكمبيوتر وملحقاتها موجودة لخدمة الموظفين والمستخدمين لأذاء الأعمال بطريقة أفضل» وعليه فإنه.  
اليس من الممكن استغلالها لأغراض شخصية.  
  
توفر إجهة العمل) مجموعة واسعة من الطابعات المتصلة بالشبكة للمساعدة في اداه اعمال (جهة العمل  
كما يُسمح بطابعات سطح المكتب الفردية؛ وسيتم دعمها من قبل قسم تقنية المعلومات.  
  
يحظر على موظقي (جهة العمل) شراء معدات الشبكات الخاصة بهم» بما في ذلك على سبيل المثال لا الحصر:  
بطاقات الشبكة المحلية والبطاقات اللاسلكية واجهزة 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 بصعب 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 ملقات لا علاقة لها بالعمل في المساحات المخصصة للموظقين 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 يسم لأي شخص من خارج (جهة العمل) باستخدام حواسيب (جهة العمل) إلا بإذن كتلى رسمي.  
  
يجب على المستخدم عدم ابطال عمل برامج مكافحة الفبروسات والبرامج الخبيثة على اجهزة كمبيوتر [جهة.  
العمل)؛ كما يجب ان يتم فحص وسائل تخزين البيانات (مثل الأقراص المضغوطة أو محركات الأقراص الثابتة  
أوذاكرة الفلاش) قبل فتح أي ملف أو برتامج.

2 العمل) لتوزيعها خارجها  
بحظ أية مواد أو برامج من اجهزة الكمبيوتر الخاصة ب (جهة العمل) لتوزيه  
يحظر على المستخدمين نسخ أبة موا  
  
دون موافقة خطية وصريه

الحادي عشر: سياسة مضاد القيروسات.  
  
نت  
العتاد البرمجي والمادي الذي يكونان معاً الشبكة الداخلية بعد مورداً أساسياً لعمل ل (جهة العمل)» فهي تعين الموظقين على  
إجراء أعمالهم البومية ولي لن يتمكنوا من تنفيذها من دون وجود هذه الأنظمة. تشكل الفيروسات خطراًكيياً على هذه  
الأنظمة, إذا يمكتها التسبب في اضطراب عملها وقد تسفر إلى فقد المعلومات أو تخرييها وفسادها مما يؤدي إلى ضر بإتتاجية.  
[جهة العلاء  
ات  
صممت هذه الوثيقة للإرشاد والتوجيه نحو العمل على التقليص من خطر الإصابة بالفيروسات وإلى ما يجب اتخاذه في حالة.  
مواجهتها.  
ع سوسس  
تنطبق هذه السياسة على:  
\* كل الموظفين طالما كانوا بستخدمون معدات (جهة العمل). للدخول على شبكة (جهة العمل). من أي مكان؛ ومن  
أي كمبيوتر وعير أي وصلة انترنت.  
\* الأشخاص الآخرين العاملين للمؤسسة والاقراد والجهات المنخرطين في أي عمل ما معها والمستعملين لمعدات  
وشبكات (جهة العمل  
أيأأحد أعطي له الحق في الدخول على شبكة (جهة العمل).  
  
بيده  
  
> مسؤوليات المستخدم  
  
\* يجب أن يستعمل فقط برنامج مضاد الفيروسات المعتمد لدى (جهة العمل). والذي بجب أن يكون متوفراً  
من خلال موقع التحميل الخاص بإجهة العمل) مثلاً: يجب تحميل وتنصيب الإصدار الحالي, كما يجب  
تحميل وتتصيب آخر التحديثات لرنامج قور توقرها.  
  
‎٠‏ يمتع فت أي ملف أو ماكرو مرفق برساا  
يجب حذف هذه الملحقات على الفور ومن ثم تأكيد الحذف بتفريع سلة المهملات.  
  
‏\* يجب مسح الوسائل المزعجة (50201 (والرسائل المتسلسلة) 60816 وغيرها من رسائل البريد الغير  
مرغوب بها وعدم إعادة إرسالها للغير  
  
‎٠‏ يمتع تحميل الملفات من مصادر غير معروفة أو مشبوهة.  
  
‏بريد الكتروني من مصدر غير معروف أو مشيوه أو غير موثوق به.

يجب تجنب المشاركة المباشرة على قرص التخزين بصلاحيات القراءة والكتابة مالم يكن هناك حاجة.  
ضرورية لذلك وتلبية لمتطلبات العمل الي لا يمكن تحقيقها بطريقة أخرى.  
يجب إجراء كشف عن الفيروسات لي وسيط تخزين متنقل قبل استخدامه.  
يتوجب حفظ تسخ احتياطية لبيانات الحساسة وإعدادات النظام بشكل دوري وتخزيتها في مكان آمن.  
يحظر على المستخدمين الخوض ف إي نشاط يستهدف به صناعة و/أوتوزيع الوامج الخبيثة] مثل  
الفيروسات والديدان واحصنة طروادة ورسائل البريدالالكترون المقخخة . .إل (داخل شبكة أوأنظمة.  
(جهة العملا  
يتوجب على المستخدمين إعلام فريق تقنية المعلومات ب (جهة العمل) في حالة اكنشاف وجود فيروس  
بأنظتهم.  
أنظمة تقنية المعلومات المصابة بونامج خبيث أو فيروس ولم يتمكن مضاد الفبروسات من معالجتها يجب  
فصلها وعزلها من شبكة (جهة العمل) إلى أن تصبح خالية من العدوى.  
إذا اكنشف المستخدم أن نظامه مصاب بعدوى ما فيجب عليه القيام بالتالى:  
«إبلاغ فريق تقتية المعلومات بإجهة العمل) على الغو  
  
إطقاء الجهاز  
  
2 ضمان ألا يستعمل الجهاز موظفين آخرين.  
  
3. أن يكون مستعدا لاطلاع فريق تقنية المعلومات على أي إجراء قام به قد يكون سيب 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.  
العملا  
  
يجب توزيع ونشر تحديثات برنامج مضاد الفيروسات عبر شبكة (جهة العمل) بشكل آلي فور وصولها من  
الشركة المصتعة وبجب ضبط الونامج ليتحقق من وجود التحديثات كل 60 دقيقة.  
  
تعريفات الفيروسات والبرامج الخبيئة يجب نشرها عبر شبكة (جهة العمل) بشكل آلى فور وصولها من  
المصنعة وبجب ضبط الونامج ليتحقق من وجود التحديثات كل 10 دقائق, كما بجب ريط جميع  
نسخ الونامج الموجودة بالأنظمة بمخدم تحميل تعريقات ثانوي بحيث إذا لم يسجل الجهاز دخوله بشبكة  
(جهة العمل) بمكته تحميل التعريفات من المخدم الثانوي.  
  
يجب ضبط برنامج مضاد الفيروسات للقيام بمسح في الوفت الحقيقي (52200108 71008 0801) وإجراء  
  
مسوحات دورية مجدولة زمتا!

‎٠»‏ يجب تفعيل ميزة المسح التلقاني عند الدخول (ع500010 00-200855) في مضاد الفبروسات لوسائط  
التخزين المحمولة.  
  
‏» مخدم مضاد الفيروسات يجب مراقبته بشكل بوي من قبل عضو معين من فريق تقنية المعلومات بإجهة.  
العمل) ومتابعة ما يصدره من تنبيهات وإنذارات» وكما بجب إحالة زي مشكلة لا يمكن حلها عن بعد عبر  
واجهة الإذارة المركزية للخادم إلى مكتب دعم تقنية المعلومات والذي بدورهم يعتبرونها حادثة وبقومون.  
بتكليف أحد الاخصائيين للتحقيق في الأمر.  
  
‏\*» إذا أصيب عدد من الأجهزة إثلاثة أو أكثر) بونامج خبيث في نفس الوقت فيتوجب إصدار تقوير في حول  
أسباب العدوى وإحالته إلى مسؤولي الأمن السيرانية باإدارة العليل  
  
‏نصف سنوي بخصوص مدى الام الجميع بتطبيق السياسة وإحالته لمسؤول الأمن  
  
‏السيواني بالإذارة العليا ومدير فرع بإجهة العمل) إن وجد وإلى فريق التخطيط الاستراتيجي لتقتية المعلومات  
  
‏في موعد محدد  
  
‏\* يتوجب إصنار  
  
‏\* يجب وضع آلية لمتع التلاعب بإعدادات وضبط برتامج مضادالفبروسات من قبل المستخدمين.  
  
‏\* في حالة اشتيه المستخدم في وجود فبروس بجهاه وقام بالتليغ عنه لمكتب دعم تقنية المعلومات» قعل  
فريق تقنيةالمملومات القيام بالثالي؛  
  
‏الكشف على الجهاز وأي وسائط تخزين ملحقه به  
  
‏إعادة ضبط الجهازني حالة كانت الإصابة حرجة برمجية القديةالخبيثة مثلاً.  
  
‏الكشف على أي خادم قد يكون اتصل به الجهازالمصاب.  
  
‏محاولة معرفة مصدر العدوى.  
  
‏ضمان توثيق الحادثة.  
  
‏سياسات حماية الشبكات  
أو سياسة جهاز التوجيه ومبدل (541400 200 00486) الشبكة.  
  
‏عا يعس  
  
‏لا توجد الية معينة لحمابة الشبكة, لأن أي نظام أمني يمكن أن يتعرض للتخريب والاختراق, إن لم يكن من الخارج ,فإنه  
  
‏المؤكد أن من الداخل, ف نهاية المطاف لتأمين شبكة يجب تنفيذ طبقات مختلفة من الأمن, بحيث بجب على المهاجم

اختراق تظامين أوأكثر للوصول إلى الأصول الهامة, الخطوة الأول في تطبيقات السياسيات هي تحديد السياسيات التي سيتم  
تنفيذها, وغالبا ما تفي التدايرالأمنية اأفراد في ممارساتهم التشيلية, مما بدي إلى تعزيراللوائج الأمنية بلذار تحكم  
سياسات الشبكة, كيفية تنفيذ الشبكة وتهينتها لتبسيط عمل الموظف في الظروف العادية بوكذلك إرشادات كيفية لتفاعل  
أو التعامل أثناء حدوث الحوادث في هذا السياق , يشرح القسم التلي فرض مقاييس السياسات لكل مصطلح أو مبدا من  
  
الشبكة لحماية المعلومات والنظم.  
  
سياسات جها التوجيه ومبدل :500 800 800066) الشبكة  
توف أجهزة التوجيه ومبدلات الشبكة وظائف أمان مهمة داخل الشبكة إذا ماتم تهيتها بشكل صحيح؛ فهما  
من العديد هن الأجهزة لامج التوفرة والي تساعد ف إدارة وحمابة الشبكة الخاصة من الشبكة العامة  
  
تحدد سياسة أمن الموجه ومبدل الشبكة متطلبات التهيئة لتلبية معايير الأمان ومتطلبات إدارة التغير  
والمتطلبات التشغيلية.  
  
