الهيئة الوطنية لأمن
وسلامة المعلومات
National Information Security
& Safety Authority

السياسات الوطنية
لأمن وسلامة المعلومات

المحتويات

اعداد

فريق تجهيز دليل ارشادي لسياسات ومعايير أمن وسلامة المعلومات

مراجعة

مدير إدارة أمن وسلامة النظم والتطبيقات
مدير إدارة معالجة حوادث المعلوماتية والشبكات
رئيس قسم السياسات والمعايير

اعتماد

مديرعام الهيئة

Prepared By

Information Security Policy Manuel Team

Reviewed By

Systems & Applications Security Head of Department
LibyaCERT Head of Department
Assurance & Compliance Head of Division

Approved By

NISSA General Manager

سياسة حماية البيانات

1 سياسة تصنيف المعلومات

1.1 مقدمة

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

1.2 الغرض

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

1.3 النطاق

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

1.4 السياسة

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

1.4.1 **سرية (مقيدة):** تعرّف البيانات السرية على أنها عالية الحساسية، ويسبب الكشف عنها أو فقدانها أو تدميرها أضرار كبيرة لشخص أو أكثر أو جهة العمل. ويمكن أن تشمل ما يلي:

- البيانات الشخصية للموظفين أو العملاء في جهة العمل، مثل هوية المستخدم (User ID) والضمان الاجتماعي أو أرقام الهوية الوطنية وأرقام جواز السفر وأرقام بطاقات الائتمان وأرقام رخصة القيادة، والسجلات الطبية.
- بيانات المصادقة: مثل مفاتيح التشفير الخاصة، واسم المستخدم وكلمة المرور.
- السجلات المالية: مثل أرقام الحسابات المالية.
- المواد التجارية: مثل الوثائق أو البيانات التي تكون ملكية فكرية فريدة أو محددة.
- البيانات القانونية: بما في ذلك البيانات المصرح بها للجهات القانونية فقط.

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

- البريد الإلكتروني، معظم الرسائل يمكن حذفها أو نشرها دون أن تتسبب في أضرار (باستثناء البريد الإلكتروني من الأشخاص الذين يتم تحديدهم في التصنيف السري).
- الوثائق والملفات التي لا تتضمن بيانات سرية.

- أي بيانات مصنفة على أنها غير سرية. ويمكن أن تشمل معظم بيانات الأعمال، حيث أن معظم الملفات التي يتم إدارتها أو استخدامها يومياً يمكن تصنيفها على أنها حساسة. ومن أمثلة هذه البيانات محاضر الاجتماعات وخطط العمل والتقارير الداخلية للمشاريع.

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

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

2. سياسة حماية البيانات

2.1 مقدمة

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

2.2 الغرض

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

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

2.3 النطاق

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

2.4 السياسة

2.4.1 المسؤول عن البيانات

- يجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته مع قيمة الأصول التي سيتولى إدارتها وحمايتها.
- يجب عدم تكليف موظف مسؤول رسمي للبيانات التي ليس لها تصنيف أمني وتكون ذات قيمة عملية محدودة، كما يجب التخلص من البيانات إذا لم يكن هناك حاجة قانونية أو تشغيلية لإبقائها، وينبغي تعيين المسؤولين المؤقتين لهذه البيانات داخل كل إدارة لضمان إتمام عملية التخلص منها.

- يكون منشيء المستندات الجديدة التي لها استخدام داخلي محدد على المدى القصير هو المسؤول عنها، وهذا يشمل الرسائل والخطط والجداول والتقارير ، كما يجب إبلاغ جميع الموظفين بمسؤوليتهم عن الوثائق التي ينشئونها.
- يجب تعيين مسؤول موثوق وتحديد مسؤولياته بشكل واضح اتجاه أصول البيانات التي يتم استخدامها في "جهة العمل" على نطاق واسع. وينبغي أن يملك هذا الشخص القدرة على التحكم في هذه البيانات.

2.4.2 تخزين البيانات

- يتم تخزين جميع البيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتياطية منتظمة.
- يجب عدم السماح للموظفين للوصول إلى البيانات إلا بعد اعلامهم وموافقتهم على شروط الاطلاع على البيانات التي سيتعاملون معها.
- قواعد البيانات التي تحتوي على بيانات شخصية يكون لها إجراءات محددة لإدارتها وتأمين السجلات والوثائق.
- يجب تخزين الملفات التي يتم تصنيفها كمخاطر أمنية محتملة في أكثر المناطق أمناً على الشبكة.

2.4.3 الكشف عن البيانات

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

3. سياسة الاحتفاظ بالسجلات و اتلافها

3.1 مقدمة

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

3.2 الغرض

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

3.3 النطاق

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

3.4 السياسة

3.4.1 سجلات المحاسبة والمالية، وتشمل على:

- الوثائق المتعلقة بكشوف المرتبات وإجراءات المحاسبة ودفاتر الحسابات الدائنة والجداول الزمنية، ودفاتر الحسابات والفواتير وتقارير نفقات الموظفين. ويجب الاحتفاظ بها خمس سنوات على الأقل.
- ينبغي الاحتفاظ بصفة دائمة بتقارير المراجعة السنوية والبيانات المالية، والاحتفاظ بالخطط السنوية والميزانيات للمدة اللازمة لتنفيذها والرجوع إليها عند الحاجة.

3.4.2 يجب الاحتفاظ بالعقود والمراسلات ذات الصلة بالعقود (بما في ذلك أي تعديلات على بنود العقد وجميع الوثائق الداعمة الأخرى).

3.4.3 سجلات "جهة العمل" (محاضر الاجتماعات، التكاليف الموقعة من الادارة، أختام "جهة العمل"، أحكام التأسيس واللوائح، سجلات المساهمة والتقارير السنوية) والتراخيص والتصاريح ووثائق التأمين يجب أن تحتفظ بشكل دائم.

3.4.4 يجوز إتلاف المستندات المعتبرة في حكم المستندات ذات القيمة بعد اتخاذ الاجراءات اللازمة لتسجيل بياناتها أو ملخصها إذا مضى على استعمالها أو على إجراء آخر قيد فيها خمس سنوات إلا إذا كانت هذه المستندات محل فحص أو مراجعة أو كانت مطلوبة في دعوة قائمة أو كانت القوانين واللوائح أو تعليمات وزارة المالية تقرر الاحتفاظ بها لمدة أطول.

3.4.5 الوثائق الالكترونية

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

3.4.6 الملفات والمستندات القانونية

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

- ملفات الدعاوي القضائية وما يصدر فيها من أحكام ابتدائية ونهائية، وقرارات وأوامر المحاكم بما في ذلك جميع الملفات ذات الصلة.
- المذكرات والآراء القانونية الصادرة عن المكاتب القانونية.

3.4.7 السجلات الشخصية

- ملفات الموظفين وما يتضمنه من مستندات تخص حياتهم والوظيفية تحفظ بشكل دائم حتى بعد إنهاء علاقة الموظف "بجهة العمل"

- سجلات الإدارية الوظيفية (وتشمل سجلات الحضور والانصراف، استمارة الطلبات، سجل تغيرات العمل، أوراق انهاء الخدمة، نتائج الاختبارات، سجلات التدريب) يتم الاحتفاظ بها وفق الحاجة إليها وللمدة اللازمة وفق تقديرات "جهة العمل"
- سجلات وأوراق امتحانات شغل الوظائف: تحتفظ "جهة العمل" بأوراق إجابة الامتحانات التحريرية والسجلات والقوائم وسائر الوثائق المتعلقة بالامتحانات التي تجريها لمدة سنتين تبدأ من تاريخ اعتماد نتيجة الامتحان.

3.4.8 سجلات ومستندات تتمتع "جهة العمل" بسلطة تقديرية في تحديد المدة اللازمة للاحتفاظ بها وترتبط السلطة التقديرية باستمرار حاجة "جهة العمل" لها أو استخدامها والرجوع إليها ومنها:

- التقارير الاستشارية.
- دليل السياسات والإجراءات (الأصلي / النسخ)
- التقارير السنوية.

3.4.9 إجراءات اتلاف الوثائق

- يجب عدم إزالة أو اتلاف السجلات الا ان كانت مصنفة بذلك او عند انتهاء مدة الاحتفاظ بها.
- عند الاحتفاظ بالسجلات خلال الفترة المحددة لها في جداول الاحتفاظ، يتم إعدادها للإتلاف.
- الوثائق المالية يتم إتلافها والتخلص منها وفق الإجراءات المحددة بلائحة الميزانية والحسابات والمخازن:
- الوثائق المالية و سجلات المتعلقة بالموظفين يتم اتلافها بوسيلة تضمن إتلاف المستندات إتلافا كلياً
- يتم التخلص من البيانات الإلكترونية المحتفظ بها في الوسائط الأخرى عن طريق الاتلاف المادي لتلك الوسائط.
- يجب أن تتم عملية اتلاف السجلات بشكل آمن وكامل.
- يجب تسجيل عملية الاتلاف في وثيقة رسمية لاتلاف البيانات داخل "جهة العمل".

4. سياسة نشر البيانات

4.1 مقدمة

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

- **بيانات لا يمكن الكشف عنها**
  - البيانات الشخصية، وتشمل سجلات الموظفين والبيانات الطبية، وبيانات عن الراتب والمزايا.
  - البيانات المالية.
  - المسائل والإجراءات القانونية أو التأديبية أو محاضر التحقيق ويتم إعلان صاحب الشأن بالطرق الرسمية.
  - جميع البيانات السرية.
- **البيانات التي يتعين الكشف عنها فيما يتعلق بارتباط مع جهات عمل الأخرى**

- ملخصات المشروع الأولية.
- البيانات والمعلومات التي ترى "جهة العمل" ضرورة نشرها لاستخدامها أو لأخذ العلم بها.

4.2 الغرض

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

4.3 النطاق

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

4.4 السياسة

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

5. سياسة الوصول للبيانات

5.1 مقدمة

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

5.2 الغرض

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

5.3 النطاق

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

5.4 السياسة

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

Data Protection Policy

1 Information Classification Policy

1.1 Introduction

It is essential for "Organization" to classify its information assets to help manage and protect it. The various departments at "Organization" have a multitude types of documents and data, each business unit or department should classify its data by considering the potential for harm to individuals or the University in the event of unintended disclosure, modification, or loss. This can be done by identifying which information should be protected and which information shall be placed open to the public and third parties.

1.2 Purpose

In order to preserve the appropriate confidentiality, integrity and availability of "Organization's" information assets, the information classification policy describes principles that need to be followed to protect information through specifying how and to whom you can distribute information with a particular classification.

To provide the basis for protecting the confidentiality of data at "Organization" by establishing a data classification system. Further policies and standards will specify handling requirements for data based on their classification.

1.3 Domain

This policy applies to all data or information that is created, collected, stored or processed by "Organization", in electronic or non-electronic formats, irrespective of the data location or the type of device it resides on. All staff should consequently use it, and third parties who interact with information held by and on behalf of "Organization".

1.4 Policy

All data at "Organization" shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.

1.4.1 **Confidential (restricted):** Information that is classified as confidential or restricted includes data that can be catastrophic to one or more individuals and/or organizations if compromised or lost. Such information is frequently provided on a "need to know" basis and might include:

- Personal data, including personally identifiable information such as Social Security or national identification numbers, passport numbers, credit card numbers, driver's license numbers, medical records.
- Financial records, including financial account numbers such as checking or investment account numbers.
- Business material, such as documents or data that is unique or specific intellectual property.
- Legal data, including potential attorney-privileged material.
- Authentication data, including private cryptography keys, username password pairs.

1.4.2 **For internal use only (sensitive):** Information that is classified as being of medium sensitivity includes files and data that would not have a severe impact on an individual and/or organization if lost or destroyed. Such information might include:

- Email, most of which can be deleted or distributed without causing a crisis (excluding mailboxes or email from individuals who are identified in the confidential classification).
- Documents and files that do not include confidential data.
- Anything that is not confidential. It can include most business data, because most files that are managed or used day-to-day can be classified as sensitive.

1.4.3 **Public (unrestricted):** Information that is classified as public includes data and files that are not critical to business needs or operations. This classification can also include data that has deliberately been released to the public for their use, such as marketing material or press announcements. In addition, this classification can include data such as spam email messages stored by an email service.

1.4.4 "Organization" associates shall be guided by the information category in their security-related handling "Organization" information.

2 Information Protection Policy

2.1 Introduction

Information is a major asset that "Organization" has a responsibility and requirement to protect. Differently classified information should appropriately protected in storage, transit, access etc. from modification or disclosure.

2.2 Purpose

Information Protection Policy addresses the stocks of information (electronic data or paper records) that "Organization" maintains, and also the people that use them, the processes they follow and the physical computer equipment used to access them, all these areas addresses to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at "Organization". The policy specifies the means of information handling and transfer within the Business.

2.3 Domain

This Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of "Organization" who have access to Information Systems or information used for "Organization" purposes.

2.4 Policy

2.4.1 Information assets Owner

- All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalized and agreed.
- Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each

department to ensure that this is done.

- For new documents that have a specific, short term localized use, the creator of the document will be the originator. This includes letters, spread sheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.
- For information assets whose use throughout "Organization" is widespread a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

2.4.2 Information storage

- All electronic information will be stored on centralized facilities to allow regular backups to take place.
- Employees should not be allowed to access information until they understand and agree the legislated responsibilities for the information that they will be handling.
- Databases holding personal information will have a defined security and system management procedure for the records and documentation.
- Files which are identified as a potential security risk should only be stored on secure network areas.

2.4.3 Disclosure of Information

- In the case of sharing restricted information with other organization, disclosing such information must not be to any other person or organization via any insecure method.
- Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.
- Disclosing restricted information to any external organization is also prohibited.

3 Record Retention and Destruction Policy

3.1 Introduction

Record retention and destruction is an important substantive component of many of the laws with which most corporations must comply, and it is often the vehicle by which compliance is established.

3.2 Purpose

The purpose of this policy is to ensure that necessary records and documents of "Organization" are adequately protected and maintained and to ensure that records that are no longer needed by "Organization" or are of no value are discarded at the proper time.

3.3 Domain

This Policy applies to all records generated in the course of "Organization's" operation, including both original documents and reproductions.

All employees should comply with any published records retention policies.

3.4 Policy

3.4.1 Accounting and Finance records include, but may not be limited to,

- Documents concerning payroll, accounting procedures, accounts Payable ledgers and schedules, accounts receivable ledgers and schedules, employee expense reports, interim financial statements, notes receivable ledgers and schedules. These should be retained for at least five years.
- Annual audit reports and financial statements should be permanent retained, and the annual plans and budgets should retained for the time required to implement them and/or refer to them as needed.

3.4.2 Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation) should be permanently retained

3.4.3 “Organization” records (minute books, signed minutes of the Board and all committees, corporate seals, articles of incorporation, Contribution records and annual corporate reports) as well as licenses, property insurance and permits should have a permanent retention.

3.4.4 It is also possible to destroy documents considered in the judgment of a valuable documents and have never been used or modified for the last 5 years, only if these documents are subject to examination or review or were required in an ongoing legal proceeding, or Instructions/regulations set by the Ministry of Finance decides to keep them longer.

Destruction of those documents only after taking the necessary procedures to record their data or its summary.

3.4.5 Electronic documents

- Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.
- Electronic Mail: Not all email needs to be retained, depending on the subject matter, E-mail that needs to be saved should be either printed in hard copy and kept in the appropriate file, or downloaded to a computer file and kept electronically or on disk as a separate file.
- Web Page Files: All workstations: Internet Browsers should be scheduled to delete Internet cookies once per month.

3.4.6 Legal files and papers

Permanent retention of "Organization" legal archive as follows:

- Files of the judicial proceedings and the decisions of the preliminary and final judgments, decisions and orders of the courts, including all relevant files.
- Legal notes and opinions issued by legal offices.

3.4.7 Personnel records

- Employee Personnel file should have a permanent retention even after Termination of employee relationship with the "Organization"
- Employment records (including individual attendance records, application forms, job or status change records, termination papers, test results, training and qualification records) shall be retained as needed and for the necessary period according to "Organization estimates.
- "Organization" should retained for a period of 2 years all Job interview related documents (including written examinations, records, lists and all other documents relating to the exam).

3.4.8 Records and documents The "Organization" has the discretion to determine the time required to retain them and the discretionary authority is related to the continued need of the "Organization"

- Consultant's reports.
- Policy and procedures manuals (Original / Copies)
- Annual reports.

3.4.9 Document destruction procedures:

- Records must not be removed or destroyed before retention period expiration;
- Once records have been retained for the applicable period of time, set forth in the record

retention

- Destruction of finance records shall be in accordance to budget and accounts procedures.
- Destruction of financial and personnel-related documents and all paper documents will be accomplished by a method that prevents retrieval of this data.
- Electronic data contained on all other media shall be destroyed by the physical destruction of that media.
- Records must be destroyed securely and completely.
- Recorded Destruction in formal documented processes, for data destruction within the "Organization".

4 Information Dissemination Policy

4.1 Introduction

This policy discuss the types of information that can be disseminated to internal and external groups, as well as the methods by which this information is disseminated. Moreover, this policy explains the specific type of information that will be disclosed and not to be disclosed.

- **Information not to be disclosed**
  - Personal information includes staff records, medical information, information on salary and benefits.
  - Financial information.
  - Legal, disciplinary or investigative matters; the concerned person shall be notified by official means.
  - Deliberative information including e-mail, notes, letters, memoranda, draft reports.
  - All of the confidential information.
- **Information to be disclosed in connection with other organizations**
  - Initial project abstracts.
  - Any information the “Organization” deems necessary for dissemination

4.2 Purpose

Is to ensure personal information and confidential information are protected from unauthorized use and disclosure and also to facilitate the identification of information to support routine disclosure and active

dissemination of information. This policy was also set to protect the intellectual property of "Organization".

4.3 Domain

This policy applies to all information produced, collected and stored by "Organization"

4.4 Policy

4.4.1 Information which is considered unrestricted can be open to the public and all employees as well as Third Parties.

4.4.2 Information which needs to be protected is accessed by authorized access such as employees, contractors and on a "need-to-know" basis for business related purposes. This access should be granted for a specific period required and set by higher level management.

4.4.3 Confidential information is limited to individuals in a specific function, group or role. pre clearance based on position is required in order to access confidential information held by "Organization".

4.4.4 In term of restricted information where access is granted to limited named individuals based on job position.

5 Access to Information Policy

5.1 Introduction

"Organization" will determine the extent to which security classification needs to be applied to information assets. The security classification of information assets should highlight what type of information can be viewed or accessed by members of "Organization" staff or external parties. The different levels of information particularly sensitive or confidential information will require higher level of authorization for access.

5.2 Purpose

The purpose of this policy is to limit the threat of losing or disclosing data that will affect the integrity, availability or confidentiality of data assets, by controlling the access to information with authorizations.

5.3 Domain

This policy applies to all reports, research information, and supporting documentation originally produced or collected by "Organization".

5.4 Policy

5.4.1 Authorized individuals only access current and complete information

5.4.2 Authorized users have access to and can use information when required.

5.4.3 Authorized individuals, entities or processes only access information and the value of intellectual property are protected as needed.

سياسة الاستخدام المقبول

1. مقدمة

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

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

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

2. الغرض من السياسة

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

3. النطاق

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

4. السياسة

4.1 الاستخدام العام والملكية

4.1.1 تمتلك **(جهة العمل)** البيانات المحفوظة على أجهزة الكمبيوتر والأجهزة الالكترونية الأخرى، المملوكة أو المستأجرة من قبل المؤسسة، أو من طرف ثالث، ويجب التأكد من خلال الوسائل القانونية أو التقنية أن معلومات الملكية محمية وفقًا لمعيار حماية البيانات.

