الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

السياسات الوطنية لأمن وسلامة المعلومات

الإصدار الثاني 2.0



ليبيا
نوفمبر - 2021
رقم الإصدار 2.0
www.nissa.gov.ly
© NISSA - Nov. 2021

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

السياسات الوطنية لأمن وسلامة المعلومات

الإصدار الثاني 2.0



ليبيا
نوفمبر - 2021
رقم الإصدار 2.0
www.nissa.gov.ly

© NISSA - Nov. 2021

إعداد

فريق تجهيز دليل إرشادي
لسياسات ومعايير أمن وسلامة المعلومات

مراجعة

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

اعتماد

مدير عام الهيئة

Prepared By

Information Security Policy Manual Team

Reviewed By

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

Approved By

NISSA General Manager

دولـــــــة ليبيا

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

رقم (44) لسنة 2021ميلادي

بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات:

- بعد الإطلاع على الإعلان الدستوري الصادر في أغسطس 2011ميلادي وتعديلاته.
- وعلى الاتفاق السامي الموقع بتاريخ 17 ديسمبر 2015 ميلادي.
- اللائحة الإدارية للهيئة العامة للإتصالات والمعلوماتية.
- وعلى القانون رقم (12) لسنة 2010 ميلادي بإصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013 ميلادي بشأن إنشاء الهيئة الوطنية لأمن وسلامة المعلومات.
- وعلى قرار وزير الاتصالات والمعلوماتية رقم (52) لسنة 2013ميلادي بشأن اعتماد الهيكل التنظيمي للهيئة الوطنية لأمن وسلامة المعلومات وتعديلاته.
- وعلى كتاب السيد/ نائب مدير عام الهيئة رقم (1/763) بتاريخ 2021/12/14 ميلادي.
- وعلى كتاب السيد/ مدير مكتب المدير العام رقم (2/765) بتاريخ 2021/12/14 ميلادي.
- وعلى ما تقتضيه المصلحة العامة.

قـــــــــرر

المادة الأولى

تُعتمد السياسات الوطنية لأمن وسلامة المعلومات وتعمم على كافة الوزارات والمؤسسات والشركات العامة والخاصة لتتولى تنفيذها والإلتزام بها وتعميمها على الجهات التابعة لها لضمان أمن وسلامة المعلومات والبيانات الخاصة بها ضد التهديدات السيبرانية، وتتمثل السياسات في الآتي:

ت	السياسة	ت	السياسة
1	سياسة تصنيف المعلومات	2	سياسة حماية البيانات
3	سياسة الإحتفاظ بالسجلات وإتلافها	4	سياسة نشر البيانات
5	سياسة الوصول للبيانات	6	سياسة الإستخدام المقبول
7	سياسة كلمة السر (المرور)	8	سياسة أستعمال البريد الإلكتروني
9	سياسة استخدام الإنترنت	10	سياسة أمان محطات العمل (الكمبيوتر وملحاقاته)
11	سياسة الحماية من البر مجيات الخبيثة	12	سياسة التوعية والتدريب
13	سياسة الوسائط القابلة للإزالة	14	سياسة جهاز التوجيه ومبدل الشبكة

يتبع ...

يتبع قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

رقم (44) لسنة 2021ميلادي بشأن اعتماد السياسات الوطنية لأمن وسلامة المعلومات

15	سياسة الإتصالات اللاسلكية	16	سياسة الشبكة الإفتراضية الخاصة (VPN)
17	سياسة جدار الحماية الناري (Firewall)	18	سياسة التشفير
19	سياسة أمان الحوسبة السحابية	20	سياسة الوصول للأطراف الثالثة
21	القواعد الإرشادية لاتفاقية عدم الإفصاح	22	سياسة الوصول عن بعد
23	سياسة الأمان المادي	24	سياسة التعامل مع الحوادث
25	سياسة النسخ الإحتياطي	26	سياسة خطة التعافي من الكوارث
27	سياسة خصوصية بيانات العملاء		

المادة الثانية

تلتزم كافة المؤسسات العامة والخاصة بوضع هذه السياسات موضع التنفيذ والتطبيق العملي لضمان سلامة معلوماتها وبياناتها.

المادة الثالثة

يُعمل بهذا القرار اعتباراً من تاريخ صدوره، وعلى المخاطبين بأحكامه تنفيذه.