نت  
  
هذه الوثيقة مصممة لحمابة معدات وبيانات (جهة العمل) وشرائها التجاريين أوآي بيانات مملكة أوتحث  
تصرف (جهة العمل) من خلال تحديد الحد الأدق لمعايير التكوين والضبط لجميع أجهزة التوجيه والمبدلات.  
الي تتصل بشبكة إجهة العمل  
  
للا سند  
  
يجب على جميع الموظفين والمتعاقدين والمستشارين والعاملين المؤفتين وغيرهم ممن يستخدمون أجهزة  
الشبكة مثل الموجه و/ أو المبدل لازام بهذه السياسة, كما تخضع لهذه السياسة جميع أجهزة التوجيه  
والمبدلات المتصلة بالشبكة  
  
له نيد  
  
يجب أن يستوق كل جهاز توجيه / مبدل معاي التهيئة الالية:  
  
» لايتم تكوين أي حسابات مستخدمين محليين على جهاز التوجيه و/ أو التبديل تفسه» بل  
يجب ان تستخدم أجهزة التوجيه والمبدلات خادم هرثم مخصص لهذا الغرض مثل  
(+18685) للقيام بجميع مصادقات المستخدب  
  
\* يجب استخدام كلمة السر (56661 02818ع) بدلا من تمكين كلمة المرور ( 803018  
مسيم  
  
\* يجب الحفاظ على كلمة السر (56681 0028018) مشفرة ومؤمتة على جهاز التوجيه أوالمبدل.

\* يجب تعطيل الخدمات أوالميات التالية:  
البث الموجه عبر بروتوكول الاترنيت (515ة0200: 8:80:00 ©) يمكن تفعيل  
البث الموجه نحو بروتوكول الانترتيت عند الرغبة في تتفيذ خدمات الإدارة عن بعد  
مثل النسخ الاحتياطية على الأجهزة المضيفة في شبكة فرعية ليس لها اتصال مباشر  
بالأترنيت  
  
2. الحزم الواردة لجهاز التوجيه/التبديل والقادمة من مصادر ذات عناوين غير صالحة  
مصل عناوين 8621918  
  
3 خدمات 160 الصغيرة (م6امةة القاصة (16)  
4 خدمات 08لا الصغيرة (580:1685 0011 008)  
5 جميع خدمات الويب الي تعمل على جهاز التوجيه  
التكوين التطقاني (1600ة 0012 مالم  
  
7. بروتوكول استكشاف الأجهزة للطبقة الثانية مثل (11088608) وبرتوكولات  
الاكتشاف الأخرى.  
  
\* بجب عدم سماح مايلي على واجهة منافذ أجهزة التوجيه/ التبدبل:  
ثيابة عن (وكيل) بروتوكول حل العناوين (88-/000:0).  
2 رسائل (16108 الغير قابلة للوصول  
3 التبديل السريع (ع94116010 :25ع) والتبديل الذاي (ع58116510 5ل2010000101)  
4 التخزين المؤفت للمسار متهدد البث 14015254  
  
5 بروتوكول عمليات الصيانة (1408)  
  
\* يجب ضبط الخدمات التالية:  
1 تشفيركمة المرور  
2 مزامنة الوقت (1017) يجب مزامنة جميع ساعات الشبكة من مصدر زمن مشترك  
  
‎٠‏ جميع تحديئات التوجيه (80101108) يجب أن تتم باستخدام تحدينات التوجيه الامن.

استخدام نصوص 500108 الموحدة ل (جهة العمل) يجب إزلة النصوص الافتراضية؛ مثل  
العامة أوالخاصة (01/916 :8 ع208) يجب تهيئة 50418 لاستخدام النسخة الأكثر آماناً  
من الوتوكول المدعومة من كلال الطرفين , الجهاز وأنظمة الإدارة.  
  
يجب استخدام قوائم التحكم في الوصول [515اا 6001/0 860855) للحد من مصدر ونوع  
حركة المرور التي يمكن ان تصل للجهاز نفسه.  
  
بجب أن يحتوي كل جهاز توجيه (00008») على اشعار تنبيه يظهر في تافذة أوأوا الدخول  
للنظام يحوي عل معلومات تفيد بأن الدخول هنا مسموح به للمستخدمين المصرح لهم بذلك.  
فقط لاغ البيان التالي يجب أن يظهر عند استخدام أي شكل من أشكال تسجيل الدخول  
سواء كانت محلية اوعند بعد  
  
\* بحظر الدخول لهذا الجهاز غير المصرح لهم.  
  
يجب أن يكون لدبك إذن صريح للدخول الى هذا الجهاز او ضبطه. أي إجراء أوتغيير تقوم به  
يكون عرضة للتوثيق والحفظ إذا ما رتكبت 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 تلقاية على مراقبة ما تقوم به  
  
لا يجوز أبدا استخدام بروتوكول 781061 عبر أي شبكة لغدارة جهاز توجيه؛ مالم يكن هناك  
  
نفق آمن يحمي مسار الاتصال بالكامل, الإصدار من بروتوكول (5581) هو بروتوكول الإدارة  
  
المفضل  
  
ينبني وضع أجهزةالتوجيه والمبدلات في مكان يقتصر فيه الدخول على الأشخاص المرخص  
  
مم  
  
يجب أن يقوم المبدل بتعطيل منفذ أو مجموعة من المنافذ فى حالة ظهر بها عناوين أجهزة  
  
(1406) جديدة ا خير مسجلة مسبقاً على المنفذ ذاكانت هذه الميزة متاحة.  
  
بجب ان يقوم المبدل بتوليد رسائل (7080 501048) إذا وقع الاتصال وتم إعادة توليده في  
  
حال تواقرت هذه العيزة  
  
يجب ان تستخدم بروتوكولات التوجيه الديناميكية المصادقة عند إرسال تحديئات التوجيه  
  
على الأجهزة المجاورة (يجب تمكين ميزة تحويل كلمة المرور بدالة الخال (ع15010] في  
  
نص المصادقة عند دعمها.  
  
من خلال المعيار المعتمد لدى (جهة العمل) يتم تحديد فئة من الأجهزة تتبر ذات وضع  
  
حساس تظراآلطبيعة عملهاء وبذلك فإتها تحتاج إلى خدمات وضبط إضافي والذي يجب أن  
  
يشمل:  
  
متابعة راقية لقوائم التحكم في الوصول لبرتوكول الاترنيت ( :كنا 18466245  
  
(والصاممم  
  
2 تسجيل وتوثيق أحدا الجهاز (2102عما ©08016)

3  
  
يجب إسقاط الحزم الواردة للموجه التى يكون مصدرها من عناوين غير صالحة, مثل  
عناوين 0661918 أوتلك الي يمكن استخدامها لخداع 50000 حركة مرور  
الشبكة  
  
\* يجب توثيق عمليات ضيط الشبكة والتغيرات الى تتم عليها بشكل منتظم وذلك لقهم بنيتها  
'بجب أن بتضمن مستند توثيق الشبكات ما بلي:  
  
1  
2  
3  
  
ثانيا: سياسة الاتصالات اللاسلكية:  
  
له مس  
  
رسم تخطيطي للشبكة.  
  
ضوابط النظام 660581061500 51870رع)  
فواعدالجدار لناري  
  
عناوين برتوكولات الترنيت (85 280155 18)  
  
قوائم التحكم في الوصول  
  
مع الانتشار المتسارع للهواتف الذكية والأجهزة اللوحية, فإن الاتصال اللاسلق أصبح واسع الاتنشار وهو ما أصيح أمراًمسلماً  
به ولا تخلومن أي مؤسسة؛ يمكن الضبط اللاسل الغي الآمن توفير باب مفتوح وسهل للمخترقين والقراصنة.  
  
نعد سياسات الاتصالات اللاسلكية صرورية لأمن الكمبيوتر نظ لوجود طلب مترايد على المعدات اللاسلكية في كل (جهة.  
عمل) اليوم. قد تحدد سياسة الاتصال اللاسلق انه لا يجب استخدام أي معدات لاسلكية لذلك ان يكون عملياً وواقعاً لأن  
ذلك قد يؤدي للجوء بعض الإدارات على انتهاك لهذه السياسة؛ لذلك كان من الأفضل تحديد الشروط وتحديد المعدات  
المعتمدة للاستخدام اللاسلك لتقليل مخاطر الأمان المرتبطة باللاسلك الذي لابد منه.  
  
8# سب  
  
الغرض من هذه السياسة هو تامين وحماية أصول المعلومات الى تملكها (جهة العمل). تمتج (جهة العمل) الوصول  
الى هذه المواد كامتياز ويجب أن تدار هذه الموارد بطريقة مسؤولة للحفاظ على سرية ونزاهة وتوافر جميع الأصول  
  
المعلوء  
  
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 متحها استثناء من قبل إدارة امن المعلومات للاتصال بشبكة (جهة العمل).  
  
له ست  
  
تتطبق هذه السياسة على جميع أجهزة البنبة التحتية اللاسلكية المتصلة بشبكة (جهة العمل) أو تكون موجودة  
ضمن (جهة العمل) والتى توفر اتصالاً لاسلكياً بأجهزة طرفية بما في ذلك على سبيل المثالء أجهزة الكمبيوتر  
المحمولة وأجهزة سطح المكتب والهواتف الوبة والأجهزة اللوحية. وبشكل في ذلك أي شكل من أشكال أجهزة  
الاتصال اللاسلق القادر على نقل حزم لبيانات, لذلك يجب ان يلتم بهذه السياسة جميع الموظفين والاستشارين  
والعاملين المؤقنين وغيرهم في (جهة العمل)؛ كما تشمل جميع الموظفين التابعين لأطراف ثالثة والموكل لها إدارة.  
أجهزة البنية التحتية اللاسلكية لناب عن ( جهة العمل ).  
  
جميع أجهزةالبنية التحتية اللاسلكية الموجودة في موقع (جهة العمل) والمتصلة بشبكتهاء أوالي توفر  
الوصول إلى معلومات مصنفة على أنها سرية بجب عليها ما بلى:  
+ الالام بالمعابير المحددة في معيار الاتصالات اللاسلكية  
» استخدام برتوكولات المصادقة والبنية التحنية المعتمدة من قبل (جهة عمل)  
\* استخدام برتوكولات التشفير المعتمدة لدى [جهة العمل)  
‎٠‏ الحفاظ على العناوين المادية للأجهزة (1//46) اللي يمكن تسجيلها وتتبعها.  
للحد من احتمال إساءة استخدام الشبكة اللاسلكية.  
  
\* بنبي ان تكون هنالك مصادقة سليمة للمستخدم مع الاستبدال المناسب لآلية 14/88 وتيع  
الشذوذ (ع12000 /2000031) على الشبكة المحلية اللاسلكية.  
  