4.1.2 تقع على عاتقك مسؤولية الإبلاغ عن سرقة أو فقدان أو كشف غير مصرح به عن معلومات الملكية المتعلقة بالمؤسسة.

4.1.3 يُسمح بالوصول إلى أو استخدام أو مشاركة معلومات الملكية فقط في حدود ما هو مصرح به وضروري للإيفاء بمتطلبات الوظيفة التي يتم التكليف بها.

4.1.4 كل موظف مسؤول عن تطبيق معايير الاستخدام الأمن للأجهزة الإلكترونية في إطار الوظيفة، كل إدارة مسؤولة عن وضع مبادئ توجيهية بشأن الاستخدام الشخصي الأمثل للأنظمة داخل المؤسسة، ويجب أن يسترشد الموظفون بسياسات الإدارة بشأن الاستخدام الشخصي، واستشارة مشرفيهم أو مدراءهم.

4.1.5 يجوز للأفراد المصرح لهم مراقبة المعدات والنظم وحركة الشبكة في أي وقت لأغراض الأمان وصيانة الشبكة وذلك وفقًا **لسياسة المراقبة وسياسة التدقيق.**

4.1.6 تحتفظ **(جهة العمل)** بحقها في التدقيق على الشبكات والأنظمة دوريًا لضمان الالتزام بهذه السياسة.

4.2 معلومات الملكية

4.2.1 كل الأجهزة المحمولة وأجهزة الكمبيوتر المملوكة للمؤسسة والتي تتصل بشبكة الانترنت يجب أن تلتزم بسياسة **التحكم في الوصول.**

4.2.2 يجب أن تتوافق كلمات المرور للأنظمة والمستخدم مع سياسة كلمة المرور، و يُحظر منح إمكانية الوصول إلى شخص آخر عمداً أو عن طريق عدم تأمين الوصول .

4.2.3 يجب تأمين جميع أجهزة الكمبيوتر باستخدام شاشة توقف محمية بكلمة مرور مع تعيين ميزة التنشيط التلقائي إلى 10 دقائق أو أقل، يجب عليك قفل الشاشة أو تسجيل الخروج عندما يكون الجهاز غير مراقب / غير مستخدم.

4.2.4 النشر عن طريق الموظفين باستخدام البريد الالكتروني للمؤسسة يجب أن يتضمن إخلاء للمسؤولية بأن رأيهم لا يمثل رأي (جهة العمل) وإنما يعبر عن وجهة نظرهم الشخصية إلا فيما يتعلق بمهام العمل.

4.3 الاستخدام غير المقبول

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

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

4.4 أنشطة النظام والشبكة

الأنشطة التالية محظورة تماماً، وبدون استثناءات:

4.4.1 انتهاكات حقوق أي شخص أو شركة محمية بحقوق النشر أو السر التجاري أو براءة الاختراع أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة، بما في ذلك على سبيل المثال لا الحصر، تركيب أو توزيع " برامج ليست مرخصة بشكل مناسب للاستخدام من قبل **(جهة العمل)**.

4.4.2 النسخ غير المصرح به للمواد المحمية بموجب حقوق الطبع والنشر، بما في ذلك على سبيل المثال لا الحصر، تحويل الصور الفوتوغرافية من المجلات أو الكتب أو غيرها من المصادر المحمية بحقوق النشر إلى صور رقمية وتوزيعها، وأيضاً مواد الوسائط المتعددة المحمية بحقوق النشر. . إلخ، وتثبيت أي برنامج محمي بموجب حقوق النشر والتي لا تمتلك (جهة العمل) أو المستخدم له ترخيص بذلك.

4.4.3 الموظفون المصرح لهم بالوصول إلى شبكة الانترنت يجب عليهم عدم استخدامها لتحميل برمجيات وألعاب، كما ينبغي عليهم عدم استغلالها في اللعب ضد خصوم على شبكة الانترنت.

4.4.4 الوصول إلى (البيانات أو الخادم أو الحساب) لأي غرض آخر غير القيام بأعمال تخص (جهة العمل)، حتى مع وجود تصريح بالدخول.

4.4.5 انتهاك لقوانين مراقبة التصدير المحلية والدولية عند القيام بتصدير البرمجيات أو المعلومات التقنية أو برامج أو تقنيات التشفير، ويستوجب استشارة الإدارة المناسبة قبل تصدير أي مادة محل شك.

4.4.6 استخدام أجهزة الكمبيوتر المملوكة للمؤسسة للانخراط بفاعلية في شراء أو نقل مواد تنتهك القانون.

4.4.7 تقديم عروض احتيالية من المنتجات أو العناصر أو الخدمات موجهة من حساب (جهة العمل).

4.4.8 التأثير على الخروقات الأمنية أو تعطيل اتصالات الشبكة، و تشمل الخروقات الأمنية ، على سبيل المثال لا الحصر.

الوصول غير المصرح للبيانات أو الولوج إلى الخادم أو الحساب بدون تصريح رسمي إذا لم يكن ذلك من واجبات

الوظيفة، أما تعطيل اتصالات الشبكة فيتضمن مثلاً، عملية مراقبه تدفق البيانات داخل الشبكة Network Sniffing، وعمليات حجب "الحرمان" من الخدمة (Distributed Denial of Service "DDOS")، والتلاعب في الحزمة البيانات (Packet spoofing) ومعلومات التوجيه المزورة لأغراض خبيثة.

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

4.4.10 القيام بتنفيذ أي شكل من أشكال مراقبة الشبكة التي من شأنها اعتراض البيانات غير المخصصة لمضيف Host المستخدم، ما لم يكن هذا النشاط جزءًا من المهام أو الأعمال الروتينية للموظف.

4.4.11 اجتياز عملية مصادقة المستخدم أو أمان أي مضيف أو شبكة أو حساب .

4.4.12 استخدام تقنيات مصائد مخترقي الشبكات honeypots أو أي تقنيات مشابهة في شبكة (جهة العمل) دون إذن.

4.4.13 التدخل في / أو رفض الخدمة لأي مستخدم غير مضيف Host الموظف (على سبيل المثال، هجمة رفض الخدمة denial of service attack).

4.4.14 استخدام أي برنامج/ نص / أمر، أو إرسال رسالة من أي نوع، بنية التدخل في / تعطيل جلسة عمل مستخدم ما بأي وسيلة، في الشبكة المحلية محلياً أو عبر (Internet/Intranet/Extranet) .

4.4.15 إفشاء معلومات عن/ قائمة بأسماء الموظفين إلى أي أطراف خارج (جهة العمل).

4.4.16 يجب تشفير الملفات التي تحتوي على بيانات حساسة خاصة ب(جهة العمل) والتي يتم نقلها بأي شكل عبر الإنترنت، كما هو محدد في سياسة أمن البيانات الموجودة.

4.5 أنشطة البريد الإلكتروني والاتصالات

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

4.6 التواصل الاجتماعي والتدوين / النشر الالكتروني

4.6.1 التدوين أو النشر الالكتروني من قبل الموظفين سواء كان ذلك باستخدام ممتلكات وأنظمة **(جهة العمل)** أو عبر أنظمة كمبيوتر خاصة يندرج أيضاً ضمن القيود المتعلقة بهذه السياسة، والاستخدام المحدود في مناسبات معينة لأنظمة **(جهة العمل)** للانخراط في التدوين مقبول، بشرط أن يكون بشكل محترف وأخلاقي ولا ينتهك سياسات **(جهة العمل)**، ولا يضر بمصالحها ولا يتداخل مع واجبات الوظيفة، والتدوين باستخدام أنظمة **(جهة العمل)** معرض للمراقبة.

4.6.2 سياسة سرية المعلومات ب(جهة العمل) تنطبق أيضاً على التدوين، حيث يُحظر على الموظفين الكشف عن أي معلومات حساسة خاصة ب(جهة العمل)، وكذا الأسرار التجارية والمهنية أو أي مواد تحت مظلة سياسة سرية المعلومات عن الانخراط في عمليات التدوين أو النشر الالكتروني.

4.6.3 يجب ألا ينخرط الموظفون في أي عملية تدوين أو نشر الكتروني يمكن أن تضر أو تشوه صورة وسمعة أو يمس كل ما يتعلق بالرضا عن مؤسسة ما، كما يُحظر على الموظفين نشر تعليقات تدل على تمييز، وإحراج، وإهانة، ومضايقة أو تبنى أي سلوك الكتروني من السلوكيات المحظورة.

4.6.4 على الموظفين عدم نسب تصريحات شخصية أو آراء أو معتقدات لـ(جهة العمل) عند الانخراط في عمليات تدوين أو نشر الكتروني، و إذا قام موظف ما بالتعبير عن رأي ما أو معتقد خاص به فلا يمكنه بأي حال من الأحوال أن يتحدث بصفة موظف في (جهة العمل) أو ممثلاً لها صراحةً أو ضمنياً، كما يجب على الموظف أن يضع في الاعتبار المخاطرة التي تتضمنها عملية التدوين /النشر الالكتروني.

4.6.5 وبغض النظر عن أهمية اتباع جميع القوانين المتعلقة بمناولة المواد الخاضعة لحقوق النشر الخاضعة للرقابة والكشف عنها، كما لا يجوز أيضًا استخدام العلامات التجارية والشعارات وأية ملكية فكرية أخرى خاصة ب(جهة العمل) فيما يتعلق بأي نشاط تدوين أو نشر الكتروني .

Acceptable Use Policy

1. Overview

Information security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to **(Organization)**'s established culture of openness, trust and integrity. Information Security Department is committed to protecting **(Organization)**'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of **(Organization)**. These systems are to be used for business purposes in serving the interests of the **(Organization)**, and of clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every **(Organization)** employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at **(Organization)**. These rules are in place to protect the employee and **(Organization)**. Inappropriate use exposes **(Organization)** to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct **(Organization)** business or interact with internal networks and business systems, whether owned or leased by **(Organization)**, the employee, or a third party.

4. Policy

4.1 General Use and Ownership

4.1.1 **(Organization)** proprietary information saved on electronic and computing devices whether owned or leased by **(Organization)**, the employee or a third party, remains the sole property of **(Organization)**. You must ensure through legal or technical means that proprietary information is protected in accordance with the ***Data Protection Standard***.

4.1.2 You have a responsibility to report the theft, loss or unauthorized disclosure of **(Organization)** proprietary information.

4.1.3 You may access, use or share **(Organization)** proprietary information only to the extent it is authorized and necessary to fulfill your assigned job requirements.

4.1.4 Every Employee is responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within **(Organization)** may monitor equipment, systems and network traffic at any time, per **Monitoring and Audit Policies**.

4.1.6 **(Organization)** reserves the right to audit networks and systems periodically to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the **Access control Policy.**

4.2.2 System level and user level passwords must comply with the **Password Policy**. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a **(Organization)** email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily representing the **(Organization)**'s opinions, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, banned. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of **(Organization)** authorized to engage in any activity that is illegal under local, state, local or international law while utilizing **(Organization)**-owned resources.

The lists below are by no means extensive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly banned, with no exceptions:

4.4.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution software products that are not appropriately licensed for use by **(Organization)**.

4.4.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted multimedia material .. etc, and the installation of any copyrighted software for which (Organization) or the end user does not have an active license is strictly prohibited. Accessing data, a server or an account for any purpose other than conducting (Organization) business, even if you have authorized access, is prohibited.

4.4.3 Accessing data, a server or an account for any purpose other than conducting (Organization) business, even if you have authorized access, is prohibited.

4.4.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.4.5 Using the (Organization)'s computing asset to actively engage in procuring or transmitting material that is in violation of any harassment or hostile workplace laws in the user's local jurisdiction.

4.4.6 Making fraudulent offers of products, items, or services originating from any (Organization) account.

4.4.7 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.4.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.4.9 Port scanning or security scanning is expressly prohibited unless prior notification to Information Security Department is made.

4.4.10 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.4.11 Circumventing user authentication or security of any host, network or account.

4.4.12 Introducing honeypots, honeynets, or similar technology on the (Organization) network with no permission.

4.4.13 Interfering with /or denying service to any user other than the employee's host (for example, denial of service attack).

4.4.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.

4.4.15 Providing information about, or lists of, (Organization) employees to parties outside (Organization).

4.4.16 Files containing sensitive (Organization) data, as defined by existing Data Classification and Data Security Policy, which are transferred in any way across the Internet should be encrypted.

4.5 Email and Communication Activities

Email is essential to the everyday jobs. (Organization) want to ensure that the employees understand the limitations of using their corporate email accounts. The Acceptable use of email helps employees use their company email addresses appropriately, as defined in the e-mail usage policy.

4.6 Blogging and Social Media

4.6.1 Blogging by employees, whether using **(Organization)**'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of **(Organization)**'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate **(Organization)**'s policy, is not detrimental to **(Organization)**'s best interests, and does not interfere with an employee's regular work duties. Blogging from **(Organization)**'s systems is also subject to monitoring.

4.6.2 (Organization)'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any (Organization) confidential or proprietary information, trade secrets or any other material covered by (Organization)'s Confidential Information policy when engaged in blogging.

4.6.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of (Organization) and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

4.6.4 Employees may also not attribute personal statements, opinions or beliefs to (Organization) when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of (Organization). Employees assume any and all risk associated with blogging.

4.6.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, (Organization)'s trademarks, logos and any other (Organization) intellectual property may also not be used in connection with any blogging activity.

سياسات المستخدم

1. سياسة كلمة السر/المرور

1.1 مقدمة

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

1.2 الغرض من السياسة

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

1.3 النطاق

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

1.4 السياسة

1.4.1 فرض كلمة مرور قوية: يجب ان تكون كلمة المرور قوية ولا تتضمن في تركيبها الكلمات التي يسهل على الاخرين إيجادها.

1.4.1.1 يجب استخدام توليفة من الأحرف الكبيرة والصغيرة، مع أرقام، ورموز أو علامات الترقيم قدر الامكان عند اختيارك لكلمة السر/المرور.

1.4.1.2 لا يجب استخدام كلمات سر رائجة والتي يمكن التكهن بها بسهولة، كالأسماء وتاريخ الميلاد أو أرقام الهواتف.

1.4.1.3 يجب ان لا يقل عدد رموز كلمة السر/المرور عن 12 رمزاً.

1.4.1.4 لا يجب استعمال اسم المستخدم في كلمة السر.

1.4.1.5 لا يجب استخدام أرقاماً أو حروف متكررة مثل (3333 او AAAA).

1.4.1.6 في حالة اختيار كلمة تقليدية يفضل خلط حروفها بحيث لا تعطي معني متعارف عليه.

1.4.1.7 يفضل ان تكون كلمة المرور "جملة مرور" لا يفهمها الا المستخدم، مُكونة من تركيبة الاحرف والأرقام والرموز.

1.4.1.8 تطبيق ضوابط صارمة على كلمات المرور على مستوى النظام وكلمة مرور الحسابات المشتركة.

1.4.2 يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها.

1.4.2.1 يجب التعامل مع جميع كلمات المرور في **(جهة العمل)** على أنها بيانات سرية.

1.4.2.2 لا يحتفظ بكلمات المرور كنص عادي يمكن قراءته، وإنما يتم حفظ كلمات السر على شكل نص مشفر لا يمكن فكه او استخدامه من الشخص المخول.

1.4.2.3 يجب ألا يتم تخزين كلمات المرور على أنظمة الكمبيوتر في شكل غير محمي.

1.4.2.4 كلمات المرور للأنظمة (جذر النظام/مسؤول النظام Root/Administrator) يجب ان تخزن باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.

1.4.2.5 يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وادخال البيانات في كل مرة من جديد.

1.4.3 الحفاظ على سرية كلمات المرور: يجب عدم مشاركة أو كشف كلمة المرور مع أي شخص لأي سبب من الأسباب.

1.4.3.1 يجب عدم أفشاء كلمة المرور وعدم كتابتها بطريقة صريحة مما يجعلها عرضة للاطلاع أو حتى التلميح عن تركيبتها، إلا في حالةِ الضرورةِ القصوى ويجب تغييرها بعد الكشف عنها.

1.4.3.2 يجب اخد الحذر من الاشخاص المتطفلين عند طباعة لكلمة السر/المرور أثناء عملية الولوج.

1.4.3.3 يمنع إرسال كلمة المرور عبر البريد الالكتروني أو من خلال اي وسيلة عبر الانترنت.

1.4.3.4 يجب تغيير كلمات المرور اذا ظهر أي مؤشر على احتمال اختراق للنظام أو لكلمة المرور.

1.4.3.5 يجب تغيير كلمات المرور المستخدمة للحسابات المشتركة على الفور في حالة اختراقها أو عندما يغادر مالكها **(جهة العمل)**.

1.4.3.6 لا يجب استخدام نفس كلمة المرور لحسابات المسؤولين المتعددة.

1.4.3.7 يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في **(جهة العمل)**.

1.4.3.8 يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والاجهزة داخل **(جهة العمل)** والحسابات والاجهزة الاخرى خارجها.

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

1.4.4.1 على المستخدم تغيير كلمة المرور الأولية التي يستلمها من الجهة المختصة في أول استخدام له وقبل انتهاء وقت صلاحيتها؛ وذلك لضمان عدم تسريب كلمة السر لمستخدمين آخرين.

1.4.4.2 يجب إعطاء كلمات المرور المؤقتة للمستخدمين بطريقة آمنة؛ ينبغي تجنب نقلها على ورقة مكشوفة (نص عادي) او عن طريق أطراف ثالثة أو رسائل البريد الإلكتروني غير المحمية (النص الواضح) .

1.4.4.3 وضع إجراءات للتحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة أو بديلة أو مؤقتة.

1.4.4.4 يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقتة.

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

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

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

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

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

سياسة استعمال البريد الإلكتروني

2.1 مقدمة

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

2.2 الغرض من السياسة

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

2.3 النطاق

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

2.4 السياسة

2.4.1 حساب البريد الالكتروني

2.4.1.1 يمنح كل موظف حساب بريد إلكتروني، ويجب أن يكون محدد بشكل فريد لكل مستخدم.

2.4.1.2 عند إنشاء بريد إلكتروني جديد للمستخدم، يجب على المستخدم تغيير كلمة المرور الأولية الخاصة به في تسجيل الدخول التالي، حيث يجب تكوين النظام يفرض على المستخدمين تغيير كلمات المرور الأولية الخاصة بهم.

2.4.1.3 يجب أن تكون كلمة مرور البريد الإلكتروني الخاصة بالمستخدم تتوافق مع **سياسة كلمة المرور** الصادرة عن**(جهة العمل)**.

2.4.1.4 يجب التحكم في حجم صندوق البريد من خلال تحديد سعة الحصة المخصصة، وكل مستخدم مسؤول إذا تجاوز السعة المحدودة، لذا يجب على المستخدم أرشفة الرسائل المهمة بشكل دوري وحذفها من البريد الوارد.

2.4.2 استخدام البريد الالكتروني

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

2.4.2.1 يجب أن يكون استخدام البريد الإلكتروني متوافقاً مع سياسات **(جهة العمل)** وإجراءاتها ومع القوانين المعمول بها والممارسات السليمة والامتثال للقوانين المعمول بها.

2.4.2.2 يجب استخدام حسابات البريد الإلكتروني لـ**(جهة العمل)** لأعمال تتعلق بـ**(جهة العمل)**، حيث يستخدم لمساعدة الموظفين في تأدية وظائفهم.

2.4.2.3 لا ينبغي استخدام البريد الإلكتروني المخصص للموظف لأغراض شخصية.

2.4.2.4 يجب تأمين جميع بيانات **(جهة العمل)** الواردة في رسالة بريد إلكتروني أو مرفق طبقًا لسياسة **حماية البيانات**.