م. صلاح الدين أبوزيد التبيني
مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

صدر في طرابلس بتاريخ 16 / 12 /2021م
الشؤون القانونية محمد

المحتويات

توطئة 8
1.سياسة تصنيف المعلومات 11
2.سياسة حماية البيانات 15
3.سياسة الاحتفاظ بالسجلات وإتلافها 19
4.سياسة نشر البيانات 25
5.سياسة الوصول للبيانات 27
6.سياسة الاستخدام المقبول 29
7.سياسة كلمة السر/المرور 38
8.سياسة استعمال البريد الإلكتروني 44
9.سياسة استخدام الإنترنت 49
10.سياسة أمان محطات العمل (الكمبيوتر وملحقاته) 55
11.سياسة الحماية من البرمجيات الخبيثة 59
12.سياسة التوعية والتدريب 65
13.سياسة الوسائط القابلة للإزالة 71
14.سياسات جهاز التوجيه ومبدل الشبكة 77
15.سياسة الاتصالات اللاسلكية 83
16.سياسة الشبكة الافتراضية الخاصة (VPN) 87
17.سياسة جدار الحماية/الناري (Firewall) 91
18.سياسة التشفير 101
19.سياسة أمان الحوسبة السحابية 107
20.سياسة الوصول للأطراف الثالثة 123
21.القواعد الإرشادية لاتفاقية عدم الإفصاح 126
22.سياسة الوصول عن بعد 133
23.سياسة الأمان المادي 139
24.سياسة التعامل مع الحوادث 151
25.سياسة النسخ الاحتياطي 171
26.سياسة خطة التعافي من الكوارث 180
27.سياسة خصوصية بيانات العملاء 186

توطئة

تسعى الهيئة الوطنية لأمن وسلامة والمعلومات بجدية للرفع من مستوى الوعي العام بضرورة ترسيخ مفاهيم ومبادئ وممارسات الأمن المعلوماتي في مختلف تصنيفات جهات العمل الخاص و العام، مواكبةً بذلك للتطور المستمر الذي يتسم به قطاع تكنولوجيا المعلومات وما ارتبط به من تطورٍ موازٍ في أساليب الحفاظ على استمرارية و كفاءة و فاعلية و أمن العناصر المرتبطة بتكنولوجيا المعلومات.

من المعروف أن أمن المعلومات يتمتع بالدور المحوري في حماية أصول الشركات والمؤسسات، وقد شهدنا مؤخراً ما نتج عن الحوادث الأمنية من قرصنة للخوادم وتسريب البيانات وتشويه سمعة المؤسسات والشركات في كل أنحاء العالم، وقد أصبحت كابوساً يُقلق راحة أصحابها والمسؤولين عليها، بل وقد اتسعت دائرة القلق لتشمل موظفيها وعملائها، وهنا تظهر الحاجة المستمرة والمتزايدة لتكريس موارد تلك الشركات والمؤسسات في القطاع الحكومي والخاص على حد سواء لحماية معلوماتها والحفاظ على سرية وتكامل ووفرة بياناتها.

ولا يمكن ضمان ما سبق بشكل كامل بالطبع، بيد أن وضع مجموعة من السياسات والمعايير يمكنه ضمان وتحقيق مستوى ملائم ومرضٍ من الأمان المعلوماتي. ومن المهم جداً تكوين الفهم الجيد لكيفية تطبيق الأسس التي يقوم عليها مجال أمن المعلومات على جميع جزئياته، ومنها تظهر أهمية الفهم الجيد للسياسات والمعايير، فالضعف في البنية الأمنية في بعض المؤسسات على سبيل المثال يكون على الأغلب نتيجة لغياب السياسات المكتوبة الواضحة والمفهومة.

وأي مؤسسة حكومية أو خاصة تتكون عادة من عدد من الإدارات والأقسام خلال أعمالها الروتينية فهي تتعامل مع معلومات ذات مستويات مختلفة من ناحية الحساسية، وقد تتعرض إلى مخاطر المعلومات في حال تعرض (سرية، توافر، تكامل) تلك المعلومات إلى اختراق أمني ما أثناء تداول المعلومات داخل المؤسسة.

كما تتعامل المؤسسات مع بيئتها الخارجية من مؤسسات حكومية أو خاصة . . وهي تستخدم في هذا التعامل وسائل وأنشطة مختلفة قد تؤثر عليها سلباً إذا ما تم انتهاك سرية، توافر، أو تكامل المعلومات المتبادلة مع الأطراف سابقة الذكر أو ما يطلق عليها اصطلاحاً الأطراف الخارجية.