\* في تقس الوقت القائم لثالية تحوي على عددا من الأحداث المشيوهة الي قد تقع داخل  
الشكة المحلية اللاسلكية والي ينبني دائما أن تأخذ في عين الاعتبار عند ضبط أنظمة كشف  
الملل

1. إطارات الإرشاد (830165م 800600 القادمة من نقطة وصول لاسلكية لم يطلب منها  
  
ذلك (ممتتافيمن)  
2 فيضان الأطر غير المصادق عليها هجوم (10171)  
3. اطربانات تحوي عنوان 1486 مكرر  
  
4 تغيير عنوان 1486 بشكل عشواني  
  
بروتكولات التشفير اللاسلكية:  
  
يفضل استخدام برونوكول حماية الوصول للواي فاي الإصدار 2 (10/82) كبرتوكول تشغير للشبكات  
اللاسلكية بدلً من بروتوكول حماية الوصول للواي فاي الإصدار الأول (10/80) وبرتوكول الخصوصية  
المكافئة للشبكات السلكية (0089) وذلك لأنه يوفر خوارزمية أمان أقوى وتشغيرا متقدماكما بتحقق من  
  
صحة الرسالة وتكامله.  
بجب توثيق عمليات ضبط الشبكة والتغيرات الي تتم عليها بشكل منتظم وذلك لفهم بنيتهاء يجب أن  
يتضمن مسقند توثيق الشبكات ما بلي:  
  
1  
  
2  
  
3  
  
رسم تخطيطي للشبكة  
  
ضوابط النظام (00 600121021 60كر6)  
قواعد الجدار اناري  
  
عناوين برنوكولات الأتزنيت (5565ة:208 18  
  
قوائم التحكم ق الوصول  
  
ثالث سياسة الشبكة الافتراضية الخاصة (014/).  
  
له مسد  
  
الشبكة الخاصة الظاهرية (810/) هي شبكة اتصال خاصة وآمنة توفر طريقة ملائمة للوصول الة موارد الشبكة.  
  
الداخلية عن بعد عبر الشبكة العامة [الانرنيت]ء حيث توفر 1/81 وصولاًآمنامن خلال توفي وسيلة لحمابة  
  
البيانات أثناء انتقالها عير شبكة غير موثوق بها.

ع  
  
الفرض:  
  
تهدف هذه لسياسة إلى توفير إرشادات خاصة باتصالات الوصول عن بعد عبر 8566 أ, شبكة 1218 الخاصة.  
الافتراضية (1/810 إلى شبكة (جهة العمل).  
  
ع  
  
التطاق:  
  
تتطبق هذه السياسة على جميع موظفي (جهة العمل) والمقاولين والمستشارين والموظفين المؤقتين وغيرهم من  
العمال با في ذلك جميع الموظفين المنتسيين إلى أطراف ثالثة المستخدمين لشبكات 1/000 ليتمكتوا من الدخول إلى  
الشبكة (جهة العمل).  
  
تتطبق هذه السياسة على تطبيقات 801/ التي يتم توجيهها للمرور عبر مركز ©856! (6008001/3000 18562)  
  
ع  
  
السياسة؛  
  
على عاتق الموظفين الذي لديهم امتيازات استخدام الشبكة الافتراضية الخاصة 1/804 ضمان عدم  
السماح للمستخدمين غير المصرح لهم بالوصول إلى الشبكات الداخلية ل (جهة العمل) عبر وصلات ال  
(810/) الخاصة بهم.  
  
يجب التحكم في استخدام الشبكة الافتراضية الخاصة 1/801 باستخدام مصادقة بكلمة المرور لمرة واحذ  
(8255003 1116 008) كجهاز إشارة السماح (06:408 10680) أو نظام المقتاح العام / الخاص مع  
  
اختيار غيارة مرور قوية (02550011358)  
  
عندما يكون الاتصال بشبكة (جهة العمل) ند  
وم يإجبار كل حركة المرور من وإلى الكمبيوتر عبر تف 1/800 بينما يقوم بطرح وتجاهل أي حركة بيانات.  
  
فإن آلية الشبكات الافتراضية الخاصة (000/) يجب ان  
  
أخرى.  
  
تقاسم أو ازدواج الاتصال عبر نقق التشغير (710006108 50188 00091) غير مسموح؛ إذلا يسمح بحصول  
أكثر من اتصال شبك واحد فقط في نفس الوقث»  
  
تقاسم أوازدواج الاتصال عبر نفق التشفير يسمح بوجود اتصالين نشطين متزامنين في نفس الوقت, احدهما  
الشبكة آمنة عبر (1/010) ولثاني لشبكة غير آمنة, هذا الوضع بشكل ثغرة تسهل الاتصال المباشر من  
الانرنيت الغير آمن إلى الشبكة المؤمنة بإتصال بتقنية 1/81  
  
بوابات الشبكات الافتراضية الخاصة (89:6»25 1001) يتم اعدادها وإدارتها من قبل موظنى القسم  
الخاص بعمليات الشبكة لإجهة العمل

يتوجب على كل الأجهزة التق تتصل بالشبكة الداخلية لإجهة العمل) باستخدام (800/) أوغيرها من  
التقتيات ان تستخدم برامج مضاد للفيروسات محدثة ومطابقة للمعايير من قبل (جهة العمل)؛ بما في ذلك  
الحواسيب الشخصية.  
  
بجب فصل مستخدي 001 تلقائيا عن شبكة (جهة العمل) بعد ثلاثين دقيقة من عدم النشاط. ويج على  
المستخدم تسجيل الدخول مرة أخرى لإعادة الاتصال بالشبكة.  
\* يمنع استخدام 81086 او عمليات شبكة مصطنمة أخرى للحفاظ على الاتصال مفتوحا”  
  
يجب ضبط جهاز (6000001/2:06 1/801) بتحديد وقت أي اتصال بحيث لا يتجاوز الأريع وعشرين  
  
ساعة  
بجب على مستخدي أجهزة الكمبيوتر اللي ليست من الأجهزة التي تملكها [جهة العمل) تهيئة الأجهزة  
بحيث تتوافق مع سياسات الشبكة وسياسات الربط بتقنية الشبكة الافتراضية الخاصة (1/81ل (جهة.  
العمل  
باستخدام تكنولوجيا 1/80 مع الأجهزة الشخصية؛ يجب أن بي المستخدمون أن اجهزتهم أصبحت  
امتدادا فعلياً وجزه من شبكة (جهة العمل)؛ وبلتالي فعي تخضع لنفس القواعد واللوائج الي تتطبق على  
المعدات اللي تستخدمها جهة العمل.  
بجب توثيق عمليات ضبط الشبكة والتغييرات الي تتم عليها بشكل منتظم وذلك لفهم بنيتهاء يجب أن  
يتضمن مستند توثيق الشبكات ما بلي:  
1 رسم تخطيطي للشبكة  
2 ضوابط النظام (600180/2000 51800ر)  
3 قواعد الجدار اناري  
4 عناوين برتوكولات الأنترنيت (5565ة:200 8  
  
5. قوائم التحكم في الوصول  
  
رابعاً: سياسة جدار الحماية/الناري (620311).  
  
يي

الاتصال بشبكة مفتوحة وغير آمنة مث الانترنيت يؤدي الى احتمالية فت مدخلاًكيماًللهجمات السيوانية على الشبكة  
الداخلية لإجهة العمل). أحد أفضل الطرق للدفاع ضد هذه الهجمات هي استخدام الجدران لتارية عند نقطة الاتصال بشبكة  
الانتنيت؛ حيث أنه من الضروري حماية الشبكات الخاصة الداخلية ومرافق الاتصالات الخاصة ب (جهة العمل  
  
ل سن  
يتم تعريف جدران الحماية [الجدار الناري) على أنها أنظمة أمان تتحكم وتقيد اتصال الشبكة وخدماتهاء جدران الحمابة تنش  
نقطة تحكم يمكن عبرها فرض عناصر التحكم بالوصول. بسعة هذا المستند إلى مساعدة (جهة العمل) فى فهم قدرات تقتيات.  
جدار الحماية وسياسات الجدارالناري.  
  
لله ست  
تحدد هذه السياسة القواعد الأساسية المتعلقة بإارة وصيانة الجدران النارية؛ وتنطبق على جميع الجدران الناية الى تملكها  
أو تؤجرها أوتتحكم بها (جهة العمل)  
  
ا  
  
مراجعة مجموعة القواعد للتأكد من اتباعها لترتبب كالتلي:  
\* مرشحات مكافحة الانتحال (حجب العناوين الخاصرة والعناوين الداخلية التي تظهر من الخارج)  
  
\* قواعد تصريح المستخدم (على سبيل المثال السماح ب 4178 إلى خادم الوبب العام).  
  
\* قواعد تصريح الإدارة (مثل رسائل تنبيه (285) /5101) 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 بعمل بالتيابة (وكيل)  
81:62 /8)0«0 1625005م4) ما بين المستخدم المتصل عن بعد والخادم المخصص  
ولذلك لإخفاء هوية الخادم.  
  
\* التأكد من مراقية المسؤولين لآية محاولات لانتهاك سياسة الأمن باستخدام سجلات التدقيق الي  
تم انشاؤها بواسطة جدار الحماية على مستوى التطبيق.  
  
» ضمان أن هنالك آلية لتحديث وسد لغرات الجدار الناري على مستوى التطبيقات والتحقق بأنها  
محدئة لسد آخر الثفرات.  
  
تاكد من وجود عملية لتحديث البرنامج بأحدث بصمات الهجوم.  
  
\* في حال زيل التواقيع من موقع الموردين والشركات المصنعة, يجب التأكد من انها من موقع  
  
مولوق.

\* في حال إرسال البصمات بالبريد الالكتروني إلى مسؤول النظام يجب التأكد من استخدام  
التوقيعات الرفمية للتحقق من المورد وان المعلومات المنقولة لم يتم تغيوها أاءالنقل.  
‎٠‏ يجب حظر الأوامرالتالية ل (58478) في جدار الحماية على مستوى التطبيق:  
001 (التوسيع - 6:0000)  
ما (تحقق -/00606  
6نف  
معقتا  
‎٠‏ يجب حظرالامرالتالي !1ع  
د كام  
  
مراجعة وحظر العناوين (815ل) والتأكد بانها ملائمة, فعلة سبيل المثالء يجب حظر أي عنوان  
8لا لمواقع المخترقين.  
  
\* التأكد من أن المستخدمين المخولين هم فقط من يتم التصديق عليهم بواسطة جدار الحماية.  
على مستوى التطبيق.  
  
تفحص بحالة الاتصال (5:218001105080000)  
  
\* مراجعة جداول الحالة (و816ة7 5:206) للتأكد من إعداد القواعد المناسبة من حيث عتاوين  
المصدر والوجهة ومنافذ المصدر والوجهة والمهلة.  
  