2.4.2.5 يجب توخي الحذر عند إرفاق المستندات أو الملفات بالبريد الإلكتروني، فقد تكون هذه المرفقات تابعة للآخرين، وإعادة توجيه هذه البيانات إلى مستلم آخر دون الحصول على إذن من المرسل قد يعتبر انتهاكاً لحقوق الطبع والنشر.

2.4.2.6 يجب على جميع المستخدمين توخي الحذر عند فتح رسائل البريد الإلكتروني والمرفقات من مصادر غير معروفة.

2.4.2.7 يجب على جميع المستخدمين ضمان أن يكون محتوى البريد الإلكتروني دقيقًا وواقعيًا وموضوعيًا، حيث يجب تجنب الآراء الشخصية حول الأفراد أو المؤسسات الأخرى.

2.4.2.8 يجب أن يدرك المستخدمون أن رسائل البريد الإلكتروني قد تخضع للتدقيق للتأكد من أنها تلبي متطلبات هذه السياسة. ينطبق هذا على محتوى الرسائل والمرفقات والعناوين ورسائل البريد الإلكتروني الشخصية.

2.4.2.9 تعتبر جميع الرسائل المرسلة عبر نظام البريد الإلكتروني الخاص لـ**(جهة العمل)** ملكية خاصة بـ**(جهة العمل)** وتشمل رسائل البريد الإلكتروني الشخصية أيضاً. يجب ألا يكون لدى المستخدم أي توقع للخصوصية في أي شيء يقوم بإنشائه أو تخزينه أو إرساله أو استلامه على نظام البريد الإلكتروني الخاص بـ**(جهة العمل)**.

2.4.2.10 يمكن مراقبة الرسائل الإلكترونية دون إخطار مسبق إذا رأت **(جهة العمل)** ذلك ضروريًا. إذا وجد دليل على أن الموظف لا يلتزم بالتوجيهات المنصوص عليها في هذه السياسة، تحتفظ **(جهة العمل)** بالحق في اتخاذ إجراءات تأديبيه وفق اللوائح المعمول بها.

2.4.2.11 يجب انتقاء الألفاظ اللائقة وعدم كتابة أي لفظ مسيء او مهين للآخر.

2.4.2.12 يجب على المستخدمين عدم الإفصاح عن كلمات المرور الخاصة بحساباتهم أو السماح لأي شخص آخر باستخدام حساباتهم، كما يجب عدم استخدام حساب مستخدم آخر.

2.4.2.13 في الحالات التالية **(الاستقالة، الفصل/الطرد، الإيقاف)** سوف يتم أعلام الموظف بأنه سيتم قفل حساب بريده الالكتروني ومنحه فرصة محددة لنسخ وأرشفة محتويات بريده.

2.4.2.14 يجب على من يتعرف على أو يلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بقسم أمن المعلومات في **(جهة العمل)** والابلاغ بشكل فوري.

2.4.2.15 إرفاق كل رسالة بتوقيع نصي في النهاية يحمل الاسم والوظيفة ورقم الهاتف والقسم التابع له واسم **(جهة العمل)**.

2.4.2.16 على المستخدم أخذ العلم والدراية أنه المسؤول الوحيد عما تحتويه الرسائل المرسلة من خلال حساب بريده الإلكتروني.

2.4.2.17 يجب على المستخدمين ضمان إرسال رسائل البريد الإلكتروني إلى المستخدمين الذين يحتاجون إلى معرفة الأمر فقط.

2.4.3 الاستخدام الغير مقبول للبريد الالكتروني

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

2.4.3.1 استخدام نظام البريد الإلكتروني لـ**(جهة العمل)** لإنشاء أو توزيع أي رسائل مدمرة أو هجومية. يجب على الموظفين الذين يتلقون أي رسائل بريد إلكتروني بهذا المحتوى من أي موظف بـ**(جهة العمل)** إبلاغ الأمر إلى المسؤول على الفور.

2.4.3.2 استخدام حساب البريد الإلكتروني لـ**(جهة العمل)** لتسجيل الدخول في أي من مواقع الشبكات الاجتماعية ما لم يكن ذلك لأغراض العمل، كما يجب الحصول على موافقة من الإدارة العليا لذلك.

2.4.3.3 استخدام هوية مزيفة في رسائل البريد الإلكتروني الخاصة بـ**(جهة العمل)**.

2.4.3.4 العبث بمحتوي وعناوين الرسائل المعاد توجيهها أو مرفقاتها بدون توضيح ذلك بشكل صريح.

2.4.3.5 إرسال رسائل بريد الكتروني غير مرغوب فيها بما في ذلك إرسال "بريد غير هام" JUKE MAIL ، أو مواد إعلانية إلى أفراد لم يطلبوها تحديداً كـ (رسائل البريد الالكتروني المزعج SPAM).

2.4.3.6 استخدام غير مصرح به لمعلومات البريد الالكتروني أو تزويرها .

2.4.3.7 إنشاء أو إجراء تحويل لـ "سلسلة رسائل chain letters "، "بونزي Ponzi " ، أو أي أشكال هرمية من أي نوع .

2.4.3.8 استخدام رسائل بريد غير مرغوب بها داخل شبكات (جهة العمل) لمزودي خدمات آخرين نيابة عن أو للدعاية لأي خدمة مستخدمة من قبل (جهة العمل) أو متصلة عبر شبكتها .

2.4.3.9 نشر الرسائل غير ذات العلاقة بالعمل أو ما شابه ذلك لعدد كبير من مجموعات الأخبار newsgroups أو مايسمى بـ (newsgroup spam).

2.4.3.10 تغيير محتوى و/أو عناوين البريد الإلكتروني للرسائل المعاد توجيهها أو مرفقاتها دون الحصول على موافقة.

3. سياسة استخدام الانترنت

3.1 مقدمة

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

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

3.2 الغرض

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

3.3 النطاق

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

3.4 السياسة

3.4.1 استخدام الموارد

3.4.1.1 يتم الموافقة على الوصول إلى الإنترنت فقط إذا تم تحديده ضمن احتياجات العمل. يتم منح خدمات الإنترنت على أساس مسؤوليات الوظيفة الحالية للموظف.

3.4.1.2 ستقوم إدارات **(جهة العمل)** بمراجعة متطلبات وصول المستخدمين إلى الإنترنت بشكل دوري لضمان استمرار احتياجهم للإنترنت.

3.4.1.3 يصرح لمستخدمي الانترنت في **(جهة العمل)** باستخدامها لأغراض تخص العمل وبطريقة لا تخالف الأنظمة واللوائح المعمول بها في **(جهة العمل)**، أو بما يؤدي إلى الإضرار بها او بسمعتها.

3.4.1.4 لا تكفل (جهة العمل) دقة المعلومات التي يتم الحصول عليها عن طريق الإنترنت، ذلك يقع على عاتق مصدر ومنتج هذه المعلومات.

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

3.4.2 الاستخدام المسموح

3.4.2.1 التواصل بين الموظفين وغير الموظفين لأغراض العمل.

3.4.2.2 ما يقوم به فني دعم تكنولوجيا المعلومات من تنزيل لتحديثات البرامج والتصحيحات.

3.4.2.3 استعراض مواقع الويب للبائعين المحتملين للحصول على معلومات عن المنتجات.

3.4.2.4 مراجعة المعلومات التنظيمية أو البيانات الفنية.

3.4.2.5 إجراء الابحاث

3.4.3 الاستخدام الشخصي

3.4.3.1 قد يُعد استخدام اجهزة كمبيوتر **(جهة العمل)** للوصول إلى الإنترنت لأغراض شخصية، دون موافقة مدير المستخدم وقسم تكنولوجيا المعلومات، سببًا لاتخاذ إجراءات تأديبيه حسب اللوائح المعمول بها.

3.4.3.2 يجب أن يكون جميع مستخدمي الإنترنت مدركين أن شبكة **(جهة العمل)** تقوم بإنشاء سجل تدقيق يبين طلب الخدمة، سواء في العناوين الداخلية أو الخارجة، حيث يتم مراجعتها هذه السجلات بشكل دوري.

3.4.3.3 المستخدمون الذين يختارون تخزين أو نقل المعلومات الشخصية مثل المفاتيح الخاصة أو أرقام بطاقات الائتمان أو الشهادات أو الاستفادة من "محافظ" الإنترنت يقومون بذلك على مسؤوليتهم الخاصة. **(جهة العمل)** ليست مسؤولة

عن أي فقدان للمعلومات، مثل المعلومات المخزنة في المحفظة، أو أي ما قد ينتج من خسائر لاحقة للممتلكات الشخصية.

3.4.3.4 المستخدم مسؤول مسؤولية كاملة عن أجهزة الكمبيوتر الخاصة به واستخدامها، وعليه أن يكون على دراية بأمن وحفظ موارد تكنولوجيا المعلومات.

3.4.3.5 يجب على المستخدمين الذين يتعرفون على أو يلاحظون وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بالقسم المختص في(جهة العمل) والابلاغ بشكل فوري.

3.4.4 الاستخدام المحظور

3.4.4.1 يمن منعاً باتاً استخدام الانترنت أو استغلالها بطريقة تعرض شبكة **(جهة العمل)** للخطر، أو فتح ثغرات أمنية في الشبكة أو نشر برمجيات ضارة أو غير مشروعة.

3.4.4.2 لا يجوز انتحال شخصية الاخرين أو جهاز آخر.

3.4.4.3 يمنع استخدام اسم **(جهة العمل)** أو أي من أقسامها أو أي من موظفيها دون إذن كتابي رسمي.

3.4.4.4 يمنع العبث بالمعلومات الخاصة بموظفين آخرين أو بجهات أخرى أو الاطلاع عليها بشكل غير قانوني.

3.4.4.5 يمنع نشر المعلومات الخاصة بـ **(جهة العمل)** أو الخاصة بالآخرين دون إذن صريح بذلك.

3.4.4.6 يمنع محاولة فك تشفير بيانات الآخرين في الأنظمة المعلوماتية بدون تصريح رسمي من الجهة المعنية.

3.4.4.7 لا يجوز الإخلال بأي من حقوق النشر أو التأليف، أو حقوق الملكية الفكرية لأي بيانات، تطبيقات، برامج أو معلومات.

3.4.4.8 يمنع مراقبة الاتصالات الإلكترونية للمستخدمين الآخرين لغرض التجسس وانتهاك الخصوصية.

3.4.4.9 لا يجوز استخدام الانترنت بشكل يؤثر سلباً على المستخدمين الآخرين، أو على أداء الأجهزة والشبكات.

3.4.4.10 يمنع استخدام الانترنت لأي أغراض غير قانونية أو غير شرعية. ومن الأمثلة على ذلك إرسال مواد عنيفة أو تهديدية أو خداعية أو إباحية أو فاحشة أو غير قانونية أو غير شرعية والذي يمكن أن يتسبب في أي تهديد، أو تخريب، أو إزعاج، أو مضايقة لأي شخص أو جهة أو أمنها السيبراني.

3.4.4.11 يمنع إهدار الموارد المعلوماتية، أو إحداث أي تغيير في الموارد المعلوماتية دون امتلاك صلاحية تخول ذلك.

3.4.4.12 يمنع إنشاء موقع الكتروني أو حساب على مواقع التواصل الاجتماعي يمثل (**جهة العمل**)، أو إدارتها أو أي جزء منها دون إذن كتابي رسمي من صاحب الصلاحية.

3.4.4.13 عدم استخدام قنوات اتصال بالموارد المعلوماتية الأخرى أو الارتباط بها إلا من خلال القنوات المتاحة والمصرح بها رسمياً من **(جهة العمل)**.

3.4.4.14 يمنع استخدام الموارد المعلوماتية بشكل يؤدي إلى إهدار وقت الموظف.

3.4.4.15 يجب عدم استخدام الاتصال بالإنترنت الخاص بـ **(جهة العمل)** لأغراض تجارية أو سياسية، أو بهدف تحقيق ربح شخصي أو تجاري أو تسويقي.

3.4.4.16 يمنع إنشاء نسخ الكترونية غير مصرح بها من المستندات والوثائق التي تخص **(جهة العمل)** وإداراتها او لأي مواد محمية بحقوق نشر لغرض نشرها أو إرسالها عبر شبكة (**جهة العمل**).

4. سياسة أمان محطات العمل (الكمبيوتر وملحقاته)

4.1 مقدمة

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

4.2 الغرض من السياسة

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

4.3 النطاق

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

4.4 السياسة

4.4.1 يسمح للمستخدم باستعمال أجهزة الكمبيوتر المخصصة له، أو التي المصرح له باستعمالها. ولا يجوز استخدام أجهزة الآخرين، أو محاولة الدخول عليها.

4.4.2 تقع المسؤولية الكاملة على المستخدم للاستخدام الملائم لجميع الموارد المخصصة له بما فيها من اجهزة الكميوتر وملحقاتها أو برمجيات الأجهزة.

4.4.3 لا يسمح للمستخدمين بالوصول إلى الشبكة باستخدام الحواسيب الشخصية واللوحية والهواتف الذكية. الا بتصريح من الادارة الفنية المختصة.

4.4.4 يجب عدم محاولة الوصول إلى أجزاء ممنوعة الوصول من الشبكة، مثل نظام التشغيل الرئيسي، برامج الأمان وغيرها دون الموافقة من الادارة المختصة.

4.4.5 يجب عدم وضع أو تنصيب أو استخدام أي برامج أو أدوات أو أجهزة قد تؤدي إلى أو تساعد على تلف البرامج أو الأجهزة أو مكونات النظام.

4.4.6 يمنع تثبيت أو استخدام الأدوات التي عادةً ما تستخدم لمهاجمة أنظمة الأمن أو اختراق أنظمة الكمبيوتر أو الشبكات الأخرى (مثل كاشفات كلمات السر أو ماسحات الشبكة... إلخ).

4.4.7 يجب احترام الخصوصية الشخصية وحقوق الآخرين وعدم الحصول على بيانات تخص مستخدم آخر، إضافة إلى البرامج أو الملفات الأخرى من دون إذن مسبق.

4.4.8 يطلب موافقة خاصة من قسم تقنية المعلومات قبل تنصيب أي برامج أو تركيب أجهزة خاصة على أنظمة **(جهة العمل)**.

4.4.9 أجهزة الكمبيوتر تعتبر اعارة من **(جهة العمل)** لذا فهي للاستخدام الرسمي لـ**(جهة العمل)** فقط ولا يجوز استخدامها من قبل أفراد الأسرة أو الأصدقاء تحت أي ظرف من الظروف.

4.4.10 عند إرجاع جهاز الكمبيوتر، تحتفظ إدارة تقنية المعلومات بالحق في تنظيف القرص الثابت من أي بيانات وإعادة تثبيت كافة البرامج المبدئية. المستخدم مسؤول عن أي بيانات يتركها على الكمبيوتر المحمول عند إعادتها إلى **(جهة العمل)**.

4.4.11 تحتفظ إدارة تكنولوجيا المعلومات بحقها في استرجاع جميع المعدات التي تم اعارتها للمستخدمين من أجل إجراء تحديثات وتحسينات للبرامج، و / أو استبدال أو تحديث الأجهزة في أي وقت.

4.4.12 لا يقوم موظفو ادارة تقنية المعلومات بالدخول (login) للأجهزة الشخصية لأعمال الصيانة الا بعد اخذ الاذن من صاحب العلاقة مباشرة.

4.4.13 اجهزة الكمبيوتر وملحقاتها موجودة لخدمة الموظفين والمستخدمين لأداء الأعمال بطريقة أفضل، وعليه فإنه ليس من الممكن استغلالها لأغراض شخصية.

4.4.14 توفر **(جهة العمل)** مجموعة واسعة من الطابعات المتصلة بالشبكة للمساعدة في اداء اعمال **(جهة العمل)**، كما يُسمح بطابعات سطح المكتب الفردية، وسيتم دعمها من قِبل قسم تقنية المعلومات.

4.4.15 يحظر على موظفي **(جهة العمل)** شراء معدات الشبكات الخاصة بهم، بما في ذلك على سبيل المثال لا الحصر: بطاقات الشبكة المحلية والبطاقات اللاسلكية وأجهزة التوجيه والمبدلات وتوصيل كابلات الشبكة والطابعات الجاهزة للربط بالشبكة.

4.4.16 يعتبر استقرار الشبكة أمرًا بالغ الأهمية في بيئة **(جهة العمل)**، وقد تؤدي إضافة معدات الشبكة غير المصرح بها لشبكة **(جهة العمل)** إلى حدوث مشكلات يصعب تشخيصها.

4.4.17 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.

4.4.18 لا يجب تخزين أي وثائق أو ملفات لا علاقة لها بالعمل في المساحات المخصصة للموظفين على الخادم المخصص لذلك.

4.4.19 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.

4.4.20 لا يسمح لأي شخص من خارج **(جهة العمل)** باستخدام حواسيب **(جهة العمل)** إلا بإذن كتابي رسمي.

4.4.21 يجب على المستخدم عدم ابطال عمل برامج مكافحة الفيروسات والبرامج الخبيثة على اجهزة كمبيوتر **(جهة العمل)**، كما يجب ان يتم فحص وسائل تخزين البيانات (مثل الأقراص المضغوطة أو محركات الأقراص الثابتة أو ذاكرة الفلاش) قبل فتح أي ملف أو برنامج.

4.4.22 يحظر على المستخدمين نسخ أية مواد أو برامج من اجهزة الكمبيوتر الخاصة بـ **(جهة العمل)** لتوزيعها خارجها دون موافقة خطية وصريحة.

User Policies

1. Password Policy

1.1 Introduction

Password is an important information security component. They are used for user authentication to prove identity or access approval to gain access to a resource, and used in many ways to protect users, data, systems, and network, and also used to protect files and other stored information from access from unauthorized individuals both internally and externally.

Since strong passwords one of the effective security controls, and given the need of passwords for high-priority matters, this requires strong, highly encrypted passwords so that would be hard to predict.

1.2 Purpose

To provide a set of minimum security standards governing the use of passwords for **(Organization)** information technology systems.

1.3 Domain

This policy applies to all **(Organization)** Staff.

This policy applies to all username and password pairs on all devices, systems and applications that are part of the **(Organization)** network that provide access to **(Organization)** owned information.

1.3 Policy

1.4.1 Enforce strong passwords

1.4.1.1 Passwords should be at least 12 positions in length.

1.4.1.2 All users must choose passwords that cannot be predicted easily. It should be a combination of the four available character types: Alphabetic, Combination of both upper and lower case letters, Numeric: 0 to 9, and Special Characters.

1.4.1.3 Users shouldn't use popular, easily predictable passwords, such as names, birthdays, or phone numbers.

1.4.1.4 Users shouldn't use their username in the password.

1.4.1.5 Password shouldn't be repeated numbers or characters such as (3333 or AAAA).

1.4.1.6 In case of using a common word, users should mix the characters, so it doesn't give a clear meaning.

1.4.1.7 Implement strict controls for system-level and shared service account passwords.

1.4.2 Passwords must be stored in a secure manner to ensure not to be detected

1.4.2.1 All passwords should be treated as sensitive, confidential information at **(Organization)**.

1.4.2.2 Users shouldn't write password down or store it in an insecure manner anywhere in the office, and shouldn't store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

1.4.2.3 Passwords should never be stored on computer systems in an unprotected form.

1.4.2.4 System level passwords (e.g. Root, Administrator) must be stored within an encrypted password vault.

1.4.2.5 Users shouldn't use "Remember Password" feature of applications.

1.4.3 Keep passwords confidential: Password mustn't be shared with anyone for any reason.

1.4.3.1 Passwords should not be shared or disclosed, and shouldn't be written in an explicit manner, and it should be changed immediately in case of disclosure.