لذا وجب وضع قواعد عملية و فنية مكتوبة لحماية مؤسسة ما من وقوع حوادث تمس أعمالها و بنيتها التحتية التقنية، وتقدم وثائق مكتوبة وصفاً عاماً للضوابط المطلوبة لإدارة مخاطر أمن المعلومات .. كما تُمثل إعلاناً رسمياً عن نية المؤسسة في حماية بياناتها و معلوماتها.

سياسة أمن المعلومات وثيقة حية يتم تحديثها باستمرار للتكيف مع تطور الأعمال ومتطلبات تكنولوجيا المعلومات . . وحيث تختلف مخاطر و متطلبات سياسات أمن المعلومات من جهة لأخرى حسب طبيعة أعمالها و بيئتها الداخلية والخارجية، عليه وجب تصنيف تلك السياسات لرؤية أكثر وضوحاً بناءً على الهيكل التنظيمي للمؤسسة والأنظمة واللوائح الإدارية التي يتعين الالتزام بها، وطبيعة أعمال المؤسسة وعلاقاتها الداخلية والخارجية، و متطلبات سرية وتوافر وتكامل المعلومات المتعامل بها داخل المؤسسة وخارجها، والوسائل المستخدمة في تجميع ومعالجة وتخزين وإتلاف المعلومات.

وقد أولت الهيئة الوطنية لأمن وسلامة المعلومات

اهتماماً مركزاً على وضع إطار عام و دليل استرشادي للسياسات الوطنية لأمن وسلامة المعلومات التي تساهم في تحقيق الهدف الرئيسي لإنشاءها وهو دعم الاستخدام الآمن للتكنولوجيا مع الحفاظ على أصول المعلومات وحمايتها من المخاطر المحدقة بها.

أما عن الفئة المستهدفة من هذا الدليل فتتمثل الجهات العامة في دولة ليبيا . . غير أنه يمكن استخدامه من قبل جهات القطاع الخاص أيضاً . . وقد تم إعداد هذا الدليل من أجل استخدامه من قبل إدارات أمن المعلومات أو مكاتب تقنية المعلومات لدى تلك الجهات بهدف تطوير سياسات و إجراءات أمن المعلومات لديها .

وقد تم إصدار النسخة الأولى من الدليل الإرشادي في سنة 2019 ويحوي مجموعة من السياسات التي توفر الحد الأدنى من المتطلبات الأساسية لأمن تكنولوجيا المعلومات بأفضل المعايير والممارسات المقبولة عالمياً . . يتضمن الإصدار الأول من الدليل السياسات التالية:

- **سياسات حماية البيانات**
  - سياسة تصنيف المعلومات
  - سياسة حماية البيانات
  - سياسة الاحتفاظ بالسجلات وإتلافها
  - سياسة نشر البيانات
  - سياسة الوصول للبيانات
- **سياسة الاستخدام المقبول**
  - سياسات المستخدم
  - سياسة كلمة السر/المرور
  - سياسة استعمال البريد الإلكتروني
  - سياسة استخدام الانترنت
  - سياسة أمان محطات العمل (الكمبيوتر وملحقاته)
- **سياسة الحماية من البرمجيات الخبيثة**
- **سياسات حماية الشبكات**
  - سياسات جهاز التوجيه ومبدل الشبكة
  - سياسة الاتصالات اللاسلكية
  - سياسة الشبكة الافتراضية الخاصة (VPN)
  - سياسة جدار الحماية/الناري
- **سياسة الأطراف الثالثة**
- **سياسة النسخ الإحتياطي**
- **سياسة الأمان المادي**

ولكون نهج الهيئة يرتكز على مواكبة التطور في مجال تكنولوجيا وأمن المعلومات، فقد عملت على مراجعة الاصدار الأول من الدليل وتجهيز سياسات جديدة إضافية لتكون من ضمن الاصدار الثاني، والسياسات الجديدة كالتالي:

- **سياسة حماية الحوسبة السحابية**
- **سياسة الوصول عن بعد**
- **سياسة التعامل مع الحوادث**
- **سياسة التوعية والتدريب**
- **سياسة خصوصية بيانات العملاء**
- **سياسة خطة التعافي من الكوارث**
- **سياسة الوسائط القابلة للإزالة**
- **سياسة التشفير**

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 النشر 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.

2.1. الغرض

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

3.1. النطاق

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

4.1. 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.

2.4.1. **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.

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

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

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. سياسة حماية البيانات

1.2. 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)**.