تأكد من أن المهلة مناسبة حتى لا تعطي المتسلل الكثير من الوقع لشن هجوم تاجح  
  
بالنسية لعناوين 1081  
  
\* في حال استخدام خادم نصفية عناوين 081ا: تأكد من تحديده بشكل مناسب في برنامج جدار  
الحماية. (إذ كان خادم التصقية من خارج (جهة العمل)ء فتأكد من أنه من مصدر موثوق به)  
  
\*» إذاكان الترشيح على عناوين ©14:امسموح به فيجب مراجعة المرشحات للتأكد من انها مقتصرة  
على عناوين 1/186 المناسبة ل [جهة العمل).  
  
تسجيل الأحداث:  
  
\* تاكد من تفعيل خاصية تسجيل الاحداث وان يتم مراجعة السجلات لتحديد أي أنماط محتملة  
قد نشي الى وجود هجوم.  
  
\* سجلات إدارة جدار حماية الشبكة [الأنشطة الإدارية] وسجلات الأحداث إنشاط حركة المرور)  
يجب انا  
  
1. يتم تخزينها على وحدة تخزين بديلة (ليس على نفس الجهاز)  
2. تتم مراجعتها يومياً على الأقلء مع الاحتفاظ بالسجلات لمدة تسعين يوماً

0  
  
التصحيحيات والتحديثات:  
  
‎٠‏ تأكد من اختبار وتثبيت أحدث التصحيحات والتحديثات المتعلقة بجدار الحماية الخاصة بك  
  
‏\* إذا تم تنزيل التصحيحات والتحديئات تلقائاً من مواقع الويب الخاصة بالموردين, فتأكد من  
استلام التحديث من موقع مولوق به  
  
‏\* في حال إرسال التصحيحات والتحديئات بالبريد الالكتروني غلة مدير النظام» تأكد من استخدام  
التوقيعات الرقمية للتحقق من المورد (1/60800) والتأكد من عدم تعديل المعلومات في الطريق.  
  
‏تقييم / اختبار الضعف  
  
‏\* بجب التحقق ما إذاكان هناك إجراء لاختبا المنافذ المفتوحة باستخدام (100488)» وما إذاكانت  
المنافذ غير الضرورية مغلقة.  
  
‏\*» التأكد من وجود إجراء لاختبار القواعد عند تأسيسها اوتغبيرها حى لا يؤدي إلى رفض الخدمة او  
السماح باستمرار وجود نقاط ضعف دون أن يتم اكتشافها.  
  
‏الالزام بسياسة الأمن:  
  
‏\* تأكد من أن القواعد تتوافق مع سياسة أمن (جهة العمل).  
  
‏تأكد من أن المناوين التالية الخاصة. (1918 ©86) المنتحلة والعشوائية محظورة:  
  
‎)8621918( ‏عناوين خاصة‎ ٠  
10255 255 2553-0  
17231 255255-20  
192 168 255 255 - 192 16800  
  
‎٠‏ عناوين محجوزة  
000مم2  
  
‎٠‏ عناوين غير قانونية  
0000  
  
‏م ف 008  
  
‎056 2644( ‏بك عا‎ ٠  
  
‏الوصول عن بعد  
  
‏\* في حالة استخدام الوصول عن بعدء تأكد من استخدام برتيكول 5504 [المنقذ 22) بدلا من  
  
‏عماء7  
  
‏نقل الملقات

» إذاكان بروتوكول 218 مطلوي. فتأكد من وضع ‎١١‏  
‏مختلقة عن تلك المخصصة للشبكة المحمية الداخلية  
حركة اليد الالكتروني  
\* التحقق من البوتوكول المستخدم للبريد والتأكد من وجود قاعدة لحظر حركة الريد اوارد باستثناء  
تلك القاصدة حادم البريد الداخلي.  
حظر حركة 16148 غير المرغب فيها (8,11,3 1648)  
‎٠‏ تأكد من وجود فاعدة تمتع طلبات ورسائل ارتداد 16148  
  
الذي بدعم 18 في شبكة فرعية  
  
\* تاكد من وجود قاعدة تمنع ارسال رسائل تجاوزت الوقت (6:666060 11818) ورسائل الإبلاغ  
عن عدم القدرة على وصول الهدف (100663603018)  
الخوادم الحرجة والحساسة (610601520086)  
\* التأكد من وجود قعدة تمتع حركة المرور الموجهة إلى عتاوين داخلية حرجة وحساسة من مصادر  
خارجية. يجب أن تستند هذه القاعدة إلى المتطلبات التنظيمية, نظ لأن بعض (جهات العمل)  
قد تسمج بتوجيه حركة المرور عبر تطبيق ويب وعب المنطقة المجردة من السلاح (00/42)  
جدران الحماية الشخصية:  
‎٠‏ تأكد من حصول مستخدي الكمبيوتر المحمول على التدريب المناسب فيما يتعلق بالتهديدات  
وأنواع المناصر المحظورة بواسطة جدار الحماية والمبادىئ التوجيهية لتشيل جدا الحماية.  
الشخصي. خذا العنصر ضروري: حيث تعتمد الجدران النارية الشخصية أحياناً على مكالية  
المستخدم بالرد على الهجمات؛ على سبيل المثال؛ ما إذاكنث تريد قبول/ رفض طلب من عنوان  
» قم بمراجعة إعدادات الحماية الخاصة بجدار الحماية الشخصي للتأكد من أنه يقيد الوصول إلى  
مناقذ ممينة, ويحمي من الهجمات المعروفة؛ وأن هتالك تنبيهات كافين لتسجيل الدخول  
وتتبيهات للمستخدم في حالة حدوث اختراق.  
» تأكد من وجود إجراء لتحديث البرنامج لآية هجمات.  
ذلك الاعتماد على ما توفره معظم الأدوات المشابهة من خيارات تحميل التحديثات التلقائية عبر  
الانترنيت. في مثل هذه الحالات» يجب التأكد من تلقي التحديئات من مواقع موثوق بها.  
جدران الحماية الموزعة  
  
أصبحت معروفة. ويمكن بدلأمن  
  
\* التأكد من توزيع سياسة الأمن باستمرار على جميع الأجهزة المضيفة» خاصة عند وجود تغيرات  
  
في السياسة.

18580 ‏التأكد من وجود ضوابط كاقية لضمان سلامة السياسة أثاء النقلء على سبيل المثال.‎ ٠  
‏التشفير السياسة عند التقل.‎  
  
\* تاكد من وجود ضوابط كافية لمصادقة المضيف المتاسب  
  
| أخرى يمكن استخدام 866 للمصادقة مع شهادات التشفير  
  
استمرار توافر جدران الحماية:  
  
\* تاكد من وجد جدار حماية بديل على جدار الحماية الأساسي ( 10 07 140151260  
متسيس  
بجب توثيق عمليات ضبط الشبكة والتغييرات الي تتم عليها بشكل منتظم وذلك لفهم بنيتهاء يجب أن  
يتضمن مسنتد توليق الشبكات ما بلي:  
1 رسم تخطيطي للشبكة  
  
ضوابط النظام (2800 م6008 5:601/)  
  
قواعد الجدا التري  
عناوين برتوكولات الأنترنيت (200685565 18]  
قوائم التحكم في الوصول  
  
سياسة الأطراف الثالثة.  
  
أو سياسة الوصول للأطراف الثالثة.  
  
ا انه  
  
تعمل سياسة الوصول للأطراف الثالثة على بيان الإجراءات الي تحكم وصول أطراف ثالث إلى شبكة (جهة العمل) وتطبيقاتها.  
وتتمثل الأطراف الثلثة في الجهات الخارجة عن (جهة العمل) من مؤسسات أو أفراد  
تغط السياسة الجواتب التالية للتعاملات مع الطرف الثالث:  
  
‎٠‏ تقييم مخاطر الطرف الثالث.  
  
‎٠‏ الاتفاقيات والعقود  
  
‎٠‏ توفي رخدمات للشبكة.  
  
‎٠‏ صلاحيات الوصول والاتصال للأنظمة والشبكات.  
  
‏> أمن الوصول من قبل الاطراف ‎١‏

ا 0  
الغرض من هذه السياسة هو تحديد السياسات والمعايير لجميع الأطراف الثالثة التي تسى للوصول إلى شبكة (جهة العمل).  
الغرض التعامل المشترك مع الأعمال المتعلقة ب (جهة العمل)؛ وقد تم تصميم هذه السياسة للحد من التعرض المحتمل  
للمخاطر المرتيطة بوصول الطرف الثالث ل (جهة العمل).  
  
سس  
تتطيق هذه السياسة على الموظفين في جهة العمل) المختصين بتوفير وصول الأطراف الثلئة إلى شبكة (جهة العمل) أو  
الأجهز الملحقة بهاء وكذلك على جميع الأطراف الثالئة سواء انوا فرا ا أوشزات أو مؤسسات أو متعاقدين أو استشارين أو  
  
متخصصين.  
  
بن تت  
  
يجب التوقيع على اتفافية عدم الإفصاح عند التعاقد مع الطرف الثال  
  
» وتحديد دور ومسؤوليات الطرف  
الثالث بوضوح في هذه الاتفاقية.  
  
\* لن يمتح الطرف الثالث إمكانية الوصول إلى مرافق شبكة (جهة العمل) إلا بعد توقيع عقد رسي  
يحدد الشروط والضوابط الت يجب على الأطراف الثلثة لاقام بها لضمان الوصول الأمن إلى  
مرافق شبكة (جهة العمل) من قبل الأطراف الثلثة.  
  
» تتطلب جميع طلبات الاتصال الجديدة بين ا لأطراف ‎١!‏  
‏الثالث وممئل (جهة العمل) على الاتفاقية والتوقيع عليها.  
  
> المتطلبات ‎١‏ لأولية (قبل الاتفاق): ستخضع عملية متح الوصول لمعدات تقنية المعلومات للمراجعة.  
والتصديق من القسم المختص بذلك (قسم أمن المعلومات)  
  
» تجري المراجعة الأمنيةللتأكد من أن أي توصيل بتطابق مع متطلبات العمل بأفضل مارية  
ممكنة, وأنه ينيع مبدا "أقل صلاحيات وصول".  
  
\* يجب على جميع الأطراف الثلثة لازام بمتطلبات أمن المعلومات واللي تضمن الحد الأدنى من  
مستوى الأمان الذي تطلبه (جهة العمل) من قبل الطرف الثالث» واللي بتحدد من خلالها ما الذي  
بجب على (جهة العمل) تنفيذه والحفاظ عليه من تدايير أمنية تخص جميع جوانب أمن  
المعلومات وجميع عمليات الدعم المرتبطة بها.  
  