1.4.3.2 During access to accounts, users should be aware of obtrusive people while typing password.

1.4.3.3 Users shouldn't send passwords via email or any other media via the internet.

1.4.3.4 Users should change passwords whenever there is any indication of possible system or password compromise

1.4.3.5 Passwords used for shared accounts should be changed immediately if compromised or when a holder transfers or leaves the **(Organization)**.

1.4.3.6 Users shouldn't use the same password for multiple administrator accounts.

1.4.3.7 Where possible, users must not use the same password for various **(Organization)** access needs.

1.4.3.8 Users must not use the same password for **(Organization)** accounts and devices as for other non- **(Organization)** access.

1.4.4 Initial passwords: Users must require a change of the initial passwords they receive, and force expiration of initial passwords.

1.4.4.1 Users must change their initial passwords they receive and before expiration; in order to ensure that passwords not to be leaked to other users.

1.4.4.2 Temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided, and it shouldn't be transmitted in plain-text.

1.4.4.3 Users should acknowledge receipt of initial passwords.

1.4.4.4 Establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password.

1.4.5 Require screening of new passwords against lists of commonly used or compromised passwords.

1.4.6 Access to internal and private systems must be prevented after 3 false attempts within a period of time not exceeding 15 minutes. Prevention lasts for a minimum of 30 minutes and a maximum of 3 hours.

1.4.7 Users should be required to sign a statement to keep personal passwords confidential; this signed statement could be included in the terms and conditions of employment.

1.4.8 All users are responsible for reporting any suspected misuse of passwords. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

1.4.9 All users must be aware that they are solely responsible for protecting their password.

2. Email Usage Policy

2.1 Introduction

E-mail is the primary communication tool in most business areas for its speed and efficiency, and because it is an expressive reliable tool, misuse of it can post many legal, privacy and security risks. Thus it's necessary to develop a policy to understand the appropriate use of email to avoid such problems. This policy outlines the minimum requirements for use of email within **(Organization)** Network.

2.2 Purpose

The purpose of this policy is to ensure the proper use of **(Organization)** email system and make users aware of what **(Organization)** deems as acceptable and unacceptable use of its email system, and to ensure that every user has a responsibility to maintain the **(Organization)**'s image, to use it in a productive manner and to avoid placing the **(Organization)** at risk of legal liability based on their use.

2.3 Scope

This policy applies to all employees, vendors, and agents operating on behalf of **(Organization)**, and to the Email system in use within **(Organization)**.

2.4 Policies

2.4.1 Email Account

2.4.1.1 Every employee is granted an email account, and it must be uniquely identifiable.

2.4.1.2 When creating a new user email, the user must be enforced to change his/her password at next logon. The system must be configured to enforce the users to change their passwords.

2.4.1.3 All user emails must have a password that complies with **(Organization)**'s Password Policy.

2.4.1.4 Email box size must be controlled by a quota, and every user is responsible if they exceed the limited capacity, users must periodically archive the important mail and delete them from the inbox.

2.4.2 Use of email

All users must adhere to the following when using **(Organization)** E-mail facilities:

2.4.2.1 The use of email must be compliant with **(Organization)** policies and procedures and with the applicable laws and proper business practices.

2.4.2.2 **(Organization)** email accounts should be used only for **(Organization)** business-related purposes to help employees in their job duties.

2.4.2.3 The e-mail address allocated to an employee should not be used for personal purposes.

2.4.2.4 All **(Organization)** data contained within an email message or an attachment must be secured according to the **Data Privacy Policy**.

2.4.2.5 Great care must be taken when attaching documents or files to an email. Letters, files and other documents attached to emails may belong to others. By forwarding this information, without permission from the sender, to another recipient user may be liable for copyright infringement.

2.4.2.6 All users should be cautious when opening e-mails and attachments from unknown sources.

2.4.2.7 All users should ensure that email content is accurate, factual and objective. Users should avoid subjective opinions about individuals or other organizations.

2.4.2.8 Users should be aware that e-mails may be subject to audit to ensure that they meet the requirements of this policy. This applies to message content, attachments and addresses and to personal e-mails.

2.4.2.9 All messages distributed via **(Organization)**'s email system, even personal emails, are **(Organization)** property. User must have no expectation of privacy in anything that they create, store, send or receive on the **(Organization)**'s email system.

2.4.2.10 Emails can be monitored without prior notification if **(Organization)** deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, **(Organization)** reserves the right to take disciplinary action in accordance with the applicable regulations.

2.4.2.11 It is necessary to select the appropriate words and not to write any offensive or insulting words.

2.4.2.12 Users should not disclose account passwords or allow anyone else to use their accounts, and shouldn't use another user account.

2.4.2.13 In the following cases (resignation, dismissal, suspension), user will be informed that email account will be locked and given timed opportunity to copy and archive the email contents.

2.4.2.14 If recognizing or noticing an actual or suspected security issue, users must contact the Information Security Department and report immediately.

2.4.2.15 Attach each email with a text signature with the name, job, telephone number, department and the name of **(Organization)**.

2.4.2.16 The user should be aware that he / she is solely responsible for the contents of the messages sent through his / her email account.

2.4.2.17 Users must ensure that email messages are sent only to users who need to know the information in the email content.

2.4.3 Unacceptable Use of E-Mail

2.4.3.1 The **(Organization)** email system shall not to be used for the creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any **(Organization)** employee should report the matter to their supervisor immediately.

2.4.3.2 Use **(Organization)** email account to sign in any of social media websites unless for a business related purposes, and must have an approval from higher management.

2.4.3.3 Using a false identity in **(Organization)** emails.

2.4.3.4 Tampering with email content or addresses of redirected messages or attachments without getting an approval.

2.4.3.5 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Spam Emails).

2.4.3.6 Unauthorized use, or forging, of email header information.

2.4.3.7 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

2.4.3.8 Use of unsolicited email originating from within **(Organization)**'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by **(Organization)** or connected via **(Organization)**'s network.

2.4.3.9 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (Newsgroup Spam).

2.4.3.10 Changing content and / or email addresses of the forwarded emails or their attachments without getting an approval.

3 Internet Usage Policy

3.1 Introduction

Internet is now the most utilized source of information, it provides access to endless sources of data, ideas, research and news. Concurrently easing the access of users to these sources encouraging them to optimize their usage of internet.

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources, this may present **(Organization)** with new risks that must be addressed to safeguard the its vital information assets. Additionally, **(Organization)** may face loss of reputation and possible legal action through other types of misuse. Having the **Internet Usage Policy** in place helps to protect both the business and the employee from the misuse of using the internet.

3.2 Purpose

Internet usage policy aims to provide employees with rules and guidelines regarding the appropriate use of **(Organization)** equipment, network and Internet access to ensure that employees make the most effective use of the internet

3.3 Scope

This policy applies to all Internet users (employees and all third parties) who access the Internet through **(Organization)**'s computing or networking resources and to its related services.

3.4 Policy

3.4.1 Resource Usage

3.4.1.1 Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities.

3.4.1.2 User Internet access requirements will be reviewed periodically by **(Organization)** departments to ensure that continuing needs exist.

3.4.1.3 Employees of the **(Organization)** are allowed to use internet for **(Organization)** business-related purposes, and in a way that consistent with this policy and doesn't conflict with **(Organization)** rules and laws.

3.4.1.4 **(Organization)** doesn't ensure the accuracy of any information obtained through the Internet, it's the responsibility of the originator and producer of such information.

3.4.1.5 **(Organization)** reserves the right to impose the permitted capacity for the use of the internet, as the competent technical authority deems appropriate to the requirements of each department.

3.4.2 Allowed Usage

3.4.2.1 Communication between employees and non-employees for business purposes.

3.4.2.2 IT technical support downloading software upgrades and patches.

3.4.2.3 Review of possible vendor web sites for product information.

3.4.2.4 Reference regulatory or technical information.

3.4.2.5 Research

3.4.3 Personal Usage

3.4.3.1 Using **(Organization)** computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action accordance with the applicable regulations.

3.4.3.2 All users of the Internet should be aware that **(Organization)** network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

3.4.3.3 Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. **(Organization)** is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

3.4.3.4 User is fully responsible for his/her computer devices and the use of them, and he/she has to be aware of the security and preserve of IT resources.

3.4.3.5 If recognizing or noticing an actual or suspected security issue, users must contact the Information Security Department and report immediately.

3.4.4 Prohibited Usage

3.4.4.1 It's strictly prohibited to use the internet in a way that may damages the **(Organization)**'s network, or to expose any security vulnerabilities or to help in spread any harm or illegal applications.

3.4.4.2 Impersonation of others or devices is forbidden.

3.4.4.3 Users must not use **(Organization)**'s name or any of its departments or employees unless there is a written approval to do so.

3.4.4.4 Tampering with other's information or disclosing them illegally.

3.4.4.5 Publishing any of **(Organization)**'s information or any of its employees without consent to do so.

3.4.4.6 It's prohibited to decipher/decrypt/decode other's data in any information systems without a consent from targeted party.

3.4.4.7 Copyright, or intellectual property rights to any data, applications, programs or information must not be infringed.

3.4.4.8 It's prohibited to monitor electronic communications by other users for the purpose of espionage and privacy violation.

3.4.4.9 Users should not abuse the usage of internet in a way that affect other users or the performance of devices and networks.

3.4.4.10 Use of the Internet for any illegal purposes is prohibited. Examples include sending media contains violence, threat, fraud, obscenity or illegal material that cause any harm to any person or authority or its cyber security.

3.4.4.11 It is prohibited to waste information resources or to make any change on them without an approval.

3.4.4.12 It is prohibited to create a website or account on social networking sites representing **(Organization)** or its departments without a permission.

3.4.4.13 Must not contact or access to any other information resources unless through available channels and officially authorized by **(Organization)**.

3.4.4.14 It's not allowed for **(Organization)**'s employees to use informational resources in a way that waste their time.

3.4.4.15 Internet connection of **(Organization)** shouldn't be used for commercial, political, or personal purposes, or for commercial or marketing profit.

3.4.4.16 It is prohibited to create unauthorized electronic copies of documents that pertaining to **(Organization)** and to its departments, or any material protected by copyright for the purpose of publishing or sending them through **(Organization)**'s network.

4 Workstation Security Policy

4.1 Introduction

User's workstation including computers and peripherals (printers, scanners, laptops, etc.) are used in daily performance in a reasonable and proportionate manner that compatible with **(Organization)**'s objectives and strategies. This policy outlines the minimum requirements for the use of computers and peripherals within **(Organization)**.

4.2 Purpose

The purpose of this policy is to protect users and workstations from potential risks by defining policies and procedures for the use of computers and peripherals within the **(Organization)**.

4.3 Scope

This policy applies to all employees and users who use computers, peripherals and associated services.

4.4 Policy

4.4.1 Users are only allowed to use their computer devices. They shouldn't use or attempt to access other's devices.

4.4.2 Users should be fully responsible for the proper use of all resources allocated to them, including computer devices, peripherals and software.

4.4.3 Users are not allowed to access network using personal computers, tablets and smartphones, unless authorized by competent technical department.

4.4.4 Users should not attempt to access to unauthorized parts of the network, such as the main operating system, security software, etc., without getting an approval to do so.

4.4.5 Users must not install, or use any software, tools, or devices that may damage software, hardware or system components.

4.4.6 It's prohibit to install or use any tools commonly used to attack security systems or to penetrate computer systems or other networks (such as password detectors, network scanners, etc.).

4.4.7 Personal privacy and the rights of others should be respected, and shouldn't attempt to obtain data from other users, as well as other programs or files without prior permission.

4.4.8 Special approval from Information Technology Department required prior to installation of any special software or hardware on the **(Organization)**'s systems.

4.4.9 Computers on loan from the **(Organization)** are for official **(Organization)** use only. They are not to be used by family members or friends under any circumstances.

4.4.10 When the computer is returned, Information Technology department reserves the right to scrub the hard disk of any data and reinstall all of the standard software. Users are responsible for any data they leave on the laptop when it is returned to the **(Organization)**.

4.4.11 Information Technology department reserves the right to recall all equipment out on loan in order to perform upgrades to software, and/or hardware replacement/upgrades at any time.

4.4.12 IT staff should not login into user's devices for maintenance work unless the permission is taken directly from the concerned user.

4.4.13 Computers and peripherals are available to serve employees and users to perform better work, therefore cannot be used for personal purposes.

4.4.14 **(Organization**) offers a wide variety of networked printers for **(Organization)** use in several central locations. Individual desktop printers are permitted, and will be supported by the Information Technology department.

4.4.15 **(Organization)**'s staff are prohibited from purchasing their own network equipment including, but not limited to, LAN cards, Wireless Cards, Routers, Switches, Network Cabling, and network-ready Printers.

4.4.16 Network stability is paramount in **(Organization)** environment, and the addition of unauthorized network gear to **(Organization)** network can potentially result in hard-to-diagnose problems.

4.4.17 Logging computer using username and password, and when leaving the device even for a short period of time, it's a must to lock screen with password.

4.4.18 Users shouldn't save files, documents, or any media into hard drivers that are unrelated to job.

4.4.19 User is responsible to learn how to use the computer and its peripherals properly, and if facing any problems while using, he/she should ask help from the competent technical department.

4.4.20 Non-employees shall not be allowed to use computer devices at **(Organization)** without an official written permission.

4.4.21 Users should not disable antivirus and malware software on **(Organization)** computer devices, and they should always check any data storage mediums (e.g. CDs, Hard drives, flash memory, etc.) before opening any file or program.

4.4.22 Users shouldn't copy any material or software from **(Organization)**'s computer devices to distribute outside **(Organization)** without a written consent to do so.

سياسة مضاد الفيروسات

1. مقدمة

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

2. الغرض

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

3. نطاق الاختصاص

تنطبق هذه السياسة على:

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

4. السياسة

4.1. مسؤوليات المستخدم

4.1.1 يجب أن يستعمل فقط برنامج مضاد الفيروسات المعتمد لدى (**جهة العمل**)، والذي يجب أن يكون متوفراً من خلال (موقع التحميل الخاص بـ(**جهة العمل**) مثلاً). يجب تحميل وتنصيب الإصدار الحالي، كما يجب تحميل وتنصيب آخر التحديثات للبرنامج فور توفرها.

4.1.2 يمنع فتح أي ملف أو ماكرو مرفق برسالة بريد الكتروني من مصدر غير معروف أو مشبوه أو غير موثوق به. يجب حذف هذه الملحقات على الفور ومن ثم تأكيد الحذف بتفريغ سلة المهملات.

4.1.3 يجب مسح الرسائل المزعجة (Spam) والرسائل المتسلسلة (Chain) وغيرها من رسائل البريد الغير مرغوب بها وعدم إعادة إرسالها للغير.

4.1.4 يمنع تحميل الملفات من مصادر غير معروفة أو مشبوهة.

4.1.5 يجب تجنب المشاركة المباشرة على قرص التخزين بصلاحيات القراءة والكتابة مالم يكن هناك حاجة ضرورية لذلك وتلبية لمتطلبات العمل التي لا يمكن تحقيقها بطريقة أخرى.

4.1.6 يجب إجراء كشف عن الفيروسات لأي وسيط تخزين متنقل قبل استخدامه.

4.1.7 يتوجب حفظ نسخ احتياطية للبيانات الحساسة وإعدادات النظام بشكل دوري وتخزينها في مكان آمن.

4.1.8 يحظر على المستخدمين الخوض في إي نشاط يستهدف به صناعة و/أو توزيع البرامج الخبيثة (مثل الفيروسات والديدان واحصنة طروادة ورسائل البريد الالكتروني المفخخة . . .إلخ) داخل شبكة أو أنظمة (**جهة العمل**).

4.1.9 يتوجب على المستخدمين إعلام فريق تقنية المعلومات بـ(**جهة العمل**) في حالة اكتشاف وجود فيروس بأنظمتهم.

4.1.10 أنظمة تقنية المعلومات المصابة ببرنامج خبيث أو فيروس ولم يتمكن مضاد الفيروسات من معالجتها يجب فصلها وعزلها من شبكة (**جهة العمل**) إلى أن تصبح خالية من العدوى.

4.1.11 إذا اكتشف المستخدم أن نظامه مصاب بعدوى ما فيجب عليه القيام بالتالي:

- إبلاغ فريق تقنية المعلومات بـ(**جهة العمل**) على الفور.
- إطفاء الجهاز.
- ضمان ألا يستعمل الجهاز موظفين آخرين.
- أن يكون مستعداً لاطلاع فريق تقنية المعلومات على أي إجراء قام به قد يكون سبب العدوى.

4.2. مسؤوليات فريق تقنية المعلومات بـ(جهة العمل)،

4.2.1 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 بـ(**جهة العمل**)

4.2.2 يجب توزيع ونشر تحديثات برنامج مضاد الفيروسات عبر شبكة (**جهة العمل**) بشكل آلي فور وصولها من الشركة المصنعة ويجب ضبط البرنامج ليتحقق من وجود التحديثات كل 60 دقيقة.

4.2.3 تعريفات الفيروسات والبرامج الخبيثة يجب نشرها عبر شبكة (**جهة العمل**) بشكل آلي فور وصولها من الشركة المصنعة ويجب ضبط البرنامج ليتحقق من وجود التحديثات كل 10 دقائق، كما يجب ربط جميع نسخ البرنامج الموجودة بالأنظمة بمخدم تحميل تعريفات ثانوي بحيث إذا لم يسجل الجهاز دخوله بشبكة (**جهة العمل**) يمكنه تحميل التعريفات من المخدم الثانوي.

4.2.4 يجب ضبط برنامج مضاد الفيروسات للقيام بمسح في الوقت الحقيقي (Real Time Scanning) وإجراء مسوحات دورية مجدولة زمنياً.

4.2.5 يجب تفعيل ميزة المسح التلقائي عند الدخول (On-access Scanning) في مضاد الفيروسات لوسائط التخزين المحمولة.

4.2.6 مخدم مضاد الفيروسات يجب مراقبته بشكل يومي من قبل عضو معين من فريق تقنية المعلومات بـ(**جهة العمل**) ومتابعة ما يصدره من تنبيهات وإنذارات، وكما يجب إحالة إي مشكلة لا يمكن حلها عن بعد عبر واجهة الإدارة المركزية للخادم إلى مكتب دعم تقنية المعلومات والذي بدورهم يعتبرونها حادثة ويقومون بتكليف أحد الاخصائيين للتحقيق في الأمر.

4.2.7 إذا أصيب عدد من الأجهزة (ثلاثة أو أكثر) ببرنامج خبيث في نفس الوقت فيتوجب إصدار تقرير فني حول أسباب العدوى وإحالته إلى مسؤولي الأمن السيبراني بالإدارة العليا.

4.2.8 يتوجب إصدار تقرير نصف سنوي بخصوص مدى التزام الجميع بتطبيق السياسة وإحالته لمسؤولي الأمن السيبراني بالإدارة العليا ومدير فرع بـ(**جهة العمل**) (إن وجد) وإلى فريق التخطيط الاستراتيجي لتقنية المعلومات في موعد محدد.

4.2.9 يجب وضع آلية لمنع التلاعب بإعدادات وضبط برنامج مضاد الفيروسات من قبل المستخدمين.

4.2.10 في حالة اشتباه المستخدم في وجود فيروس بجهازه وقام بالتبليغ عنه لمكتب دعم تقنية المعلومات، فعلى فريق تقنية المعلومات القيام بالتالي:

- الكشف على الجهاز وأي وسائط تخزين ملحقه به.
- إعادة ضبط الجهاز في حالة كانت الإصابة حرجة (برمجية الفدية الخبيثة مثلاً).
- الكشف على أي خادم قد يكون اتصل به الجهاز المصاب.
- محاولة معرفة مصدر العدوى.
- ضمان توثيق الحادثة.