ثة واجهة العمل) موافقة الطرف

يجب على جميع الأطراف الثلثة التأكد من أنها لا تنتهك أي من لوائح نظام إدارة أمن المعلومات  
في أي وقت أثناء تعاقدها مع (جهة العمل).  
  
إنشاء الاتصال:  
  
يجب أن يسنتد كل اتصال قاثم على مبدا "قل صلاحيات الوصول" وفقا لمتطلبات العمل  
  
والمراجعة الأمنية المعتمدة.  
  
تعديل أوتغير الاتصال والوصول:  
  
يجب أن تتم التغيوات في الاتصال أو الوصول بناء على ما تقتضيه مصلحة العمل وأن تخضع  
للمراجعة الأمنية كما يجب تنفيذ التغييرات من خلال عملي إدارةالتخير ب [جهة العمل).  
  
وصول الطرف الثالث المسموح به:  
  
يسمج للطرف الثالث الوصول إلى أنظمة أو شبكة (جهة العمل) للأغراض المتفق عليها في العقده  
وبشمل ذلك الشكاء لإجهة العمل) غير الموظفين مباشرة ولديهم وصول مباشر أو عن بعد إلى  
أنظمة وشبكة (جهة العمل).  
  
يجب السماح للطرف الثالث بالوصول إلى المرافق والخدمات والبيانات الي تكون مطلوية لتنفيذ  
المهام المحددة في العقد فقطء 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 أ أي أجهزة غير مملوكة لإجهة.  
العمل) للوصول إلى الموارد الموجودة على شبكة وأنظمة (جهة العمل)؛ يجب أن تضمن الأطراف الثالثة ما بلي:  
  
يجب أن تكون أنظمة التشغيل محدثة بشكل كامل مع أحدث التصحيحات.  
يجب تنصيب برامج مكافحة الفيروسات وبرمجيات التجسس والبرمجيات الضارة وبآخر  
  
التحديئات.  
  
> 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 الفي من قبل الطرفين لضمان تحقيق  
الامتثال لهذه السياسة.  
يجب تعيين المناصب التالية لكل اتصال بين الأطراف:  
  
مسؤول الخدمة أومن له الصلاحية ليكون مسؤولًا عن السماح بدخول الطرف الثالث  
  
من خلال تفويض الاتصال في تصريح كتلي.

2. المسؤول عن النظام والذي يتحمل المسؤولي الكاملة عن كل اتصال من ‎١‏ لأطراف.  
الثالثة وذلك للتأكد من تطبيق الأطراف للسياسات والمعاير لهذا الاتصال كما أنه  
المسؤول عن تأكيد ما إذاكان مسموحا للطرف الثالث بالدخول إلى أنظمة المؤسسة»  
وكدا له أن يحظر دخول الطرف الثالث إلى بعض الأنظمة الحساسة.  
الإبلاغ عن الحوادث: يجب أن تقوم االأطراف الثالثة بإبلاغ لإدارة عن أي حادثة تؤثر على أمن المعلومات.  
والخصوصية؛ وعلى جميع نقاط الضعف الأمنية المشتبه بها أوما قد بشكل تهديد ‎١‏ لأصول تقنية  
المعلومات في (جهة العمل).  
إنهاء الوصول:  
‎٠‏ عنما نتهاء الحاجة  
الوصول.  
\* يجب أن يقوم المسؤولون عن كل اتصال بمراجعة هذه الاتصالات ستوب للتحقق من وجود  
حاجة لاستمرارهاء وأن نوع الوصول الحالي ببي متطلبات الاتصال المرجوة.  
‎٠‏ يتم على الفور إنهاء جميع الاتصالات الي لم يعد لها فائدة أوحاجة في تنفيذ أعمال [جهة  
العمل  
\* في حالة تم تعريفهم داخل نظام (جهة العمل)ء يجب أن يكون لدى جميع الأطراف الثالئة.  
والمستخدمين الخارجيين تاريخ صلاحية لحساباتهم.  
  
الوصول يجب أن يقوم المسؤول عن الاتصال داخل (جهة العمل) بإتهاء  
  
القواعد الايشادية لاتفاقية عدم الإفصاح:  
  
\_  
  
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 متهما.  
  
ل سي  
الفرض من هذه القواعد هو ضبمان عملية توفيع اتفاقية عدم الافصاح ل (جهة العمل) من قبل جميع الاطراف الثالثة الذين.  
الديهم إمكانية الوصول إلى لبيانات السرية ل إجهة العمل) والاحتفاظ بها بشكل ملائم وموثوق.  
  
ل سي

نسري هذه القواعد الارشادية على (جهة العمل) وعلى جميع ‎١‏ لأطراف الثالثة سواء كانوا أقراد أوشركات أو مؤسسات أو  
  
متعاقدين أو استشاريين أو متخصصين.  
  
4  
  
القواعد الإرفادية:  
  
يجب على جميع الأطراف الثالثة توقيع اتفاقية عدم الإفصاح كخطوة أولى في بدابة عملهم مع (جهة.  
العمل)؛ مع اقرارهم بفهم هذه السياسة ولتزامهم بها.  
  
يجب على الطرف الثالث الممتوح له حق الوصول المباشر أوغير المباشر إل البيانات أو المعلومات التي  
تملكها (جهة العمل) عدم الافصاح عن هذه المعلومات أو نشرها.  
  
ترم (جهة العمل) بضمان الخدمات السرية لجميع الأطراف الثلثة. قالسرية هي بين الأطراف الثالثة و  
(جهة العمل) وليس للموظفين الذين يقدمون خدمات معينة.  
  
الوثائق اللي تحتوي على معلومات شخصية بما في ذلك على سبيل المثال لا الحصر الأسماء أوالعتاوين أو  
  
أرقام الهاتف أو السجلات الطبية أوالسجلات العالية لموظفي (جهة العمل) يجب أن تكون خاضمة لرقابة  
  
دقيقة ويجب عدم الإفصاح عنها أو الكشف عنها لأي أشخاص أو مصادر غير مصح لهم بذلك.  
يجب أن تحتوي اتقاقية عدم الإفصاح على الأقل على الآن:  
\* أسماء الأطراف المتعاقدة.  
\* أي من الأطراف المتعاقدة ملزم بحماية سرية المعلومات المكشوف عنهاء سواء كان الطرف  
المستقيل أو الطرف المفصح عنها أوكليهما (أحادي أوثناي)كما يمكن أن يكون لاتفاقية عدم  
الإفصاح أكثر من طرفين» وق هذه الحالة بجب تحديد الأطراف الملزمة بذلك.  
\* تحديد ماه المعلومات السرية في الاتفاقية.  
اللزامبالاتفاقية بالستوات.  
وشروط الحفاظ على سرية المعلومات بالسنوات.  
\* المعلومات الي سيتم استبعادها من الاتفاقية,كالمعلومات اللي تم معرفتها مسبق ‎١‏ أوالي  
تتواجد ومتاحة للعموم, أو الي يُظلع عليها لاحق امن أطراف أخرى.  
\* الشروط والقيود المتعلقة بطرق تقل المعلومات السرية.  
\* الإجراءات ال ينبني اتخاذها على المعلومات السرية عند تهاية التفاقية.  
\* مسؤوليات استلام والتعامل مع المعلومات السرية:  
1. استخدام المعلومات للأغراض المتفق عليها فقط.  
2. الكشف عنها فقط للأشخاص الذين يحتاجون إلى معرفة المعلومات لأذاء الاغراض  
المتقق عليها

3 استخدام الجهود المناسبة (بدل العناية اللازمة أو الجهود الممقولة) للحفاظ على أمان.  
المعلومات. غالياًما يتم تعريف الجهود المعقولة على أنها معيار لرعاية المعلومات  
السرية لا تقل صرامة عن تلك اللي بستخدمها المستلم للحفاظ على أمان معلوماته  
الخاصة.  
  
التأكد من أن الاشخاص الذين تم الكشف لهم عن المعلومات يلزمون بشروط تقييد  
الاستخدام وتقييد الإفصاح, وضمان حماية المعلومات.  
\* نوع الإفصاح المسموح به - المعلومات اللازمة للوصول للهدف المطلوب ف إطار القانون.  
  
\* بجب أن يختار الطرفان القانون والقضاء المختص الذي بحكم تنفيذ الاتفاقية.  
  
أسيسة لضع الاحتاطي  
ا انه  
  
تفشل الأنظمة واجهزة الكمبيوتر بشكل مفاجئ وقد تفقد السجلات الحيوية والنظم ومنتجات العمل بشكل لا رجعة فيه إذاتم  
تخزينها فقط على تلك ‎١‏ لأنظمة وأجهزة الكمبيوتر. وقد بسبب هذا الفقد نقص الإنتاجية وزيادة التكلفة, لذا وجب النسخ  
الاحتياطي للبيانات وهو عملية نسخ وتخزين واستعادة لبيانات الكمبيوتر والتى يمكن أن تكون في أي صورة م.  
يعمل النسخ الاحتياط على مابلى:  
  
توفير تخزين آمن لأصول البيانات الهامة لسير العمل في (جهة العمل).  
  
متع فقدان البيانات في حالة الحذف العرض ي أو تلف البيانات أو فشل النظام أو حدوث الكوارث.  
  
السماح باستعادةالبيانات المؤرشفة في الوقت المناسب في حالة حدوث كارثة أو فشل في النظام.  
  
ا 0  
الغرض من هذه السياسة هو توفير إطار متسق لتطبيقه على عملية التسخ الاحتياطي؛ بحيث تعطي هذه السياسة معلومات  
محددة للمساعدة في منع حدوث فقد ف 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.  
  
ب ت\_  
تتطبق هذه السياسة على جميع البيانات المخزنة على أنظمة (جهة العمل) وعلى جميع أجهزة الكمبيوتر: سواء أجهزة الكمبيوتر  
المحمولة وأجهزة سطح المكتب؛ وعلى جميع الخوادم الي تملكها (جهة العمل) وأي أجهزة إلكترونية أخرى تخزن البيانات.  
  
بن تت  
  
تحديد البيانات الهامة

يجب ان تحدد (جهة العمل) البيانات الأكثر أهمية لها وذلك من خلال عملية تصني البيانات.  
ومن خلال مراجعة أصول المعلومات, حيث يجب تحديد البيانات الهامة والحرجة بحيث يمكن  
منحها أولوية أعلى أثناء عملية التسخ الاحتياطي.  
البيانات الي يتم نسخها احتياطيا  
سيتم الاحتفاظ بنسخة احتباطية من؛  
1. جميع البيانات الي تقرر أنها هامة وحساسة لأعمال (جهة العمل) ولأ وظيفة.  
الموظف.  
2 جميع المعلومات المخزنة على خادم الملفات التابعة ل (جهة العمل). وتقع على عاتق  
المستخدم ضمان تقل أي بانات ذات أهمية إلى خادم الملفات.  
3. جميع البيانات المخزنة على خوادم الشبكة, والي قد تنضمن خوادم الويب وخوادم  
قواعد البيانات ووحدات التحكم في النطاق والجدران لنارية وخوادم الوصول عن بعاد  
  
تخزين التسخ الاحتياطي  
  
عند التخزين في موقع (جهة العمل) يجب ان تخزن وسائط النسخ الاحتياطي في حاوية مقاومة.  
للحريق في متطقة مؤمنة بضوابط تحكم بالدخول.  
  
يجب الحفاظ على الفصل الجغراق بين أماكن حفظ النسخ الاحتياطية وموقع (جهة العمل]»  
بسافة  
مناسية وذلك للحماية من الحرائق أو الفيضانات أو الكوارث الإقليمية أو الكبيرة الأخرىء للابتعاد  
عن أي ضر رفي حالة حدوث كازثة في الموقع الرئيسي.  
  
عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع يجب ضمان - وبشكل معقول- عدم  
تعرضها للكوارث كالسرقة أو التاركما يجب اختيارأماكن تخزين تستخدم أساليب حمابة من  
الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي.  
  
يسمح بالنسخ الاحتباطي عبر الإنترنث إذاكانت الخدمة.  
  
المعابير المحددة هنا  
  
تكوار النسخ الاحتياطي  
  
يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.  
الآلية الى يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح» يتعين على  
(جهة العمل) جدولة مواعيد مناسبة لعملية التسخ الاحتياطي متسقة مع طبيعة عمل المؤسسة؛  
بحيث يمكن استعادة بياذات كافية لاستمرار العمل في حالة وفوع حادث مقاجىء ولك يمكن  
اتجتب عببء 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 سطع المكتب أو الكمبيوتر المحمول الي في عهدتهم؛ ويقع على عاتقهم مسؤولية تخزين  
جميع لبيانات المهمة الموجودة لديهم على وسائط النسخ الاحتياطي المستخدمة في (جهة.  
العمل  
‎٠‏ بيجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين سخ احتياطية لهل  
\* بجب اختبار وتوثيق إجراءات استعادة لبيانات, كما يجب أن تحدد الوثائق من هو المسؤول عن  
عملية  
استعادة البيانات وكيف يتم تنفيذها وتحث أي ظروف يجب تنفيذها والمدة اللي تستغرقهاكامل  
العملية بد أمن الطلب وانتهاء إلى استعادة البيانات؛ من المهم للغية أن تكون الإجراءات.  
واضحة وموجزة بحيث ل تكون مريكة ويساء تفسيرها في وقت الأزمات من قبل القراء بخلاف  
مسؤول النسخ الاحتياطي.  
لاحتفاظ بالتسخ الاحتياطي  
\* يجب أن تحدد (جهة العمل) الوقت اللازم للاحتفاظ بالتسخ الاحتياطي, وما عدد النسخ المخزنة.  
من البيانات المنسوخة احتياطيا الكافية للحد من المخاطر بكفاءة مع الحفاظ على البياتات.  
المطلوية.  
\* يجب الاحتفاظ بتسخ احتياطية وفقا لجدول الحفظ والتخلص من النسخ الاحتياطي؛ يحدد  
الجدول حالة البيانات فيما إذاكان يمكن التخلص منها أو إعادة تدوبرها أوإبقاؤها في مخزن  
الأرشيف.  
النسع المخزئة  
‎٠‏ النسع المخزنة يجب ان تخزن مع وصف قصير يتضمن المعلومات التالية:  
تاريخ النسخ الاحتياطي / اسم المورد / نوع طريقة النسخ الاحتياطي) كامل / تزابدي)  
\* بجب الاحتفاظ بسجل للحركات المادية والالكترونية لجميع النسخ الاحتياطية؛ يجب أن نشير  
الحركة العادية والالكترونية للنسخ الاحتياطية إلى:  
. النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين.  
2. أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخرر  
يجب توفير النسخ المخزنة فور ورود طلب معتمده يجب أن تتم الموافقة على طلب البيانات المخزنة من  
قبل شخص مخول لهء بقوم بترشيحه مدير الإدارة المختصة, كما يجب أن تتضمن طليات البيانات.  
المخزقة ما بلي:

‎٠‏ تعبئة تموقج يوضح تفاصيل الطلب؛ بما في ذلك النسخة المطلوبة وأين وى يرغبا  
مقدم الطلب في استلامها والغرض من طلب النسخة.  
‎٠‏ الإفرار بان النسخة الاحتياطية سيتم إرجاعها أوإثلافها فور الانتهاء من استخدامها.  
\* تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.  
يجب توفير مستوى حماية مناسب للمعلومات المخزثة في موقع التخزين الاحتياطي وفق | للمعابير  
المطبقة  
في الموقع الرئيس ي:كما ينبني ان تمتد الضوابط المطبقة على وسائط النسخ الاحتياطى في الموقع الرئيس ي لتشمل موقع  
التخزين الاحتياطي.  
اختبار عملية استعادة البيانات  
\* يجب أن يتم فحص والقيام بإجراءات استعادة النسخ الاحتباطية بشكل منتظم لضمان فعاليتها  
وللتحقق من إمكانية استكمال اجراءات عملية الاستعادة في الوقت المحدد والإبلاغ عن قدرتها على استعادة البياتات.  
يجب اختبار وسائط النسخ الاحتياطي باننظام لمان الاعتماد عليها للاستخدام الطارىا 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:  
للتحقق من الأخطاء وتصحيحها.  
2 لمرافبة مدة عملية النسخ الاحتياطي.  
3 لتحسين أداء التسخ الاحتياطي حيثما أمكن ذلك.  
وسائط التسخ الاحتياطي  
\* يجب حماية وسائط النسخ الاحتباطي من الوصول غير المصرح به أوسوء الاستخدام أوالعيث  
بهاءبما في ذلك الحماية الكافية لتجنب أي ضر ر مادي ينش ا أثناء عملية نقلها أوتخزينها. لذا  
يجب على جميع الموظفين المسؤولين عن معالجة النسخ الاحتياطي للبيانات الآتي:  
1 أثبات هوية فوصلة  
2 إذن تخويل توصلة  
» عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أوالحساسة؛ ينبني مراعاة ما بلى:  
1 استخدام أماكن تخزين (حاويات) آمنة.  
2 التسليم باليد  
3 في الحالات الحرجة بتم تقسيم ماسيتم تسليمه إلى أجزاء يرسل كل جزه عبرط ربق  
مختلفة عن غيرد

\* يجب تدمير جميع وسائط التسخ الاحتياطية بشكل مناسب, ينم تدمير الوسائط والتخلص منها  
كما هو مو أدناه:  
1 يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.  
2 بجب ان لا تحتوي الوسائط على نسخ احتياطية يمكن إعادة استخدامها (فعالة)  
3 بيجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو  
استرجاعها من قبل طرف غير مصرح له.  
بجب العمل على أن تتلف وسائط النسخ الاحتياطي ماديا بحيث لا يمكن استعادة  
محتوباتها قبل التخلص منها  
\*» أنواع معينة من وسائط التسخ الاحتياطي لها عمر وظيفي محدود إذ أنه بعد مدة معينة من  
الخدمة لن يكون بالإمكان اعتبار هذه الوسائط مولوقابها. عند وضع وسائط النسخ الاحتياطي في  
الخدمة يجب تسجيل التاريخ عليهاء ليتم إيقافها عن الخدمة بعد أن يتجاوز وقت استخدامها  
مواصفات المضتع.  
  
'سياسة الأمان المادي  
  
الأمان المادي هو مجموعة من الإجراءات الأمني الى ينم تبنيها لضمان عدم وصول غير المصرح لهم إلى المواد والمعدات  
الخاصة بمركز لبيانات, إذ يمكن أن تتألف إجراءات الأمان المادي من طيف واسع من الطرق لودع وإحباط الدخلاء بما في  
ذلك اللجوء لطرق تعتمد على التقنية؛ وسياسة الآمان المادي المطبقة بشكل جيد يمكنها حماية موارد ومعدات مركز البيانات.  
من السرقة والعبث والكوارث الطبيعية والتخريب والهجمات السييرانية وغيرها من الأفعال المؤذية. على كل الأشخاص أن  
يكونوا على وي كامل بمحتويات هذه السياسة الأمنية وأن يتقيدوا بلأجزاء الي تشمل مجال عملهم.  
  
ب ت\_  
بعد تعيين وفرض الضوابط المادية والبيئية المطلوية لحماية الأصول والأنظمة المعلوماتية من الدخول الغير مص رح به  
وصونها من المخاطر البيئيةأمرا ل غنى عنه. وهذه السياسة تحدد متطلبات حماية مراكز الباذات من التهديدات الماديةة  
  
والبيئية لضمان سرية وتكامل وتوافر البيانات التق تحويها هذه المراكز

ب ت\_  
تصف هذه السياسة متطلبات الأمان المادي لمراكزاليانات التابع لإجهة العمل)؛ بم في ذلك مكاتب مركز عمليات الشبكة  
(1006 ,660166 06013005 :11610»0/6) وكل ما يتواجد بهاء والسياسة تغطي العديد من المتطلبات الخاصة بالأشخاص  
والممتلكات» فهي تشمل كل العاملين والمتحاقدين ومهتدس ي الخدمات وكل من يمثل (جهة العمل )والذين بدورهم يتوقع أن.  
يمنثلوا ويتقيدوا بهذه المتطلبات.  
  
بن تت  
  
بتدالعقار  
+ مخاطر الكوارث الطبيعية  
يجب أن يتم اختيار موقع مركز البيانات بحيث تكون احتمالية حدوث الكوارث الطبيعية عند مستويات مقبولة, الكوايث  
  
الطبيعية تشمل على سبيل المثال لا الحصر» المواصف الرعدية والامطار الغزيرة والعواصف الرملية والفيضاتات.  
  
\* 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 الحصرء تحطم الطائرات وأعمال الشغب والتفجيرات والاشتياكات المسلحة.  
والحرائق. يجب ألا يكون الموقع بجانب المطارات أو السجون أو التكنات العسكرية أو الطرق السريعة أوالملاعب الرياضية.  
أومسارات الاستعراضات.  
  
\* البنة التحتية  
يجب أن يعتمد مركز البيانات على المنشآت المزودة للطاقة الكهرائية بنسبة لا تقل عن 169.99, ولا بد أن يتم تزويد الكهرياء  
للموقع من محطتين (أوأكثر) فرعيتين متفصلتين ويفضل أن تتصل كل منهما بمحطات توليد متفصلة. ويجب أن يتوفر  
بالموقع مصدرين للمياه؛ كما لا بد من توفير أكثر من مزود خدمة واحد للاتصال بالشبكة.  
  