Anti-Virus Policy

1. Introduction

The software and hardware that make up the computer networks are essential resources for (**organization**). They aid staff in carrying out their everyday duties and without these important communication systems would not exist. Computer viruses pose considerable risks to these systems. They can cause them to run erratically, cause loss of information, and information to become corrupted, with the consequential loss of productivity for the (**organization**).

2. PURPOSE

This policy is designed to give guidance and direction on minimizing the risk of a virus infection, and what to do if they are encountered.

3. SCOPE

This policy applies to:

- All employees whilst using (**organization**)'s equipment and accessing the (**organization**)'s Network at any location, on any computer or Internet connection.
- Other persons working for the (**organization**), persons engaged on business or persons using equipment and networks of the organization.
- Anyone granted access to the network.

4. POLICY

4.1. User's Obligations

4.1.1. Always run (organization) anti-virus standard, supported anti-virus software is available from (e.g. the corporate download site). Download and run the current version; download and install anti-virus software updates as they become available.

4.1.2. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

4.1.3. Delete spam, chain, and other junk email without forwarding.

4.1.4. Never download files from unknown or suspicious sources.

4.1.5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

4.1.6. Always scan a portable storage media from an unknown source for viruses before using it.

4.1.7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

4.1.8. Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojans, e-mail bombs, etc) into (organization) network(s) or system(s).

4.1.9. Users MUST inform the IT Service Desk immediately if a virus is detected on their system.

4.1.10. IT system(s) infected with a malware/virus that the anti-virus software has not been able to deal with MUST be disconnected/quarantined from (organization) network until virus free.

4.1.11. If a user suspects the system may be infected, the following actions must be taken

- Inform the IT service desk immediately.
- Switch off the machine.
- Ensure no-one uses the machine.
- Be prepared to inform IT of any actions taken which may have caused the infection.

4.2. Organizations' IT Department's Obligations

4.2.1 Approved Anti-virus software MUST be made readily available for all employees and the IT department personnel MUST exclusively correctly install and configure it on all supported endpoints and servers across all the (organization)'s IT systems.

4.2.2 Anti-virus software updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 60 minutes daily.

4.2.3 Virus and malware signature updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for signature updates every 10 minutes daily. All the endpoints must be configured with the secondary anti-virus update server so if a device is not checked in on the corporate network then updates will be installed from the secondary server.

4.2.4 Anti-virus software MUST be configured for real time scanning and regular scheduled scans.

4.2.5 On-access scanning MUST be configured within Anti-virus software for removable media and websites.

4.2.6 Anti-virus server MUST be monitored on a daily basis by a nominated staff within IT department's team for virus alerts and any issues which cannot be resolved remotely via centralized management console

must be escalated to the IT Service Desk where an incident will be raised, and a technician assigned to immediately investigate.

4.2.7 In the event of a virus infection which infects multiple devices (more than 3 devices) at the same time. A root cause analysis report should be completed by the technician for (**organization**) Cyber Security Senior Staff.

4.2.8 Semiannual Anti-Virus compliance reports MUST be provided to (**organization**) Cyber Security Senior Staff, Branch Manager (if any) and IT Strategy & Planning Team by a preset date.

4.2.9 Tamper protection MUST be enabled to prevent end users or malware altering the anti-virus software's configuration or disabling the protection.

4.2.10 If a user suspects the system may be infected and inform the IT service desk, The IT Team will:

- Check the infected PC and any media.
- Rebuild the PC if the infection is severe (e.g. Dridex, Ransomware).
- Check any servers that may have been accessed from the infected system.
- Attempt to determine the source of the infection.
- Ensure the incident is logged.

سياسات حماية الشبكات

نظرة عامة

لا توجد آلية محددة لحماية الشـبكة لأن أي نظام أمني يمكن أن يتعرض للتخريب أو الاختراق، إن لم يكن من الخارج فمن المؤكد أنه من الداخل، في نهاية المطاف لتأمين شـبكة يجب تنفيذ طبقات مختلفة من الأمن بحيث يجب على المهاجم اختراق نظامين أو أكثر للوصـول إلى الأصـول الهامة، الخطوة الأولى في تطبيق السـياسـات هي تحديد السـياسـات التي سـيتم تنفيذها، وغالبا ما تقيد التدابير الأمنية الأفراد في ممارسـاتهم التشـغيلية مما يؤدي إلى تعزيز اللوائح الأمنية، لذا، تحكم سـياسـات الشـبكة كيفية تنفيذ الشـبكة وتهيئتها لتبسـيط عمل الموظف في الظروف العادية، وكذلك إرشـادات كيفية التفاعل او التعامل أثناء حدوث الحوادث. في هذا السياق، يشرح القسم التالي فرض مقاييس السياسات لكل مصطلح أو مبدأ أمن الشبكة لحماية المعلومات والنظم.

1. سياسات جهاز التوجيه ومبدل (Router and Switch) الشبكة

1.1 المقدمة

توفر أجهزة التوجيه ومبدلات الشـبكة وظائف أمان مهمة داخل الشـبكة إذا ما تم تهيئتها بشـكل صحيح، فهما ضـمن العديد من الأجهزة والبرامج المتوفرة والتي تسـاعد في إدارة وحماية الشـبكة الخاصـة من الشـبكة العامة .تحدد سـياسـة أمن الموجه ومبدل الشبكة متطلبات التهيئة لتلبية معايير الأمان ومتطلبات إدارة التغيير والمتطلبات التشغيلية.

1.2 الغرض

هذه الوثيقة مصـممة لحماية معدات وبيانات **(جهة العمل)** وشـركائها التجاريين أو أي بيانات مملوكة أو تحت تصـرف **(جهة العمل)** من خلال تحديد الحد الأدنى لمعايير التكوين والضـبط لجميع أجهزة التوجيه والمبدلات التي تتصـل بشـبكة **(جهة العمل)**.

1.3 النطاق

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

1.4 السياسة

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

1. لا يتم تكوين أي حسابات مستخدمين محليين على جهاز التوجيه و/ أو التبديل نفسه، بل يجب أن تستخدم أجهزة التوجيه والمبدلات خادم AAA مخصصًا لهذا الغرض مثل (+ TACACS) للقيام بجميع مصادقات المستخدمين.
2. يجب استخدام كلمة السر (enable secret) بدلاً من تمكين كلمة المرور (enable password).
3. يجب الحفاظ على كلمة السر (enable secret) مشفرة و مؤمنة على جهاز التوجيه أو المبدل.
4. يجب تعطيل الخدمات أو الميزات التالية :

- البث الموجه عبر بروتوكول الإنترنت (IP directed broadcasts) (يمكن تفعيل البث الموجه نحو بروتوكول الإنترنت عند الرغبة في تنفيذ خدمات الإدارة أو الإدارة عن بعد مثل النسخ الاحتياطية على الأجهزة المضيفة في شبكة فرعية ليس لديها اتصال مباشر بالإنترنت)
- الحزم الواردة لجهاز التوجيه/التبديل والقادمة من مصادر ذات عناوين غير صالحة مثل عناوين RFC1918.
- خدمات TCP الصغيرة (TCP small services).
- خدمات UDP الصغيرة (UDP small services).
- جميع خدمات الويب التي تعمل على جهاز التوجيه.
- التكوين التلقائي (Auto-configuration).
- بروتوكول استكشاف الأجهزة للطبقة الثانية (مثل CDP وLLDP) وبروتوكولات الاكتشاف الأخرى.

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

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

6. يجب ضبط الخدمات التالية:

- تشفير كلمة المرور.
- مزامنة الوقت (NTP). يجب مزامنة جميع ساعات الشبكة مع مصدر زمن مشترك.

7. جميع تحديثات التوجيه (Routing) يجب ان تتم باستخدام تحديثات التوجيه الآمن.
8. استخدام نصوص SNMP الموحدة لـــ(**جهة العمل**). يجب إزالة النصوص الافتراضية، مثل العامة أو الخاصة (public وprivate). يجب تهيئة SNMP لاستخدام النسخة الأكثر أماناً من البروتوكول المدعومة من كلا الطرفين؛ الجهاز وأنظمة الإدارة .
9. يجب استخدام قوائم التحكم في الوصول (Access control lists) للحد من مصدر ونوع حركة المرور التي يمكن أن تصل للجهاز نفسه.
10. يجب أن يحتوي كل جهاز توجيه (Router) على إشـــعار تنبيه يظهر في نافذة أو محث أوامر الدخول للنظام يحوي على معلومات تفيد أن الدخول هنا مسموح به للمستخدمين المصرح لهم بذلك فقط لا غير. البيان التالي يجب أن يظهر عند استخدام أي شكل من أشكال تسجيل الدخول سواء كانت محلية أو عن بعد:

"يحظر الدخول لهذا الجهاز لغير المصرح لهم.
يجب أن يكون لديك إذن صريح للدخول إلى هذا الجهاز أو ضبطه. أي اجراء أو تغيير تقوم به يكون عرضة للتوثيق والحفظ وإذا ما ارتكبت أي مخالفات للسياسات المعتمدة فسوف تتعرض لاتخاذ إجراءات عقابية صارمة ضدك حسب اللوائح المعمول بها.
ليس لك أي حق في الخصوصية على هذا الجهاز. استخدامك لهذا النظام يعد موافقة تلقائية على مراقبة ما تقوم به."

11. لا يجوز أبداً اســـتخدام بروتوكول Telnet عبر أي شـــبكة لإدارة جهاز توجيه، ما لم يكن هناك نفق آمن يحمي مســـار الاتصال بالكامل ، الإصدار 2 من بروتوكول (SSH) هو بروتوكول الإدارة المفضل.
12. ينبغي وضع أجهزة التوجيه والمبدلات في مكان يقتصر فيه الدخول على الأشخاص المرخص لهم فقط.

13. يجب أن يقوم المبدل بتعطيل منفذ أو مجموعة من المنافذ في حالة ظهر بها عناوين اجهزة (MAC) جديدة أو غير مسجلة مسبقاً على المنفذ إذا كانت هذه الميزة متاحة.
14. يجب أن يقوم المبدل بتوليد رسائل (SNMP TRAP) إذا وقع الاتصال وتم إعادة توليده في حال توفرت هذه الميزة.
15. يجب أن تستخدم بروتوكولات التوجيه الديناميكية المصادقة عند إرسال تحديثات التوجيه إلى الأجهزة المجاورة. (يجب تمكين ميزة تحويل كلمة المرور بدالة الاختزال (Hashing) في نص المصادقة عند دعمها.
16. من خلال المعيار المعتمد لدى (**جهة العمل**) يتم تحديد فئة من الأجهزة تعتبر ذات وضع حساس نظراً لطبيعة عملها، وبذلك فإنها ستحتاج إلى خدمات وضبط إضافي والذي يجب أن يشمل:

- متابعة ومراقبة لقوائم التحكم في الوصول لبروتوكول الإنترنت (IP Access List Accounting).
- تسجيل وتوثيق احداث الجهاز (Device logging).
- يجب إسقاط الحزم الواردة للموجه التي يكون مصدرها من عناوين غير صالحة، مثل عناوين RFC1918 أو تلك التي يمكن استخدامها لخداع (Spoof) حركة مرور الشبكة.

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

- رسم تخطيطي للشبكة.
- ضوابط النظام (System configurations).
- قواعد الجدار الناري.
- عناوين بروتوكولات الانترنت (IP Addresses).
- قوائم التحكم في الوصول.

2. سياسة الاتصالات اللاسلكية

2.1 المقدمة

مع الانتشار المتسارع للهواتف الذكية والأجهزة اللوحية، فإن الاتصال اللاسلكي أصبح واسع الانتشار وهو ما أصبح أمراً مسلماً به ولا تخلو منه أي مؤسسة. يمكن للضبط اللاسلكي الغير الآمن توفير باب مفتوح وسهل للمخترقين والقراصنة.

تعد سياسة الاتصالات اللاسلكية ضرورية لأمن الكمبيوتر نظراً لوجود طلب متزايد على المعدات اللاسلكية في كل **(جهة عمل)** اليوم. قد تحدد سياسة الاتصال اللاسلكي أنه لا يجب استخدام أي معدات لاسلكية، لكن ذلك لن يكون عملياً وواقعياً لأن ذلك قد يؤدي للجوء بعض الإدارات أو الأفراد إلى انتهاك لهذه السياسة، لذا كان من الأفضل تحديد الشروط وتحديد المعدات المعتمدة للاستخدام اللاسلكي لتقليل مخاطر الأمان المرتبطة باللاسلكي الذي لابد منه.

2.2 الغرض

الغرض من هذه السياسة هو تأمين وحماية أصول المعلومات التي تملكها **(جهة عمل)**. تمنح **(جهة عمل)** الوصول إلى هذه الموارد كإمتياز ويجب أن تدار هذه الموارد بطريقة مسؤولة للحفاظ على سرية ونزاهة وتوافر جميع الأصول المعلوماتية.

كما تحدد هذه السياسة الشروط التي يجب أن تستوفيها أجهزة البنية التحتية اللاسلكية للاتصال بشبكة **(جهة عمل)**، بحيث لا تتم الموافقة إلا على أجهزة البنية التحتية اللاسلكية التي تفي بالمعايير المحددة في هذه السياسة أو تلك التي تم منحها استثناء من قبل إدارة أمن المعلومات للاتصال بشبكة **(جهة عمل)**.

2.3 النطاق

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

2.4 السياسة

2.4.1 جميع أجهزة البنية التحتية اللاسلكية الموجودة في موقع **(جهة عمل)** والمتصلة بشبكتها، أو التي توفر الوصول إلى معلومات مصنفة على أنها سرية يجب عليها مايلي:

- الالتزام بالمعايير المحددة في معيار الاتصالات اللاسلكية.
- استخدام بروتوكولات المصادقة والبنية التحتية المعتمدة من قبل **(جهة عمل)**.

- استخدام بروتوكولات التشفير المعتمدة لدى **(جهة عمل)**.
- الحفاظ على العناوين المادية للأجهزة (MAC) التي يمكن تسجيلها وتتبعها.

2.4.2 للحد من احتمال إساءة استخدام الشبكة اللاسلكية:

- ينبغي أن تكون هناك مصادقة سليمة للمستخدم مع الاستبدال المناسب لآلية WEP وتتبع الشذوذ (Anomaly Tracking) على الشبكة المحلية اللاسلكية.
- في نفس الوقت، القائمة التالية تحوي عدداً من الأحداث المشبوهة التي قد تقع داخل الشبكة المحلية اللاسلكية والتي ينبغي دائماً أن تأخذ في الاعتبار عند ضبط أنظمة كشف التسلل:
  - إطارات الإرشاد (Beacon Frames) القادمة من نقطة وصول لاسلكية لم يطلب منها ذلك (unsolicited).
  - فيضان الأطر غير المصادق عليها (هجوم MITM)
  - اطر بيانات تحوي عنوان MAC مكرر.
  - تغيير عنوان MAC بشكل عشوائي.

2.4.3 بروتوكولات التشفير اللاسلكية

يفضل استخدام بروتوكول حماية الوصول للواي فاي الاصدار 2 (WAP2) كبروتوكول تشفير للشبكات اللاسلكية بدلاً من بروتوكول حماية الوصول للواي فاي الاصدار الاول (WAP) و بروتوكول الخصوصية المكافئة للشبكات السلكية (WEP) وذلك لأنه يوفر خوارزمية أمان أقوى وتشفيرًا متقدمًا كما يتحقق من صحة الرسالة وتكاملها.

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

- رسم تخطيطي للشبكة.
- ضوابط النظام (System configurations).
- قواعد الجدار الناري.
- عناوين بروتوكولات الانترنت (IP Addresses).
- قوائم التحكم في الوصول.

3. سياسة الشبكة الافتراضية الخاصة (VPN)

3.1 المقدمة

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

3.2 الغرض

تهدف هذه السياسة إلى توفير إرشادات خاصة باتصالات الوصول عن بُعد عبر IPsec أو شبكة L2TP الخاصة الافتراضية (VPN) إلى شبكة **(جهة عمل)**.

3.3 النطاق

تنطبق هذه السياسة على جميع موظفي **(جهة عمل)** والمقاولين والمستشارين والموظفين المؤقتين وغيرهم من العمال بما في ذلك جميع الموظفين المنتسبين إلى أطراف ثالثة المستخدمين لشبكات VPN ليتمكنوا من الدخول إلى الشبكة **(جهة عمل)**. تنطبق هذه السياسة على تطبيقات VPN التي يتم توجيهها للمرور عبر مُركِّز IPsec (IPsec Concentrator).

3.4 السياسة

3.4.1 تقع على عاتق الموظفين الذين لديهم امتيازات استخدام الشبكة الافتراضية الخاصة VPN ضمان عدم السماح للمستخدمين غير المصرح لهم بالوصول إلى الشبكات الداخلية لـ**(جهة عمل)** عبر وصلات الـ(VPN) الخاصة بهم.

3.4.2 يجب التحكم في استخدام الشبكة الافتراضية الخاصة VPN باستخدام مصادقة بكلمة المرور لمرة واحدة (one-time password) كجهاز اشارة السماح (Token Device) أو نظام المفتاح العام/الخاص مع اختيار عبارة مرور قوية (passphrase).

3.4.3 عندما يكون الاتصال بشبكة **(جهة عمل)** نشطاً، فإن آلية الشبكات الافتراضية الخاصة (VPN) يجب أن تقوم بإجبار كل حركة المرور من وإلى الكمبيوتر عبر نفق VPN بينما يقوم بطرح وتجاهل أي حركة بيانات أخرى.

3.4.4 تقاسم أو ازدواج الاتصال عبر نفق التشفير (Dual (split) tunneling) غير مسموح؛ إذ لا يسمح بحصول أكثر من اتصال شبكي واحد فقط في نفس الوقت. تقاسم أو ازدواج الاتصال عبر نفق التشفير يسمح بوجود اتصالين

نشطين متزامنين في نفس الوقت، أحدهما لشبكة آمنة عبر الـ(VPN) والثاني لشبكة غير آمنة، هذا الوضع يشكل ثغرة تسهل الاتصال المباشر من الانترنت الغير آمن إلى الشبكة المؤمنة باتصال بتقنية الـ(VPN).

3.4.5 بوابات الشبكات الافتراضية الخاصة (VPN gateways) يتم اعدادها وإدارتها من قبل موظفي القسم الخاص بعمليات الشبكة لـ**(جهة عمل)**.

3.4.6 يتوجب على كل الأجهزة التي تتصل بالشبكة الداخلية لـ**(جهة عمل)** باستخدام الـ(VPN) أو غيرها من التقنيات أن تستخدم برامج مضادة للفيروسات محدثة ومطابقة للمعايير المتبعة من قبل **(جهة عمل)**؛ بما في ذلك الحواسيب الشخصية.

3.4.7 يجب فصل مستخدمي VPN تلقائياً عن شبكة **(جهة عمل)** بعد ثلاثين دقيقة من عدم النشاط. ويجب على المستخدم تسجيل الدخول مرة أخرى لإعادة الاتصال بالشبكة.

(يمنع استخدام pings أو عمليات شبكة مصطنعة أخرى للحفاظ على الاتصال مفتوحاً)

3.4.8 يجب ضبط جهاز (VPN concentrator) بتحديد وقت أي اتصال بحيث لا يتجاوز الأربع وعشرين (24) ساعة.

3.4.9 يجب على مستخدمي أجهزة الكمبيوتر التي ليست من الأجهزة التي تملكها **(جهة عمل)** تهيئة الأجهزة بحيث تتوافق مع سياسات الشبكة وسياسات الربط بتقنية الشبكة الافتراضية الخاصة (VPN) بـ**(جهة عمل)**

3.4.10 باستخدام تكنولوجيا VPN مع الاجهزة الشخصية، يجب أن يعي المستخدمون أن أجهزتهم اصبحت امتداداً فعلياً وجزءاً من شبكة **(جهة عمل)**، وبالتالي فهي تخضع لنفس القواعد واللوائح التي تنطبق على المعدات التي تستخدمها **(جهة عمل)**.

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

- رسم تخطيطي للشبكة.
- ضوابط النظام (System configurations).
- قواعد الجدار الناري.
- عناوين بروتوكولات الانترنت (IP Addresses).

- قوائم التحكم في الوصول.

4. سياسة جدار الحماية/الناري (Firewall)

4.1 المقدمة

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

4.2 الغرض

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

4.3 النطاق

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

4.4 السياسة

4.4.1 مراجعة مجموعة القواعد للتأكد من اتباعها للترتيب كما يلي:

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

4.4.2 جدار الحماية القائم على التطبيق:

- في حالة الدخول على خادم مخصص، يجب وضع جدار ناري برمجي يعمل بالنيابة (وكيل) (Application Proxy Firewall) ما بين المستخدم المتصل عن بعد والخادم المخصص وذلك لإخفاء هوية الخادم.
- التأكد من مراقبة المسؤولين لأية محاولات لانتهاك سياسة الأمن باستخدام سجلات التدقيق التي تم إنشاؤها بواسطة جدار الحماية على مستوى التطبيق.
- ضمان أن هناك آلية لتحديث وسد ثغرات الجدار الناري على مستوى التطبيقات والتحقق بأنها محدثة لسد آخر الثغرات.
- تأكد من وجود عملية لتحديث البرنامج بأحدث بصمات الهجوم.
- في حالة تنزيل التواقيع من موقع الموردين والشركات المصنعة، يجب التأكد بأنها من موقع موثوق.
- في حالة إرسال البصمات بالبريد الإلكتروني إلى مسؤول النظام، يجب التأكد من استخدام التوقيعات الرقمية للتحقق من المورد وأن المعلومات المنقولة لم يتم تغييرها أثناء النقل.
- يجب حظر الأوامر التالية لـ SMTP في جدار الحماية على مستوى التطبيق:
  - EXPN (التوسيع - expand)
  - VRFY (تحقق- verify)
  - DEBUG
  - WIZARD
- يجب حظر الأمر التالي لـ FTP:
  - PUT
- مراجعة وحظر العناوين (URL's) والتأكد بانها ملائمة، فعلى سبيل المثال. يجب حظر أي عنوان URL لمواقع المخترقين.

- التأكد من أن المستخدمين المخولين هم فقط من يتم التصديق عليهم بواسطة جدار الحماية على مستوى التطبيق.

4.4.3 **تفحص بحالة الاتصال (Stateful Inspection)**

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

بالنسبة لعناوين URL

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

4.4.4 **تسجيل الاحداث**

- تأكد من تفعيل خاصية تسجيل الاحداث وأن يتم مراجعة السجلات لتحديد أي أنماط محتملة قد تشير إلى وجود هجوم.
- سجلات إدارة جدار حماية الشبكة (الأنشطة الإدارية) وسجلات الأحداث (نشاط حركة المرور) يجب أن:
  - يتم تخزينها على وحدة تخزين بديلة (وليس على نفس الجهاز)
  - تتم مراجعتها يوميًا على الأقل، مع الاحتفاظ بالسجلات لمدة تسعين (90) يوماً

4.4.5 **التصحيحات والتحديثات**

- تأكد من اختبار وتثبيت أحدث التصحيحات والتحديثات المتعلقة بجدار الحماية الخاص بك.

- إذا تم تنزيل التصحيحات والتحديثات تلقائيًا من مواقع الويب الخاصة بالموردين، فتأكد من استلام التحديث من موقع موثوق به.
- في حالة إرسال التصحيحات والتحديثات بالبريد الإلكتروني إلى مدير النظام، تأكد من استخدام التوقيعات الرقمية للتحقق من المورد (Vendor) والتأكد من عدم تعديل المعلومات في الطريق.

4.4.6 **تقييم / اختبار الضعف**

- يجب التحقق ما إذا كان هناك إجراء لاختبار المنافذ المفتوحة باستخدام (NMAP)، وما إذا كانت المنافذ غير الضرورية مغلقة.
- التأكد من وجود إجراء لاختبار القواعد عند تأسيسها أو تغييرها حتى لا يؤدي إلى رفض الخدمة أو السماح باستمرار وجود نقاط الضعف دون أن يتم اكتشافها.

4.4.7 **الالتزام بسياسة الأمن**

- تأكد من أن القواعد تتوافق مع سياسة أمن **(جهة العمل)**.

4.4.8 **تأكد من أن العناوين التالية الخاصة، (RFC 1918) المنتحلة والعشوائية محظورة:**

- عناوين خاصة (RFC 1918)

  10.255.255.255 - 10.0.0.0

  172.31.255.255 - 172.16.0.0

  192.168.255.255 - 192.168.0.0

- عناوين محجوزة

  240.0.0.0

- عناوين غير قانونية

  0.0.0.0

- UDP echo
- بث ICMP (RFC 2644)

4.4.9 **الوصول عن بعد**

- في حالة استخدام الوصول عن بعد، تأكد من استخدام بروتوكول SSH (المنفذ 22) بدلاً من Telnet.

4.4.10 **نقل الملفات**

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

4.4.11 **حركة البريد الإلكتروني**

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

4.4.12 **حظر حركة ICMP غير المرغوب فيها (ICMP 8, 11, 3).**

- تأكد من وجود قاعدة تمنع طلبات ورسائل ارتداد ICMP.
- تأكد من وجود قاعدة تمنع ارسال رسائل تجاوز الوقت (Time Exceeded) ورسائل الإبلاغ عن عدم القدرة عن وصول للهدف (Unreachable).

4.4.13 **الخوادم الحرجة والحساسة (Critical Servers)**

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

4.4.14 **جدران الحماية الشخصية**

- تأكد من حصول مستخدمي الكمبيوتر المحمول على التدريب المناسب فيما يتعلق بالتهديدات وأنواع العناصر المحظورة بواسطة جدار الحماية والمبادئ التوجيهية لتشغيل جدار الحماية الشخصي. هذا العنصر ضروري، حيث تعتمد الجدران النارية الشخصية أحيانًا على مطالبة المستخدم بالرد على الهجمات. على سبيل المثال، ما إذا كنت تريد قبول / رفض طلب من عنوان معين.

- قم بمراجعة إعدادات الحماية الخاصة بجدار الحماية الشخصي للتأكد من أنه يقيد الوصول إلى منافذ معينة، ويحمي من الهجمات المعروفة ، وأن هناك تنبيهات كافية لتسجيل الدخول وتنبيهات للمستخدم في حالة حدوث اختراق.
- تأكد من وجود إجراء لتحديث البرنامج لأية هجمات جديدة أصبحت معروفة. ويمكن بدلاً من ذلك الاعتماد على ما توفره معظم الأدوات المشابهة من خيارات تحميل التحديثات التلقائية عبر الإنترنت. في مثل هذه الحالات، يجب التأكد من تلقي التحديثات من مواقع موثوق بها.

4.4.15 **جدران الحماية الموزعة**

- التأكد من توزيع سياسة الأمن باستمرار على جميع الأجهزة المضيفة، خاصة عند وجود تغييرات في السياسة.
- التأكد من وجود ضوابط كافية لضمان سلامة السياسة أثناء النقل، على سبيل المثال، IPsec لتشفير السياسة عند النقل.
- تأكد من وجود ضوابط كافية لمصادقة المضيف المناسب.

مرة أخرى يمكن استخدام IPsec للمصادقة مع شهادات التشفير.

4.4.16 **استمرارتو افر جدران الحماية**

- تأكد من وجود جدار حماية بديل عن جدار الحماية الأساسي (hot standby for the primary firewall)

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

- رسم تخطيطي للشبكة.
- ضوابط النظام (System configurations).
- قواعد الجدار الناري.
- عناوين بروتوكولات الانترنت (IP Addresses).
- قوائم التحكم في الوصول.

Network Security Policies

Overview

There is no definitive mechanism for protecting a network because any security system can be subverted or compromised, if not from the outside then certainly from the inside. Ultimately to secure a network is to implement different layers of security so that an attacker must compromise two or more systems to gain access to critical assets. The first step in enforcing policies is to define the policies that will be enforced. Security measures often restrict personnel in their operating practices which results in a temptation to boost security regulations. Network policies are, therefore, govern how a network should be implemented and configured to streamline employee's operation in ordinary conditions as well as guides how to react during the occurrence of abnormalities. In this context, the following section explains the imposition of policies measures of each term or principle of network security to protect information and systems.

1. Router and Switch Security Policy

1.1 Introduction

Routers and smart switches provide important security functions within a network. Configured correctly, they are one of several hardware and software devices available that help manage and protect a private network from a public one. The Router and Switch Security Policy defines configuration requirements to meet security standards, change management requirements, and operational requirements.

1.2 Purpose

This document designed to protect the equipment and data of the **(organization)** and its business partners or any data the **(organization)** is in custody of by defining the minimum configuration standards for all routers and switches connecting to the organizational network.

1.3 Scope

All employees, contractors, consultants, temporary and other workers who use network devices such as Router and/or switch must adhere to this policy. All routers and switches connected to networks are affected.

1.4 Policy

1.4.1 Every router/switch must meet the following configuration standards:

1. No local user accounts are configured on the router or switch. Routers and switches must use a dedicated AAA server (e.g. TACACS+) for all user authentication.
2. The enable secret must be used instead of enable password.
3. The enable secret on the router or switch must be kept in a secure encrypted form.
4. The following services or features must be disabled:
    - IP directed broadcasts (Enable IP directed broadcast when you want to perform remote management or administration services such as backups on hosts in a subnet that does not have a direct connection to the Internet).
    - Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.
    - TCP small services
    - UDP small services
    - All web services running on router
    - Auto-configuration.
    - Layer 2 device discovery protocol (e.g. CDP and LLDP) and other discovery protocols
5. Routers and switches and/or interfaces should disallow the following:
    - Proxy-ARP.
    - ICMP unreachable messages.
    - Fast switching and autonomous switching.
    - Multicast route caching.
    - Maintenance Operation Protocol (MOP).
6. The following services must be configured:
    - Password-encryption
    - Time syncing (NTP). All network clocks should be synced to a common time source.
7. All routing updates shall be done using secure routing updates.

8. Use (**organization**) standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

9. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

10. Each router must have a Login banners that useful to inform potential users that use of the login is only for authorized users. the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action in accordance with regulation in force. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

11. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

12. Routers and switches should be placed in a location where physical access is limited to authorized persons only.

13. The switch should disable a port or group of ports if new or unregistered MAC addresses appear on a port if the feature is available.

14. The switch should generate an SNMP trap if the link drops and is re-established if the feature is available

15. Dynamic routing protocols must use authentication in routing updates sent to neighbors. (***Password hashing for the authentication string must be enabled when supported***)

16. The (**organization**) router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

    - IP access list accounting
    - Device logging
    - Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped.

17. Network configurations and changes must be documented regularly to understand its structure. Network documentation should include:

    - Network diagram
    - System configurations
    - Firewall rule set
    - IP Addresses
    - Access Control Lists

2. Wireless Communication Policy

2.1 Introduction

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

A Wireless Communication Policy is necessary for computer security since there is demand for wireless equipment in every (**organization**) today. The Wireless Communication Policy may specify that no wireless equipment should be used but this would not be very good since that may cause some departments or individuals to violate the policy. It is best to set conditions and specify equipment that is approved for wireless use in order to minimize security risk associated with wireless.

2.2 Purpose

The purpose of this policy is to secure and protect the information assets owned by **(Organization)**. **(Organization)** grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to **(Organization)** network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy, or that granted an exception by the Information Security Department are approved for connectivity to a **(Organization)** network.

2.3 Scope

This policy applies to all wireless infrastructure devices that connect to a **(Organization)** network or reside on a **(Organization)** site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data .Therefore, all employees, contractors, consultants, temporary and other workers at **(Organization)**, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of **(Organization)** must adhere to this policy.

2.4 Policy

2.4.1 All wireless infrastructure devices that reside at a **(Organization)** site and connect to a (Organization) network, or provide access to information classified as **(Organization)** Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Use **(Organization)** approved authentication protocols and infrastructure.
- Use **(Organization)** approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.

2.4.2 To stop the possible abuse of wireless network:

- There should be proper user authentication ensured along with the appropriate replacement of WEP and anomaly tracking mechanism on wireless LAN.

- At the same time, there is the following list of suspicious events on wireless LAN which should always consider for intrusion detection as;
    - Beacon frames from unsolicited access point
    - Flood of unauthenticated frames (MITM attack)
    - Frames with duplicated MAC address.
    - Randomly changing MAC address

2.4.3 Wireless encryption protocols

- WAP2 (Wi-Fi Protected Access version 2) is preferred as a wireless encryption protocol instead of WEP (Wired Equivalent Privacy) and WAP (Wi-Fi Protected Access), because WAP2 It offered a much stronger security algorithm and advanced level encryption with message authenticity and integrity validation while WEP and WPA protocols are considered vulnerable.

2.4.4 Network configurations and changes must be documented regularly to understand its structure. Network documentation should include:

- Network diagram
- System configurations
- Firewall rule set
- IP Addresses
- Access Control Lists

3. Virtual Private Network (VPN) Policy

3.1 Introduction

A Virtual Private Network (VPN) is a secured private network connection that provide a convenient way to access internal network resources remotely over the public network (Internet). VPN offers secure access by providing a means to protect data while it travels over an untrusted network.

3.2 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the **(Organization)** corporate network.

3.3 Scope

This policy applies to all **(Organization)** employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the **(Organization)** network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

3.4 Policy

3.4.1 It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to **(Organization)** internal networks through their VPN connection.

3.4.2 VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3.4.3 When actively connected to the corporate network, VPNs will force all traffic to and from the PC used by the remote user over the VPN tunnel: all other traffic will be dropped.

3.4.4 Dual (split) tunneling is NOT permitted; only one network connection is allowed. [*Dual (split) tunneling allows two simultaneous, active connections to a secure network (via VPN) and a non-secure network, without having to disconnect the VPN connection. This security vulnerability allows a direct connection from the non-secured Internet to the VPN secured network.*]

3.4.5 VPN gateways will be set up and managed by **(Organization)** network operational groups.

3.4.6 All computers connected to **(Organization)** internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

3.4.7 VPN users will be automatically disconnected from **(Organization)**'s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. *(Pings or other artificial network processes are not to be used to keep the connection open.)*

3.4.8 The VPN concentrator must be limited to an absolute connection time of 24 hours.

3.4.9 Users of computers that are not **(Organization)**-owned equipment must configure the equipment to comply with **(Organization)**'s VPN and Network policies.

3.4.10 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of **(Organization)**'s network, and as such are subject to the same rules and regulations that apply to **(Organization)**-owned equipment.

3.4.11 Network configurations and changes must be documented regularly to understand its structure. Network documentation should include:

- Network diagram
- System configurations
- Firewall rule set
- IP Addresses
- Access Control Lists

4. Firewall Policy

4.1 Introduction

When a user connects to an insecure, open network, such as the Internet, he opens a large doorway for potential attacks. One of the best ways to defense against exploitation from the insecure network is to employ firewalls at the connection point end, as it is a necessity to safeguard the **(Organization)**'s private networks and communication facilities.

4.2 Purpose

Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. This document seeks to assist **(Organization)** in understanding the capabilities of firewall technologies and firewall policies.

4.3 Scope

This policy defines the essential rules regarding the management and maintenance of firewalls, and it applies to all firewalls owned, rented, leased, or otherwise controlled by **(Organization)**.

4.4 Policy

4.4.1 Review the rulesets to ensure that they follow the order as follows:

- anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)

- User permit rules (e.g. allow HTTP to public webserver)
- Management permit rules (e.g. SNMP traps to network management server)
- Deny and Alert (alert systems administrator about traffic that is suspicious)
- Deny and log (log remaining traffic for analysis)

4.4.2 Application based firewall:

- In the case of dedicated server access, an **application proxy firewall** must be placed between the remote user and dedicated server to hide the identity of the server.
- Ensure that the administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall.
- Ensure that there is a process to update the application level firewall's vulnerabilities checked to the most current vulnerabilities.
- Ensure that there is a process to update the software with the latest attack signatures.
- In the event of the signatures being downloaded from the vendors' site, ensure that it is a trusted site.
- In the event of the signature being e-mailed to the systems administrator, ensure that digital signatures are used to verify the vendor and that the information transmitted has not been modified en-route.
- The following commands should be blocked for SMTP at the application level firewall:
    - EXPN (expand)
    - VRFY (verify)
    - DEBUG
    - WIZARD
- The following command should be blocked for FTP:
    - PUT

- Review the denied URL's and ensure that they are appropriate for e.g. any URL's to hacker sites should be blocked.

- Ensure that only authorized users are authenticated by the application level firewall.

4.4.3 Stateful inspection

- Review the state tables to ensure that appropriate rules are set up in terms of source and destination IP's, source and destination ports and timeouts.

- Ensure that the timeouts are appropriate so as not to give the hacker too much time to launch a successful attack.

For URL's

- If a URL filtering server is used, ensure that it is appropriately defined in the firewall software. (If the filtering server is external to the (**Organization**) ensure that it is a trusted source).
- If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's at (**Organization**).

4.4.4 Logging

- Ensure that logging is enabled and that the logs are reviewed to identify any potential patterns that could indicate an attack.

- Network Firewall administration logs (administrative activities) and event logs (traffic activity) should:

    - Be written to alternate storage (not on the same device)
    - Be reviewed at least daily, with logs retained for ninety (90) days.

4.4.5 Patches and updates

- Ensure that the latest patches and updates relating to your firewall product is tested and installed.

- If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.
- In the event that patches and updates are e-mailed to the systems administrator ensure that digital signatures are used to verify the vendor and ensure that the information has not been modified en-route.

4.4.6 Vulnerability assessments/ Testing

- Ascertain if there is a procedure to test for open ports using (NMAP) and whether unnecessary ports are closed.
- Ensure that there is a procedure to test the rulesets when established or changed so as not to create a denial of service on the (**organization**) or allow any weaknesses to continue undetected.

4.4.7 Compliance with security policy

- Ensure that the ruleset complies with the (**organization**) security policy.

4.4.8 Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked:

- **Private (RFC 1918) addresses**

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 - 192.168.255.255

- **Reserved addresses**

240.0.0.0

- **Illegal addresses**

0.0.0.0

- UDP echo
- ICMP broadcast (RFC 2644)

4.4.9 Remote access

- If remote access is to be used, ensure that the SSH protocol (port 22) is used instead of Telnet.

4.4.10 File Transfers

- If FTP is a requirement, ensure that the server, which supports FTP, is placed in a different subnet than the internal protected network.

4.4.11 Mail Traffic

- Ascertain which protocol is used for mail and ensure that there is a rule to block incoming mail traffic except to internal mail.

4.4.12 Block Unwanted ICMP Traffic (ICMP 8, 11, 3)

- Ensure that there is a rule blocking ICMP echo requests and replies.
- Ensure that there is a rule blocking outgoing time exceeded and unreachable messages.

4.4.13 Critical servers

- Ensure that there is a deny rule for traffic destined to critical internal addresses from external sources. This rule is based on the organizational requirements, since some **(organizations)** may allow traffic via a web application to be routed via a DMZ.