‎٠‏ تفرد الفرض  
  
‏ارك مركز البيانات نفس المساحة مع المكاتب الأخرى وخاصة تلك المملوكة لمؤسسة أخرى, وفي حال الاضطوار  
إلى ذلك فيجب ألا يكون لهذه المكتب جدران ملاصقة لمركز البيانات.  
  
‏يجبالا  
  
‎٠‏ محيط الموقع:

يجب أن تتواجد حراسة عند كل نقطة دخول لمركز لبيانات؛ وهو المكان الذي يجب أن يتم ضبط دخول العاملين بمركز  
البيانات عير باستخدام طريقة موثوقة للمصادفة الآلة.كما يجب آل يتواجد أي شيء يمكن أن يعيق الرؤية من خلال ميات  
المراقية أومن قبل حراس الدوريات في المساحات المحيطة بالمبنى والبي بد ورها يجب أن تكون مضاءة بشكل جيده ويجب  
ألا يكون هناك أي لوحات أو علامات إرشادية تبين أن المكان يخص مركزالبيانات أو هوبة (جهة العمل) المالكة.  
  
‎٠‏ المراقية:  
يجب تركيب كاميرات مراقية (620835 /211) خارج مرك البيانات لمراقبة الأماكن المجاورة كما يجب تسيير دوريات  
منتظمة من قبل الحراس داخل محيط (جهة العمل). وفي حالة وجود موقف للمركبات يجب أن يتم متح إذن خاص بدخوله  
للسيارات المملوكة للعاملين في (جهة العمل والمتعافدين والحراس وأطقم التظافة, وكل من عدا ذلك يجب أن يستعملوا  
موقف الزوار فقط؛ بينم المركبات الي لا تلم بذلك يجب سحبها خارج (جهة العمل) فور اكتشافها.  
  
‎٠‏ موضع توافذ غرف الخولام:  
يجب ألا تحتوي غرف الخوادم على نوافذ مطلة على الخارج» فهذه التوافذ تشكل خطرا بسب إمكانية استغلالها للتتصت عن  
بعد ولما تسيبه من دخول لحرارةزائدة للغرفة, لذا يجب أن تكون هذه الفرف في المنطقة الداخلية للمبى بعيداً عن الجدوان.  
الخارجية؛ وإذاكان لا بد أن تتواجد هذه الغرف قرب حواف المبنى فيجب أن بكون هناك عازل مادي خارج جدار الغرفة بحول  
دون الوصول المباشر لجدران غرفة الخوادم.  
  
‏» نقاط الدخول؛  
يجب أن تتواجد طريقة للمصادقة التلقائية عند كل نقاط الدخول ب (جهة العمل)؛ كما بجب توثيق دخول المواد والمعدات  
وكل الأشياء الي يصطحبها الأفراد الداخلين ل (جهة العمل) من قبل عناصر الحراسة؛ كما يجب متابعتها عند المغادرة مع  
تحديد الزمن وهوبة الشخص؛ ولذلك يجب أن بتوفر بمقر الحراسة إمكانية الوصول لقاعدة بيانات شارات (800285)  
المصادقة والتي يجب أن تحتوي على صورة لحامل الشارة, كما يجب أن تحتوي الشارة ذاتها على صورة لحاملها.  
  
‏\* غرف الخولام:  
1 الدخول  
  
‏يجب وضع لافنات توضح أن هذه الغرف هي مناطق محظورة الدخول لغير المصرح لهم؛ كما يجب أن تحوي على حظر  
  
‏الطعام والخراب والتدخين بداخلهاء ويجب أن تحتوي أبواب الغ رف على آلية للمصادقة اللقائية .كما يجب أن تكون هذه  
  
‏الأبواب مقاومة للحريق. ويجب أن يكون هناك بابين فقط للغرفة, فنظرآ لعدم وجود نوافذ فإن الاقتصار على باب واحد يعد  
  
‏تصميما مخالقا لمعظم ضوابط الحمابة من الحرائق المعمول بها دوليا. كما بجب السماح بالدخول لغرف الخوادم فقط لمن  
  
‏يقوم بصيانة الحواسيب أو البنية التحنية للفرف. كما يجب أن يقتصر الدخول أثناء العطل على حالات الطوارئ فقط لاغير

2. البنية التحتية  
يجب أن تخضع غرف الخوادم للمتابعة بكميرات المرافبة كما يجب توفير مصادر بديلة احتباطية للطاقة ولتبريد والاتصال  
بالشبكة عند كل غرفة؛ وبجب أن تزود القرف بأرضية مرتفعة (:100 885584) بحوالي 46 سنتيعتر من أجل السماح بسريان.  
الهواء وإدارة الكوابل, بالإضافة إلى وجوب أن تزود الغرف بألية لفلترة الهواء. كذلك يجب أن يكون سقف الغرف اليا ليسمح  
بتبديد الحرارة.  
  
3. البيئة  
درجة الحرارة في كل غرفة يجب أن يحافظ عليها ما بين 12 و24 درجة مئوية, كما يجب أن تبتى الرطوية مابين 9620 و9680  
ويتوجب مراقية درجة الحرارة والرطوبة باستخدام حساسات تركب داخل الغرف وأن توثق قراءاتهما وترسل إلى مركز عمليات  
الشبكة 1000  
  
4 الوقاية من الحرائق  
يجب تزويد كل غرفة بعامل غمر شامل (5011100 :8800 008108 (1013) كما يجب وضع أسطوانات إطفاء حريق  
مناسية في كل غرفة؛ يفضل عدم استخدام أنظمة أثابيب رش لإطفاء الحوائق في غرف الخوادم.  
  
المرافق  
‎٠‏ أنظعة البويد  
يجب تركيب نظام بويد بدبل بالمنشأة كما يجب عزل الوحدات الخارجية لنظام التبريد عن موقف المركبات الخاص بمركز  
البيانات.  
‎٠‏ الطقة  
  
يتوجب أن تحتوي غرف الخواام على مصدر طاقة مبني على البطاريات لديه سعة كافية لتشغيل الأجهزة إلى حين الانتقال إلى  
تشغيل مولدات الطافة المعتمدة على الوقود التقليدي (بالديزل مثلا)؛ في حالة عدم وجود مولد احتياطي للكهرياء فيجب أن  
تكون سعة البطاريات كافية للتشغيل لمدة 24 ساعة, كما يجب أن يتوفر وقود للمولد كاي لتشغيله لمدة 24 ساعة مخزنة في  
الموقع وأن يكون هناك تعاقد مسبق على تزويد المركز بوقودكافي للتشغيل لمدة أسبوع عند الحاجة لذلك.  
  
‎٠‏ القمامة  
يجب أن يتم مراقبة حاويات قمامة المنشأة بكاميرات الدوائر المغلقة, ويجب قرم وإتلاف كل المسنتدات التي تحتوي على  
معلومات حساسة بحيث لا يمكن استرجاعها قبل أن يتم التخلص منها.  
  
‎)006( ‏مركز ععليات الشبكة‎ ٠  
‏يجب توفير أنظمة مراقبة للحريق والطاقة والطقس ودرجة الحرارة والرطوبة بمركز عمليات الشبكة (0106): كما يجب أن‎  
‏يكون هناك طرق بدبلة احتياطية لبتواصل المركز مع العالم الخارجي. كما يجب تواجد أطقم (الموظفين المختصين) في المركز‎

على مدار 24 ساعة طول آيام الأسبوع؛ ويوصي أن بقوم موظفي المركز بمتابعة وكالات الأنباء للاطلاع على أي أحداث قد  
يكون لها تو 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 الأسئلةالتالية: م الذي يمكن اعتباره.  
كارثة؟ من الذي يتم تنبيهه بحدوث الكارثة وكيف يتم ذلك؟ من الذي بجري تقييما للأضرار ويقرر ماهي الموارد الاحتياطية.  
الي يجب استخدامها؟ أبن تقع المواقع الاحتياطية وما الذي يتم القيام به للحفاظ عليها وما هو الجدول الزدي الخاص  
بذلك؟ كم م ره وتحت أي ظروف يتم تحديث الخطة؟ إذاكانت المؤسسة لا تملك مركز لبيانات» ما طول الزمن الذي يكون  
فيه مركز لبيانات المتعاقد معه خارج الخدمة إلى حين عودته للعمل؟ يتوجب حفظ وتحديث قائمة بالأشخاص والمؤسسات  
الي يجب تبليفهم من قبل طاقم مركز عمليات الشبكة بما في ذلك أرقام المكتب والمنزل والنقال ومعرفات التواصل الفوري  
إن أمكن.  
\* التخزين الاحتياطي خارج الموقع  
يجب إجراء تسخ احتياطي للبيانات الحساسة بشكل دوري وحفظها خارج موقع مركز لبيانات» ويتوجب إصدار وتنفيذ سياسة.  
'نسخ احتياطي تحدد الخطوات الواجب اتباعها لاستعادة النسخ الاحتياطية وتحتوي جدولاً زمنيا لإجراء بروقات اختبار  
جاهزية خطوات النسخ الاحتباطي.  
كم بندما يخص البدر  
» الغير عاملين بمركزالبيانات.  
الحراس  
كل الحراس يجب أن يتم التحقق من سوابقهم الجتائية قبل توظيفهم وتكرار ذلك بشكل دوري؛ وبجب تعريفهم على الغرض  
من سياسة الأمان المادي وتدرييهم على كيفية الفرض الدقيق لهذه السياسة.  
2. أطقم النظافة  
يجب أن يعمل أقراد النظافة في مجموعات لا تقل عن شخصين وبجب حصر عمل طاقم النظافة على المكاتب ومركز  
عمليات الشبكة, في حال استدتى الأمر تواجدهم داخل غرفة الخوادم يتوجب أن يصحيهم أحد موظفي (1006)  
3 مهندسي الصيانة  
يجب توثيق زمن دخول وخروج مهندس ي الصيانة للمنشأة عند مدخل المبق. كما يجب على موظفي مركز عمليات الشبكة.  
توثيق عملية تبادل شارات الدخول لمهندس ي الصيانة عندما بدخلون غرفة الخوادم.  
4 الزوار

يجب أن يرافق الزوار الشخص الذي بزورونه طول المدة التق يقضونها بالمركزء 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  
الخولدم.  
  
يجب أن يكون المستخدمين على وعي بخطر تسرب البيانات أو المعلومات بطرق احتيلية 50/108 )58010148) وغيرها من  
طرق الهندسة الاجتماعية, كما يجب تدرييهم على الاحتراس من الدخلاء؛ ويجب أن بدربوا على تأمين حواسييهم المكتبية  
والمحمولة داخل وخارج المركز والوعي بما يحيط بهم وإجراءات الطوارئئ لني عليهم اتباعها عند الحاجة.  
‎٠‏ السيامة  
يجب أن بوقع كافة المستخدمين داخل مركزالبيانات اتفاقية عدم افصاحءكما يجب عليهم توقيع سياسة الأمان المادي التي  
يقوم حراس الأمن بفرضها.  
التعاف من الكوارث  
  
يجب أن اعتماد هيكل تنظيمي مكتوب ببين مهام كل وظيفة ومسؤولياتهاء ويحتوي على معلومات عن المهام الأخرى الي تم  
تدريب الموظف على أدائها غير تلك اللي ضمن مهام وظيفته الحالية.  
  