4.4.14 Personal firewalls

- Ensure that laptop users are given appropriate training regarding the threats, types of elements blocked by the firewall and guidelines for operation of the personal firewall. This element is essential, since often times personal firewalls rely on user prompt to respond to attacks e.g. whether to accept/deny a request from a specific address.
- Review the security settings of the personal firewall to ensure that it restricts access to specific ports, protects against known attacks, and that there is adequate logging and user alerts in the event of an intrusion.
- Ensure that there is a procedure to update the software for any new attacks that become known.

Alternatively, most tools provide the option of transferring automatic updates via the internet. In such instances ensure that updates are received from trusted sites.

4.4.15 Distributed firewalls

- Ensure that the security policy is consistently distributed to all hosts especially when there are changes to the policy.
- Ensure that there are adequate controls to ensure the integrity of the policy during transfer, e.g. IPsec to encrypt the policy when in transfer.
- Ensure that there are adequate controls to authenticate the appropriate host.

Again IPsec can be used for authentication with cryptographic certificates.

4.4.16 Continued availability of Firewalls

- Ensure that there is a hot standby for the primary firewall

4.4.17 Network configurations and changes must be documented regularly to understand its structure. Network documentation should include:

- Network diagram
- System configurations
- Firewall rule set
- IP Addresses
- Access Control Lists

سياسة الأطراف الثالثة

1. سياسة الوصول للأطراف الثالثة

1.1 مقدمة

تعمل سياسة الوصول للأطراف الثالثة على بيان الإجراءات التي تحكم وصول أطراف ثالثة إلى شبكة (جهة العمل) وتطبيقاتها. وتتمثل الأطراف الثالثة في الجهات الخارجة عن (جهة العمل) من مؤسسات أو أفراد.

تغطي السياسة الجوانب التالية للتعاملات مع الطرف الثالث:

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

1.2 الغرض من السياسة

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

1.3 النطاق

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

1.4 السياسة

1.4.1 يجب التوقيع على اتفاقية عدم الإفصاح عند التعاقد مع الطرف الثالث، وتحديد دور ومسؤوليات الطرف الثالث بوضوح في هذه الاتفاقية.

- لن يُمنح الطرف الثالث إمكانية الوصول إلى مرافق شبكة **(جهة العمل)** إلا بعد توقيع عقد رسمي يحدد الشروط والضوابط التي يجب على الأطراف الثالثة الالتزام بها لضمان الوصول الأمن إلى مرافق شبكة **(جهة العمل)** من قبل الأطراف الثالثة.
- تتطلب جميع طلبات الاتصال الجديدة بين الأطراف الثالثة و**(جهة العمل)** موافقة الطرف الثالث وممثل **(جهة العمل)** على الاتفاقية والتوقيع عليها.

1.4.2 المتطلبات الأولية (قبل الاتفاق): ستخضع عملية منح الوصول لمعدات تقنية المعلومات للمراجعة والتصديق من القسم المختص بذلك (قسم أمن المعلومات).

- تجري المراجعة الأمنية للتأكد من أن أي توصيل يتطابق مع متطلبات العمل بأفضل طريقة ممكنة، وأنه يتبع مبدأ "أقل صلاحيات وصول".
- يجب على جميع الأطراف الثالثة الالتزام بمتطلبات أمن المعلومات والتي تضمن الحد الأدنى من مستوى الأمان الذي تتطلبه **(جهة العمل)** من قبل الطرف الثالث، والتي يتحدد من خلالها ما الذي يجب على **(جهة العمل)** تنفيذه والحفاظ عليه من تدابير أمنية تخص جميع جوانب أمن المعلومات وجميع عمليات الدعم المرتبطة بها.
- يجب على جميع الأطراف الثالثة التأكد من أنها لا تنتهك أيّاً من لوائح نظام إدارة أمن المعلومات في أي وقت أثناء تعاقدها مع **(جهة العمل)**.

1.4.3 إنشاء الاتصال:

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

1.4.4 تعديل أو تغيير الاتصال والوصول:

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

1.4.5 وصول الطرف الثالث المسموح به:

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

1.4.6 الأجهزة والمعدات (محطات العمل) الخاصة بالطرف الثالث:

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

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

1.4.7 وصول الأطراف الثالثة عن بعد:

- يتم تحديد مسؤوليات إدارة أمن وصول الطرف الثالث بوضوح لكل من **(جهة العمل)** والطرف الثالث، كما يجب توفير مستوى مناسب من الإدارة والدعم الفني من قبل الطرفين لضمان تحقيق الامتثال لهذه السياسة.
- يجب تعيين المناصب التالية لكل اتصال بين الأطراف:
  - مسؤول الخدمة أو من له الصلاحية ليكون مسؤولاً عن السماح بدخول الطرف الثالث من خلال تفويض الاتصال في تصريح كتابي.
  - المسؤول عن النظام والذي يتحمل المسؤولية الكاملة عن كل اتصال من الأطراف الثالثة وذلك للتأكد من تطبيق الأطراف للسياسات والمعايير لهذا الاتصال. كما أنه المسؤول عن تأكيد ما إذا كان مسموحًا للطرف الثالث بالدخول إلى أنظمة المؤسسة، وكما له أن يحظر دخول الطرف الثالث إلى بعض الأنظمة الحساسة.

1.4.8 الإبلاغ عن الحوادث: يجب أن تقوم الأطراف الثالثة بإبلاغ الإدارة عن أي حادثة تؤثر على أمن المعلومات والخصوصية، وعلى جميع نقاط الضعف الأمنية المشتبه بها أو ما قد يشكل تهديداً لأصول تقنية المعلومات في **(جهة العمل)**.

1.4.9 إنهاء الوصول:

- عندما انتهاء الحاجة إلى الوصول يجب أن يقوم المسؤول عن الاتصال داخل **(جهة العمل)** بإنهاء الوصول.
- يجب أن يقوم المسؤولون عن كل اتصال بمراجعة هذه الاتصالات سنوياً للتحقق من وجود حاجة لاستمرارها، وأن نوع الوصول الحالي يلبي متطلبات الاتصال المرجوة.
- يتم على الفور إنهاء جميع الاتصالات التي لم يعد لها فائدة أو حاجة في تنفيذ أعمال **(جهة العمل)**.
- في حالة تم تعريفهم داخل نظام **(جهة العمل)**، يجب أن يكون لدى جميع الأطراف الثالثة والمستخدمين الخارجيين تاريخ صلاحية لحساباتهم.

2. القواعد الارشادية لاتفاقية عدم الإفصاح:

2.1 مقدمة

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

2.2 الغرض

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

2.3 النطاق:

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

2.4 القواعد الإرشادية:

2.4.1 يجب على جميع الأطراف الثالثة توقيع اتفاقية عدم الإفصاح كخطوة أولى في بداية عملهم مع **(جهة العمل)**، مع اقرارهم بفهم هذه السياسة والتزامهم بها.

2.4.2 يجب على الطرف الثالث الممنوح له حق الوصول المباشر أو غير المباشر إلى البيانات أو المعلومات التي تملكها **(جهة العمل)** عدم الافصاح عن هذه المعلومات أو نشرها.

2.4.3 تلتزم **(جهة العمل)** بضمان الخدمات السرية لجميع الأطراف الثالثة. فالسرية هي بين الأطراف الثالثة و**(جهة العمل)** وليس للموظفين الذين يقدمون خدمات معينة.

2.4.4 الوثائق التي تحتوي على معلومات شخصية بما في ذلك على سبيل المثال لا الحصر الأسماء أو العناوين أو أرقام الهاتف أو السجلات الطبية أو السجلات المالية لموظفي **(جهة العمل)** يجب أن تكون خاضعة لرقابة دقيقة ويجب عدم الإفصاح عنها أو الكشف عنها لأي أشخاص أو مصادر غير مصرح لهم بذلك.

2.4.5 يجب أن تحتوي اتفاقية عدم الإفصاح على الأقل على الآتي:

- أسماء الأطراف المتعاقدة.
- أي من الأطراف المتعاقدة ملزم بحماية سرية المعلومات المكشوف عنها، سواء كان الطرف المستقبل أو الطرف المفصح عنها أو كليهما (أحادي أو ثنائي)، كما يمكن أن يكون لاتفاقية عدم الإفصاح أكثر من طرفين، وفي هذه الحالة يجب تحديد الأطراف الملزمة بذلك.
- تحديد ماهي المعلومات السرية في الاتفاقية.
- مدة الالتزام بالاتفاقية بالسنوات.
- مدة وشروط الحفاظ على سرية المعلومات بالسنوات.
- المعلومات التي سيتم استبعادها من الاتفاقية، كالمعلومات التي تم معرفتها مسبقاً أو التي تتواجد ومتاحة للعموم، أو التي يُطّلع عليها لاحقاً من أطراف أخرى.
- الشروط والقيود المتعلقة بطرق نقل المعلومات السرية.
- الإجراءات التي ينبغي اتخاذها على المعلومات السرية عند نهاية الاتفاقية.
- مسؤوليات استلام والتعامل مع المعلومات السرية:
  - استخدام المعلومات للأغراض المتفق عليها فقط.
  - الكشف عنها فقط للأشخاص الذين يحتاجون إلى معرفة المعلومات لأداء الاغراض المتفق عليها.
  - استخدام الجهود المناسبة (بدل العناية اللازمة أو الجهود المعقولة) للحفاظ على أمان المعلومات. غالباً ما يتم تعريف الجهود المعقولة على أنها معيار لرعاية المعلومات السرية لا تقل صرامة عن تلك التي يستخدمها المستلم للحفاظ على أمان معلوماته الخاصة.
  - التأكد من أن الاشخاص الذين تم الكشف لهم عن المعلومات يلتزمون بشروط تقييد الاستخدام وتقييد الإفصاح، وضمان حماية المعلومات.
- نوع الإفصاح المسموح به – المعلومات اللازمة للوصول للهدف المطلوب في إطار القانون.
- يجب أن يختار الطرفان القانون والقضاء المختص الذي يحكم تنفيذ الاتفاقية.

Third Party Policy

1. Third Party Access Policy

1.1 Introduction

This policy outlines procedures governing third-party access to **(Organization)** owned systems, network and applications.

A third party is an organization or individual (non-permanent employee) external to the **(Organization)**

The policy covers the following aspects of third party relationships:

- Third party risk assessments
- Agreement and Contracts
- Network service provision
- Authorization of connections
- Security of access by non-permanent employees (both physical and logical)

1.2 Purpose

The purpose of this policy is to define standards for all Third Parties seeking to access the **(Organization)** systems or network for the purpose of transacting business related to **(Organization)**.

This policy is designed to minimize the potential exposure to the **(Organization)** from risks associated with Third Party Access.

1.3 Scope

This policy applies to all **(Organization)** Staff seeking to provide access to the **(Organization)** system, network or devices attached to the network to Third parties, and to all Third Parties whether they are vendors, contractors, consultant or outsourced professionals.

1.4 Policy

1.4.1 A Non-disclosure agreement is essential and must be signed contracting with a third party, and the role and responsibilities of the third party should be clearly defined in the agreement.

- Third party access to **(Organization)** system and network facilities will be given only after the signing of a formal contract defining the terms for the connection which should contain all security requirements by which the third party is to abide.

- All new connection requests between third parties and **(Organization)** require that the third party and **(Organization)** representatives agree to and sign the Agreement.

1.4.2 Pre-Requisites: All new connectivity will go through a security review and approval with the Information Security department.

- The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.
- All third parties must follow the information security requirements that determine the minimum level of security the **(Organization)** requires to be achieved by the third party. These set out the security measures that must be implemented and maintained by the **(Organization)** in relation to all aspects of information security and all associated supporting processes.
- All third parties must ensure that they do not breach any of the information security management system statements at any time during their contract with the **(Organization)**.

1.4.3 Establishing Connectivity

- All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review.

1.4.4 Modifying or Changing Connectivity and Access

- All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via **(Organization)** change management process.

1.4.5 Permitted Third Party Access

- Third Party Access to the **(Organization)**'s systems or network should be made only for the purposes agreed in the contract, this shall be applied to **(Organization)** partner not employed directly by the **(Organization)** who has remote or direct access to the **(Organization)**'s systems and network.
- Third party access must be permitted only to the facilities, services and data, which are required to perform the specified tasks, as outlined to the IT appropriate Network Manager/Administrator in the original request for access.

1.4.6 Third Party Workstations

Where Third Parties use PC's / Laptops or any other devises not owned or managed by the **(Organization)** to access the resources on the **(Organization)**'s network and systems, Third Parties must ensure the following:

- Operating Systems should be fully up-to-date with patches.
- Anti-virus software should be fully up-to-date with patches and virus definitions.
- Anti-spyware/malware software should be fully up-to-date with patches and malware definitions.

1.4.7 Remote Access by Third Parties

- Responsibilities for security management and administration of third party access will be assigned clearly to both **(Organization)** and the third party. An appropriate level of management and technical support will be provided by both parties to ensure that compliance with this policy is achieved.
- For each party connection, the following positions must be appointed:
  - A Head of Service Area or delegated authority who will be responsible for permitting third party access by authorizing the connection on a written authorization form.
  - A System Owner who will have overall responsibility for each third party connection to ensure that the policy and standards are applied. They are also responsible for confirming whether third party access to their systems would be permitted and may prohibit third party access to certain sensitive systems.

1.4.8 Incident Reporting: Third Parties shall report to management any incident affecting information security and privacy, and all observed and suspected security weaknesses in or threats to Information Technology Assets

1.4.9 Terminating Access

- When access is no longer required, the responsible of access and connection in **(Organization)** must terminate the access.
- The responsible of connection must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection.
- Connections that are found to be depreciated, and/or are no longer being used to conduct **(Organization)** business, will be terminated immediately.

- All Third party and external users, if defined on the system, should have a mandatory expiry date.

2. Non-disclosure / Confidentiality Agreement Guideline

2.1 Introduction

Confidentiality Agreements are must be signed when **(Organization)** is considering entering into a business relationship with a third party and where there is a need to understand or evaluate each other's business processes, some of which might be proprietary or otherwise sensitive in nature.

2.2 Purpose

The purpose of this guideline is to ensure a consistent process for the signing and retention of the **(Organization)** Information Confidentiality Agreement by all individuals having access to **(Organization)** confidential information.

2.3 Scope

This guideline applies to **(Organization)** and to all Third Parties whether they are vendors, contractors, consultant or outsourced professionals.

2.4 Statement of Guidelines

2.4.1 All third parties are required to sign an Information Confidentiality Agreement at the initial start of their contractual relationship, acknowledging they understand and will adhere to this policy.

2.4.2 Where a Third Part has direct or indirect access to data or information owned by the **(Organization)**, this information must not be divulged or distributed to anyone.

2.4.3 **(Organization)** is committed to ensuring confidential services to all third parties. The confidentiality is between the third parties and the organization, not the members of staff delivering a particular service.

2.4.4 Documents which contain personal information including but not limited to names, addresses or telephone numbers, medical records, financial records of **(Organization)** staff must be carefully controlled and must not be released or disclosed to any unauthorized individuals or sources.

2.4.5 The agreement should at least address the following:

- The names of the contracting parties.
- Which party of the contracting entities is obligated to protect the secrecy of the disclosed information, whether it is the receiving party or the disclosing one or both (Unilateral or Bilateral). Furthermore, NDAs could have more than two parties, therefore such NDAs should address which parties are to be obligated.

- Defining what is to be confidential.
- The term (in years) the agreement is binding.
- The term and conditions (in years) of the confidentiality, i.e. the time period of confidentiality.
- Information that to be excluded from the NDA. Such as having a prior knowledge of the information, being in public domain, or subsequently gained from other parties.
- Restrictions regarding the transfer of confidential information.
- Required actions that should be taken with the confidential information upon NDA's ending.
- The responsibilities of the recipient concerning the confidential information:
    - Using the information only for the agreed upon purposes.
    - To reveal it only to people with a need to know the information for those purposes.
    - To use appropriate efforts (not less than reasonable efforts) to keep the information secure. Reasonable efforts are often defined as a standard of care relating to confidential information that is no less rigorous than that which the recipient uses to keep its own similar information secure.
    - To ensure that anybody to whom the information is revealed further abides by obligations restricting use, restricting disclosure, and ensuring security at least as protective as the agreement.
- Types of allowed disclosure – such as those required by law or court order.
- The parties should choose the law and jurisdiction that is governing their agreement.

سياسة النسخ الاحتياطي

1. مقدمة

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

يعمل النسخ الاحتياطي على مايلي:

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

2. الغرض من السياسة

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

3. النطاق

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

4. السياسة

4.1. تحديد البيانات الهامة

4.1.1 يجب ان تحدد **(جهة العمل)** البيانات الأكثر أهمية لها وذلك من خلال عملية تصنيف البيانات ومن خلال مراجعة أصول المعلومات، حيث يجب تحديد البيانات الهامة والحرجة بحيث يمكن منحها أولوية أعلى أثناء عملية النسخ الاحتياطي.

4.1.2 البيانات التي يتم نسخها احتياطياً

سيتم الاحتفاظ بنسخة احتياطية من:

- جميع البيانات التي تقرر أنها هامة وحساسة لأعمال **(جهة العمل)** و/أو وظيفة الموظف.
- جميع المعلومات المخزنة على خادم الملفات التابعة لـ **(جهة العمل)**. وتقع على عاتق المستخدم ضمان نقل أي بيانات ذات أهمية إلى خادم الملفات.

- جميع البيانات المخزنة على خوادم الشبكة، والتي قد تتضمن خوادم الويب وخوادم قواعد البيانات ووحدات التحكم في النطاق والجدران النارية وخوادم الوصول عن بعد.

4.2 تخزين النسخ الاحتياطي

4.2.1 عند التخزين في موقع **(جهة العمل)** يجب ان تخزن وسائط النسخ الاحتياطي في حاوية مقاومة للحريق في منطقة مؤمنة بضوابط تحكم بالدخول.

4.2.2 يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع **(جهة العمل)**، بمسافة مناسبة وذلك للحماية من الحرائق أو الفيضانات أو الكوارث الإقليمية أو الكبيرة الأخرى، للابتعاد عن أي ضرر في حالة حدوث كارثة في الموقع الرئيسي.

4.2.3 عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع يجب ضمان -وبشكل معقول- عدم تعرضها للكوارث كالسرقة أو النار،كما يجب اختيار أماكن تخزين تستخدم أساليب حماية من الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي.

4.2.4 يسمح بالنسخ الاحتياطي عبر الإنترنت إذا كانت الخدمة تلبي المعايير المحددة هنا.

4.3 تكرار النسخ الاحتياطي

4.3.1 يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.

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

4.3.3 يجب تذكير جميع الموظفين بأن كلاً منهم مسؤول بصورة شخصية عن البيانات الموجودة على أجهزة كمبيوتر سطح المكتب أو الكمبيوتر المحمول التي في عهدتهم، ويقع على عاتقهم مسؤولية تخزين جميع البيانات المهمة الموجودة لديهم على وسائط النسخ الاحتياطي المستخدمة في **(جهة العمل)**.

4.3.4 يجب تحديد المستوى الذي تكون عنده المعلومات ضرورية ويتعين تخزين نسخ احتياطية لها.

4.3.5 يجب اختبار وتوثيق إجراءات استعادة البيانات، كما يجب أن تحدد الوثائق من هو المسؤول عن عملية استعادة البيانات وكيف يتم تنفيذها وتحت أي ظروف يجب تنفيذها والمدة التي تستغرقها كامل العملية بدأً من الطلب وانتهاءً إلى استعادة البيانات، من المهم للغاية أن تكون الإجراءات واضحة وموجزة بحيث لا تكون مربكة ويساء تفسيرها في وقت الأزمات من قبل القراء بخلاف مسؤول النسخ الاحتياطي.

4.4 الاحتفاظ بالنسخ الاحتياطي

4.4.1 يجب أن تحدد **(جهة العمل)** الوقت اللازم للاحتفاظ بالنسخ الاحتياطي، وما عدد النسخ المخزنة من البيانات المنسوخة احتياطياً الكافية للحد من المخاطر بكفاءة مع الحفاظ على البيانات المطلوبة.

4.4.2 يجب الاحتفاظ بنسخ احتياطية وفقًا لجدول الحفظ والتخلص من النسخ الاحتياطي، يحدد الجدول حالة البيانات فيما إذا كان يمكن التخلص منها أو إعادة تدويرها أو إبقاؤها في مخزن الأرشيف.

4.5 النسخ المخزنة

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

تاريخ النسخ الاحتياطي / اسم المؤرِد / نوع طريقة النسخ الاحتياطي (كامل / تزايدي).

4.5.2 يجب الاحتفاظ بسجل للحركات المادية والالكترونية لجميع النسخ الاحتياطية، يجب أن تشير الحركة المادية والالكترونية للنسخ الاحتياطية إلى:

- النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين.
- أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخر.

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

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

4.5.4 يجب توفير مستوى حماية مناسب للمعلومات المخزنة في موقع التخزين الاحتياطي وفقاً للمعايير المطبقة في الموقع الرئيسي، كما ينبغي ان تمتد الضوابط المطبقة على وسائط النسخ الاحتياطي في الموقع الرئيسي لتشمل موقع التخزين الاحتياطي.

4.6 اختبار عملية استعادة البيانات

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

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

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

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

- للتحقق من الأخطاء وتصحيحها.
- لمراقبة مدة عملية النسخ الاحتياطي.
- لتحسين أداء النسخ الاحتياطي حيثما أمكن ذلك.

4.7 وسائط النسخ الاحتياطي

4.7.1 يجب حماية وسائط النسخ الاحتياطي من الوصول غير المصرح به أو سوء الاستخدام أو العبث بها، بما في ذلك الحماية الكافية لتجنب أي ضرر مادي ينشأ أثناء عملية نقلها أو تخزينها. لذا يجب على جميع الموظفين المسؤولين عن معالجة النسخ الاحتياطي للبيانات الآتي:

- أثبات هوية ذو صلة
- إذن تخويل ذو صلة

4.7.2 عند الحاجة إلى ضوابط خاصة لحماية المعلومات السرية أو الحساسة، ينبغي مراعاة ما يلي:

- استخدام أماكن تخزين (حاويات) آمنة.
- التسليم باليد.
- في الحالات الحرجة يتم تقسيم ما سيتم تسليمه إلى أجزاء يرسل كل جزء عبر طريق مختلفة عن غيره.

4.7.3 يجب تخريد جميع وسائط النسخ الاحتياطية بشكل مناسب، يتم تخريد الوسائط والتخلص منها كما هو موضح أدناه:

- يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.
- يجب ان لا تحتوي الوسائط على نسخ احتياطية يمكن إعادة استخدامها (فعالة).
- يجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو استرجاعها من قبل طرف غير مصرح له.
- يجب العمل على أن تتلف وسائط النسخ الاحتياطي ماديا بحيث لا يمكن استعادة محتوياتها قبل التخلص منها.

4.7.4 أنواع معينة من وسائط النسخ الاحتياطي لها عمر وظيفي محدود، إذ أنه بعد مدة معينة من الخدمة لن يكون بالإمكان اعتبار هذه الوسائط موثوقًا بها. عند وضع وسائط النسخ الاحتياطي في الخدمة يجب تسجيل التاريخ عليها، ليتم إيقافها عن الخدمة بعد أن يتجاوز وقت استخدامها مواصفات المصنع.

Data Backup Policy

the method, critical data should be identified so that it can be given the highest priority during the backup process.

4.1.2 Data to be Backed Up

- All data determined to be critical to **(Organization)** operation and/or employee job function.
- All information stored on the **(Organization)** file server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

4.2 Backup Storage

4.2.1 When stored onsite, backup media must be stored in a fireproof container in an access-controlled area.

4.2.2 Geographic separation from the backups (sufficient distance) must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes, to escape any damage from a disaster at the main site.

4.2.3 When moved offsite, backup media should be reasonably secured from theft or fire, and should be stored in a hardened facility that uses accepted methods of environmental controls, and access controlled secure, to ensure the integrity of the backup media.

4.2.4 Online backups are allowable if the service meets the criteria specified herein.

4.3 Backup Frequency/Procedure

4.3.1 Backups shall be carried out at regular intervals.

4.3.2 Backup frequency is critical to successful data recovery. **(Organization)** has to determine a backup schedule for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

4.3.3 All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the backup media used at **(Organization)**.

4.3.4 The necessary level of back-up information should be defined.

4.3.5 The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not misinterpreted by readers other than the backup administrator, and confusing during a time of crisis.

4.4 Backup Retention

4.4.1 **(Organization)** should determine the time required for backup retention, and what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data.

4.4.2 Backup copies must be maintained in accordance with the Retention and Disposal Schedule for backup copies. The schedule will determine the status of the information, as to whether it can be disposed of, cycled back into production or remain in archive storage.

4.5 Stored copies

4.5.1 Stored copies must be stored with a short description that includes the following information: Backup date / Resource name / type of backup method (Full/Incremental).

4.5.2 A record of the physical and logical movements of all backup copies shall be maintained. Physical and logical movement of backup copies shall refer to:

- The initial backup copy and its transit to storage.
- Any movement of backup copies from their storage location to another location.

4.5.3 Stored copies must be made available upon authorized request:

The request for stored data must be approved by an authorized person nominated by a Director/Manager in the appropriate department. Requests for stored data must include:

- Completion of a form that outlines the specifics of the request, including what copy is being requested, where and when the requester would like it delivered and why they are requesting the copy.
- Acknowledgment that the backup copy will be returned or destroyed promptly upon completion of its use.
- Submission of a return receipt as evidence that the backup copy has been returned.

4.5.4 Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the backup site.

4.6 Restoration Testing

4.6.1 Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery, and report on its ability to recover data.

4.6.2 Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.

4.6.3 Backup restores must be tested when any change is made that may affect the backup system.

4.6.4 On a daily basis, log information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.

4.7 Backup Media

4.7.1 Backup media in transit and store shall be protected from unauthorized access, misuse or corruption, including sufficient protection to avoid any physical damage arising during transit and store. All personnel responsible for data backup processing shall have:

- Relevant identification
- Relevant authorization.

4.7.2 Where special controls are required, i.e. to protect sensitive or critical information, the following should be considered:

- Use of a secured container(s).
- Hand delivery.
- In extreme cases, the delivery split and dispatched by separate routes.

4.7.3 All backup media shall be appropriately disposed of. Media will be retired and disposed of as described below:

- Prior to retirement and disposal, the media must be prepared.
- The media should no longer contains active backup images.
- The media's current or former contents shouldn't be read or recovered by an unauthorized party.
- Physical destruction of all backup media should be prior to disposal.

4.7.4 Certain types of backup media have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

سياسة الأمان المادي

1. مقدمة

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

2. الغرض

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

3. النطاق

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

4. السياسة

4.1. بند العقار

4.1.1. مخاطر الكوارث الطبيعية

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

4.1.2. مخاطر الكوارث من صنع الإنسان

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

4.1.3. البنية التحتية

يجب أن يعتمد مركز البيانات على المنشآت المزودة للطاقة الكهربائية بنسبة لا تقل عن 99.9%، ولا بد أن يتم تزويد الكهرباء للموقع من محطتين (أو أكثر) فرعيتين منفصلتين ويفضل أن تتصل كل منهما بمحطات توليد منفصلة، ويجب أن يتوفر بالموقع مصدرين للمياه، كما لا بد من توفير أكثر من مزود خدمة واحد للاتصال بالشبكة.

4.1.4. تفرد الغرض

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

4.1.5. محيط الموقع:

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

4.1.5.1. المراقبة:

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

4.1.5.2. موضع نوافذ غرف الخوادم:

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

4.1.5.3. نقاط الدخول:

يجب أن تتواجد طريقة للمصادقة التلقائية عند كل نقاط الدخول بـ **(جهة العمل)**، كما يجب توثيق دخول المواد والمعدات وكل الأشياء التي يصطحبها الأفراد الداخلين لـ **(جهة العمل)** من قبل عناصر الحراسة، كما يجب متابعتها عند المغادرة مع تحديد الزمن

وهوية الشخص، ولذلك يجب أن يتوفر بمقر الحراسة إمكانية الوصول لقاعدة بيانات شارات (Badges) المصادقة والتي يجب أن تحتوي على صورة لحامل الشارة، كما يجب أن تحتوي الشارة ذاتها على صورة لحاملها.

4.1.6. غرف الخوادم:

4.1.6.1. الدخول

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

4.1.6.2. البنية التحتية

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

4.1.6.3. البيئة

درجة الحرارة في كل غرفة يجب أن يحافظ عليها ما بين 12 و 24 درجة مئوية، كما يجب أن تبقى الرطوبة ما بين 20% و 80%، ويتوجب مراقبة درجة الحرارة والرطوبة باستخدام حساسات تركب داخل الغرف وأن توثق قراءاتهما وترسل إلى مركز عمليات الشبكة (NOC).

4.1.6.4. الوقاية من الحرائق

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

4.1.7. المرافق

4.1.7.1. أنظمة التبريد

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

4.1.7.2. الطاقة

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

4.1.7.3. القمامة

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

4.1.7.4. مركز عمليات الشبكة (NOC)

يجب توفير أنظمة مراقبة للحريق والطاقة والطقس ودرجة الحرارة والرطوبة بمركز عمليات الشبكة (NOC)، كما يجب أن يكون هناك طرق بديلة احتياطية ليتواصل المركز مع العالم الخارجي، كما يجب تواجد أطقم (الموظفين المختصين) في المركز على مدار 24 ساعة طول أيام الأسبوع، ويوصي أن يقوم موظفي المركز بمتابعة وكالات الأنباء للاطلاع على أي أحداث قد يكون لها تأثير على أمان مركز البيانات.

4.1.8. التعافي من الكوارث

4.1.8.1. خطة التعافي من الكوارث

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

4.1.8.2. التخزين الاحتياطي خارج الموقع

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

4.2. بند ما يخص البشر

4.2.1. الغير عاملين بمركز البيانات

4.2.1.1. الحراس

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

4.2.1.2. أطقم النظافة

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

4.2.1.3. مهندسي الصيانة

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

4.2.1.4. الزوار

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

4.2.2. المستخدمين

4.2.2.1. التوعية

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

4.2.2.2. السياسة

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

4.2.3. التعافي من الكوارث

4.2.3.1. الهيكل التنظيمي

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

4.2.3.2. توثيق مهام العمل

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

4.2.3.3. التدريب على مهام الزملاء

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

4.2.3.4. معلومات التواصل

يجب حفظ وتحديث بيانات التواصل الخاصة بكل موظفي مركز البيانات

4.2.3.5. العمل عن بعد

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

Physical Security Policy

1. Introduction

Physical security is a set of security measures adopted to make sure that only authorized individuals are allowed access to resources, equipment, and other assets in a data center. Physical security procedures and measures can consist of a broad spectrum of methods to discourage intruders, which may also resort to methods based on technology. A well employed physical security policy protects the data center's resources and equipment against theft, vandalism, natural disaster, sabotage, cyber-attack and other malicious acts. All personnel should make themselves aware of the contents of the security policy and adhere to those parts of the policy that cover their areas of work.

2. PURPOSE

It is essential to state and enforce physical and environmental controls in order to protect information assets and systems from unauthorized access, and defense against environmental threats. This policy sets out the requirements for the protection of data centers from both physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within.

3. SCOPE

This policy describes the physical security requirements for the **(ORGANIZATION)**'s Data Center, including Network Operating Center (NOC) offices and the data center, and all contents therein. It covers a wide variety of property and people requirements. All employees, contractors, service engineers, and agents of the **(Organization)** are covered by this policy and expected to comply with its requirements.

4. POLICY

4.1 Property Section

4.1.1 Natural Disaster Risks

The location of the data center **should** be selected where the risk of natural disasters is at acceptable levels. Natural Disasters include but are not limited to lightning storms, heavy rain, sandstorms and floods.

4.1.2 Man-Made Disaster Risks

The site **should** be within an area where the risk of man-made disaster is as low as possible. Man-made disasters include but are not limited to plane crashes, riots, explosions, armed conflicts, and fires. The Site **should not** be adjacent to airports, prisons, freeways, stadiums, and parade routes.

4.1.3 Infrastructure

The reliability of the facilities providing electrical power to the site **should** be at 99.9% or better. Electricity **must** be received from two separate substations (or more) preferably attached to two separate power plants. There **should** be two sources of water available to the site. There **must** be connectivity to more than one access provider at the site.

4.1.4 Sole purpose

Data center **should not** share same space with other offices, especially those not owned by the same entity. In case the data center must share space with other offices, it **should not** have walls adjacent to them.

4.1.5 Site Perimeter

Each entry point of the data center **should** be guarded, where the data center employees' access to the facility should be controlled using a reliable method of automatic authentication. There **should not** be anything that could obstruct the surveillance via CCTV camera or by the patrolling guards in the surrounding areas. There **should not** be a sign advertising that the place is in fact a data center or what **(Organization)** owns it.

4.1.5.1 Surveillance

CCTV cameras **should** be installed outside the building to monitor places nearby properties. Guards **should** patrol the property's perimeter regularly. All vehicles belonging to (Organization)'s staff, contractors, guards, and cleaning crew **should** be issued parking permits. Others **should** only be allowed to use the visitor parking areas. Vehicles not fitting either of these classifications should be towed.

4.1.5.2 Outside Windows and Computer Room Placement

The rooms containing the computers **should not** have windows to the outside. Those windows pose the risk of remote eavesdropping and the introduction of extra heat from casting sunlight inside the rooms. Those rooms **should** also be located in the interior of the data center. If they must have a wall at the edge

of the data center, a physical barrier **should** be placed outside the wall preventing any direct access the room's wall.

4.1.5.3 Access Points

Automatic authentication technique **should** be placed at all entry points of the facility. Any equipment or items accompanying any individual entering the facility **should** be logged by security guards when entering and accounted for on exit detailing the time and person's identity. Access to the authentication badges database **should** be available at the security kiosk, where the pictures of badge's holder must be accessible. Badges **must** have a picture of the holder.

4.1.6 Server Rooms

4.1.6.1 Access

Signs designating the room as restricted access and prohibiting food, drink, and smoking in the servers' room **should** be present. Its doors **should** be equipped with an automatic authentication method. Besides, the doors **should** be fireproof. Only two doors **should** be at each server room. Due to the lack of windows, one door is considered a poor design in most fire codes. Access to computer rooms **should** only be granted to those maintaining the servers or room's infrastructure. During holidays, access **should** be restricted to emergencies.

4.1.6.2 Infrastructure

Server rooms **should** be monitored by CCTV cameras. Redundant access to power, cooling, and connectivity **should** be present at each computer room. The server rooms **should** have a raised floor of around 46 centimeters in order to provide air flow and cable management. Besides, those rooms **should** be equipped with air filtration. Server room's ceiling **should** be high to allow for heat dissipation.

4.1.6.3 Environment

The temperature at each server room **should** be maintained between 12 and 24 degrees Celsius. The humidity **should** be kept between 20% and 80%. Both the temperature and humidity **should** be monitored using sensors installed in the rooms and their readings needs to be logged and reported to the Network Operating Center.

4.1.6.4 Fire Prevention

A total flooding agent solution **should** be in place in each server room. Suitable fire extinguishers **must** be placed in each server room. Preferable Pipe sprinkler systems **must not** be used in server rooms.

4.1.7 Facilities

4.1.7.1 Cooling Systems

There **must** be redundant cooling system in place. Outdoor Parts of the Cooling Systems **must** be secluded from the car park of the Data Center.

4.1.7.2 Power

The server room **must** have at least battery based power source onsite with that can provide enough time of operation to switch over to fossil fuel power generation. In case there is no fossil fuel backup, the battery should last for at least 24 hours. The fuel **should** be enough for 24 hours and it **should** be stored onsite, while there **should** be a contract to obtain up to a week worth already in place.

4.1.7.3 Trash

While dumpsters **should** be monitored by CCTV cameras, all paper documents containing any sensitive information **should** be at least shredded onsite or destroyed beyond retrieval before discarding them.

4.1.7.4 Network Operating Center (NOC)

The NOC **must** have fire, power, weather, temperature, and humidity monitoring systems in place. There **must** be redundant methods of communication between the NOC and the outside world. It **must** be manned 24/7. It is recommended that NOC staff need to monitor news outlets for events effecting the security of the data center.

4.1.8 Disaster Recovery

4.1.8.1 Disaster Recovery Plan

The data center **must** have a disaster recovery plan. Ensure that the plan addresses the following questions: What constitutes a disaster? Who gets notified regarding a disaster and how? Who conducts damage assessment and decides what back-up resources are utilized? Where are backup sites located and what is done to maintain them on what schedule? How often and under what conditions is the plan updated? If the organization does not own the data center what downtime does the service level agreement with the center allow? A list of people within the organization to notify **must** be maintained by the NOC of the data center including office, home, and mobile phone numbers and Instant Message Names if available. How often are those people updated?

4.1.8.2 Offsite Backup

There **must** be regular offsite backups of sensitive data. A backup policy **must** be issued and implemented regarding the steps that should be followed to restore backup and containing a schedule of rehearsals for testing the readiness of the backup procedures.

4.2 People Section

4.2.1 Outsiders

4.2.1.1 Guards

All security guards **should** be submitted to criminal background checks prior to hiring and repeated regularly. They **should** be familiarized and trained on strictly enforcing the physical security policy.

4.2.1.2 Cleaning Crews

All Cleaning staff **should** work in groups of at least two. Cleaning crew **should** be restricted to offices and the NOC. If cleaning staff must access a Computer Room for any reason they **must** be escorted by NOC personnel.

4.2.1.3 Service Engineers

The times of entering and leaving the premises of the service engineers **must** be logged at the building entrance. The NOC staff **should** log the Service Engineers' badge exchange to access a server room.

4.2.1.4 Visitors

Visitors **must** be accompanied by the person whom they are visiting all the time during their visit. Visitors **must not** be permitted access to a server room without written consent from data center administration. All visitors who enter Computer Rooms **must** sign Non-Disclosure Agreements.

4.2.2 Users

4.2.2.1 Education

The users **must** be aware of the risk of shoulder surfing and other social engineering methods and they **must** be trained to watch out for intruders. They also **should** be trained on securing desktops and laptops within the center and laptops outside of it, awareness of surroundings, and emergency procedures.

4.2.2.2 Policy

All users at the data center **must** sign Non-Disclosure Agreements. A Physical Security Policy **should** be signed by each user and enforced by security guards.

4.2.3 Disaster Recovery

4.2.3.1 Organizational Chart

An organizational chart should be maintained detailing job function and responsibility. Ideally the organization chart would also have information on which functions the worker has been cross trained to perform.

4.2.3.2 Job Function Documentation

It's not enough to document only what current employees know at the moment about existing systems and hardware. All new work, all changes, must be documented as well

4.2.3.3 Cross Training

Data Center employees should be cross trained in a number of other job functions. This allows for a higher chance of critical functions being performed in a crisis.

4.2.3.4 Contact Information

A contact database **must** be maintained with contact information for all Data Center employees.

4.2.3.5 Telecommuting

Data Center employees should regularly practice telecommuting. If the data center is damaged or the ability to reach the data center is diminished then work can still be performed remotely.

4.2.3.6 Disparate Locations

If the organization has multiple Data Centers then personnel performing duplicate functions should be placed in disparate centers. This allows for job consciousness to remain if personnel at one center are incapacitated.