\* توثيق مهام العمل  
يجب عدم الاقتصار على توثيق ما يعرفه الموظقين حالياً على الأنظمة الموجودة, كل الأعمال الجديدة والتغيرات الي تطراً  
على الأنظمة يجب أن توثق أيضاً.  
  
\* التدريب على مهام الزملاء  
يجب تدريب موظفي مركز لبيانات على عدد من مهام زملائهم؛ وهو الأمر الذي بساهم في تتفيذ بعض المهام الرورية  
والحرجة عند حدوث أزمة ماء كما يضمن إنجاز العمل عند حدوث ض رف طاري لأحد الموظفين مما يسهل عملية إحلال  
  
موظف مكان الآخر  
\* معلومات التواصل  
  
يجب حفظ وتحديث بيانات التواصل الخاصة بكل موظفي مركز البيانات.  
العمل عن بعد  
  
يجب على موظفي مركز ابيانات التدرب على العمل عن بعد بشكل دوري. إذ أن ذلك سيسهل إمكانية استعرار تشغيل المركز  
فى حالة استعص ى الوصول والتواجد بالمركز لسيب ما

سياسة تصنيف البيانات:  
هدفها تصنيف البيانات ع مستويات وتحديد اجراءات الحمابة لكل مستوى. وتامين الحماية اللازمة للمعلومات وعدم تمكين  
الوصول إليها وتسريبها من غير ذوي الصلاحية, وحمابتها من أي محاولة تهديد خاريي»  
  
ويشمل هذا المصطلح العديد من الأدوات والطرق والإجراءات اللازمة والواجب توفرها لتمكين الحماية من المخاطر الي من  
المحتمل قد تحدث من الداخل اوالخارج للمنظمة,  
  
يعتبر هذا التوع 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  
أمن المعلومات في عبارة عن سلسلة من العمليات والطرق والإجراءات يت تطبيقها من قبل بعض القطاعات ومتقلمات  
التأمين لفرض أقوى طرق الحماية والتحكم على المعلومات الخاصة بها وعلى أنظمتها, ووسائطها لمتع تمكين الوصول إليها  
لغير الممتح لهم  
  
تمتاز حمابة المعلومات بأنها عملية وإجراءات مستمرة, أي إنها تتطلب بالضرورة إلى العمل بشكل دائم في مواكبة كل ما هو  
جديد ومتطور من تقتيات الامن وأسالييها في حمابة ما تملكه المنظمة من معلومات حساسة؛ كما بجب الاستمرارية بشكل  
داثم برض الرقابة على المخاطر وافتراضهاء  
  
والسي بشكل دوري لإيجاد حلول وبنكارات دائمة, لذلك لا يمن إطلاق النظام المعلوماي الأمي الحقيني على نظام أي من  
المؤسسات إلاني 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.  
  
أي تغيير عليها دون إذن مسبق»  
  
منع تسريب البيانات خارج المنظمة (01- 0100801100 1282م 0213

المعلومات السرية والمهمة تشكل هاجس لدى الكثير من المسؤولين في المنظمات للبيائات التي تمتلكها إلى خارج نطاق المنظمةر  
ووصولها لأشخاص غير مصرح لهم الاطلاع على البيانات, خسائ ركبيرة تتج عن تسرب البيانات للمنظمات هذا  
  
'سوف نركز من خلال السياسيات المتيعة على أحد مفاهيم واستراتيجيات امن المعلومات  
منع تسريب البيانات أوما يسى 01 01180800 188/286 0912 ويطلق عليه أحيانً  
(08801100 055ا 0213) وكلاهما بحملان نفس المعنى من حيث المفهوم , ولكن يطل  
في حال فقدان (58م1) يكون التسريب بشكل متعمد  
  
في حال تسرب (01:080ه1] يكون بشكل غير متعمدر  
  
بالإضافة إلى أن هناك مسميات عديدة ومفاهيم متعلقة بهذا المفهوم ومنيثقة من 018  
  
(طا) ممت مع يقوم لامعا 200 1010م  
  
((ظاا) ومتتمعاعيم غم ممتتععتعة ماقم 0120م  
(617) عمابع11 مد ع11ءماممه امعتم  
  
(100) متمق عمة مملتععتميم مملامدطام  
  
وعتامام فهو  
  
غات غاغاعا  
  
00ت عا10ع 200 /60ع5 ه001  
(01 000:808100 ©1:28دما 0212 يمكن تعريفها على انها استراتيجية أمنية شاملة للحفاظ على البيانات.  
المهمة من الأشخاص الغير مصرح لهم بالاطلاع عليها ومتع تداولها خارج نطاق المنظمة باختلاف أنواع البيانات وحالة ومكان.  
هذه البيانات سواء كانت مخزنة على وحدات التخزين (:10-689) أو أجهزة المستخدمين والخوادم (92لا- 10) أو متنقلة من  
خلال الشبكة (10-001500)  
اهم العوامل في حمابة البيانات تكمن من خلال إن بناء استراتيجية شاملة للحفاظ على البيانات من تداولها خارج نطاق المنظمة.  
يعتمد بشكل أساسي على تصنيف هذه البيانات 625516621100 0213 كذلك (25ا6اا0م 0005ر0|فتطبيق سياسات  
تصنيف البيانات من قبل المنظمات من حيث سرية البيانات وأهميتها ويساعد كثيا  
عند فرض القيود التقنية والحلول الأمنية المتاسبة لحماية البيانات, وكمثال على تصنيف البيانات في المنظمات (عام» هام»  
اسريء سري للغاية) فجميع البيانات بشكل عام متفاونة الأهمية بحسب تصنيفها  
  
هناك طرق كثيرة لتسريب البانات منها

1 الحديث بصوت عالى في الأماكن العامة على ما تحتوبه بيانات المنظمة.  
اسياسة المكتب النظيف تنص على عدم ترك ملفات بالمكتب من غير توقير حمابة من السرقة 0م :0656 6620  
ترك الأجهزة بدون تسجيل خروج أو ققل للشاشة اوعدم حمابة الملفات.  
الهندسة الاجتماعية وخداع الموظفين من خلال طرف الاحتيال لاستخراج المعلومات المهمة والسرية من الموظفين  
تسخ البيانات على أجهزة التخزين المختلفة متها (1158,110) ونقلها خارج المنظمة.  
طباعة الملفات المهمة عن طريق الأشخاص الغير مصرح لهم وعدم اتلافها أو إخراجها خارج المنظمة.  
استخدام الكموا المدمجة مع أجهزة الهواتف المحمولة لالتقاط صور للبيانات المهمة ويمكن من حمايتها عند تبي  
0ه عتعنابه ودلا مقرم ميعافها 0012)  
8 إرسال البيانات المهمة إلى خارج المنظمة بدون تصريح عبر البريد الإلكتروني  
9 ضعف أنظمة تحكم الوصول 6000101 466855 التطبيقات وقواعد البيانات ولي عن طريقها بتم الوصول للبيانات.  
المهمة  
10. وصول وتمكن المخترقين من عالم النترنت إلى الشبكة الداخلية للمنظمة عبر الخدمات الإلكترونية المقدمة من  
خلال اانترنت او التصيد الالكتروني من خلال الويد  
كثير من الشركات التقنية والبرمجية طرحت عدة أنظمة مخصصة لاستاتيجيات  
(015 062020000 286ادها 0213) وهنا سوف تكتب بشكل عام عن أبرز النقاط الي يركز عليها الكثير من المهتمين بهذا  
الجاتب والأنظمة المخصصة لذلك والي تشمل عدة جوانب منهاالتقنية والإدارية والمادية الفيزيائية وهي كالاي:  
. أولااهم خطوة قبل البده 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 البانات تُتبع عند التخلص منها سواء كانت هذه لبيانات تقنية أو  
  
ويقية  
  
4 تتقيف وتوعية موظتي المنظمة بشكل دوري تجاه المخاطر التقنية المختلقة ك اتقنوع متافنة » كنامعالقارا  
!#لاوالي قد تساهم في تسريب البياتات خارج المنظمة.  
  
5. إيجاد أنظمة التحكم بالوصول 6001101 800056 داخل المتظمة سواء كانت على البيانات أو التطبيقات وحتى  
المبان لدى المتظمة يجب أن تكون متواجدة وفعالة بالقدر الذي يحمي البيانات من الوصول الغير مصرح له  
  
6 التأكد من ان الصلاحيات الممتوحة لمستخدي أنظمة المنظمة وتطبيقاتها تستند على وفق الحاجة :1885  
  
امعودانوم

7 عدم السماح استخدام اجهزة المستخدمين وتعطيل أو مرافبة الأجهزة الت قد تساهم في تسريب البيانات مثل  
0/0/ق ,58لا  
  
أنواع البانات المستهدفة.  
1 البيانات عند تخزينها 6557 0438100  
البيانات عند تخزينها تخير إلى البيانات المخزتة الأرشفة هذه المعلومات تكون ذات أهمية بالتسبة للخركات  
والحكومات ,بشكل عام بسبب زيادة احتمالية تعرضها للاختراق قاو التسرب من قبل طرف غير مصرح به عندما لا  
يتم استخدامها,بشكل دوزي حمابة هذه المعلومات يتضمن عدة طرق مثل التحكم بالوصول؛ تشفير البيانات.  
وسياسات تطبق لحفظ البيانات.  
  
2. البيانات عند استخدامها  
6 100 0878 البيانات في حال تم استخدامها تشي إلى البينات الني يقوم المستخدم بالتعامل معها حاليا أنظمة  
منع فقد البيانات تقوم بحماية هذه البيانات عن طريق مراقي وتتبعها والتدقيق عليها وتحديد إذاكان هناك اي  
نشاطات غير مصرح بها مثل التقاط صورة للشاشة, النسخ واللبق وغيرها من محاولات نقل بيانات حساسة سواه  
كانت عن عمد أم يدونه.  
  
3 البيانات عند انتقالها 087810014011001  
البيانات عند انتقالها هي البيانات اللي من خلال شبكة الاتصال حى تصل الى جهة النهاية شبكات الاتصال قد  
تكون داخلية أوخارجية نظم منع تقل البانات تحمي هذه البيانات حيث ترافب الحساسة منهاوالتأكد عدم تسريب  
البيانات بشكل غير مصرح به حى تعبر الشبكة عبر قنوات الاتصال.