3.2. النطاق

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

4.2. السياسة

1.4.2. المسؤول عن البيانات:

1.1.4.2. يجب أن تخضع جميع أصول البيانات الهامة لمسؤول ويجب أن يكون المسؤول أحد الموظفين الذي تتناسب خبرته مع قيمة الأصول التي سيتولى إدارتها وحمايتها.

2.1.4.2. يجب عدم تكليف موظف مسؤول رسمي للبيانات التي ليس لها تصنيف أمني وتكون ذات قيمة عملية محدودة، كما يجب التخلص من البيانات إذا لم يكن هناك حاجة قانونية أو تشغيلية لإبقائها، وينبغي تعيين المسؤولين المؤقتين لهذه البيانات داخل كل إدارة لضمان إتمام عملية التخلص منها.

3.1.4.2. يكون منشئ المستندات الجديدة التي لها استخدام داخلي محدد على المدى القصير هو المسؤول عنها، وهذا يشمل الرسائل والخطط والجداول والتقارير، كما يجب إبلاغ جميع الموظفين بمسؤوليتهم عن الوثائق التي ينشئونها.

4.1.4.2. 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:

1.2.4.2. يجب تخزين جميع البيانات الإلكترونية على المنظومات الخاصة بها حتى يسمح بإجراء نسخ احتياطية منتظمة.

2.2.4.2. يجب عدم السماح للموظفين للوصول إلى البيانات إلا بعد إعلامهم وموافقتهم على شروط الاطلاع على البيانات التي سيتعاملون معها.

3.2.4.2. قواعد البيانات التي تحتوي على بيانات شخصية يجب أن يكون لها إجراءات محددة لإدارتها وتأمين السجلات والوثائق.

4.2.4.2. يجب تخزين الملفات التي يتم تصنيفها كمخاطر أمنية محتملة في أكثر المناطق أمناً على الشبكة.

3.4.2. الكشف عن البيانات:

1.3.4.2. في حالة مشاركة البيانات المقيدة مع جهة عمل أخرى، يجب الحرص في الكشف عن هذه البيانات وأن يتم بطريقة آمنة.

2.3.4.2. عندما يتم الإفصاح عن البيانات أو مشاركتها، يجب أن يتم ذلك فقط وفقاً لبروتوكول مشاركة البيانات الموثق أو اتفاقية تبادل البيانات.

3.3.4.2. يحظر الإفصاح عن البيانات المقيدة لأي جهة عمل خارجية بدون اتفاق مسبق.

2. Information Protection Policy

2.3. 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.

2.4. 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.

2.5. 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.

2.6. Policy

2.6.1. **Information assets Owner:**

2.6.1.1. 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.

2.6.1.2. 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.

2.6.1.3. 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.

2.6.1.4. 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.

2.6.2. **Information storage:**

2.6.2.1. All electronic information must be stored on centralized facilities to allow regular backups to take place.

2.6.2.2. Employees should not be allowed to access information until they understand and agree the legislated responsibilities for the information that they will be handling.

2.6.2.3. Databases holding personal information must have a defined security and system management procedure for the records and documentation.

2.6.2.4. Files which are identified as a potential security risk should only be stored on secure network areas.

2.6.3. **Disclosure of Information:**

2.6.3.1. 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.

2.6.3.2. Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

2.6.3.3. Disclosing restricted information to any external organization is also prohibited.

3. سياسة الاحتفاظ بالسجلات وإتلافها

1.3. مقدمة

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

2.3. 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 وإتلافها.

4.3. السياسة

1.4.3. **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.

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

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

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

5.4.3. **الوثائق الإلكترونية:**

- المستندات الإلكترونية: وتشمل مكتبة برامج مايكروسوفت (Microsoft Office Suite)، ملفات

(PDF). والاحتفاظ يعتمد أيضا على موضوع السجلات وتصنيف بياناتها.

- البريد الإلكتروني: يعتمد الاحتفاظ برسائل البريد الإلكتروني على محتواها فلا ينبغي الاحتفاظ بجميعها، والبريد الإلكتروني الذي يتم حفظه يجب أن يكون مطبوعاً في نسخة ورقية وأن يُحتفظ به في الملف المناسب أو يتم تنزيله إلى ملف كمبيوتر ويتم الاحتفاظ به إلكترونيا أو على القرص كملف منفصل.
- ملفات صفحة ويب: في جميع الأجهزة في محيط العمل، يجب أن يتم جدولة متصفحات الإنترنت لحذف ملفات جمع البيانات مرة واحدة في الشهر.

.6.4.3 **الملفات والمستندات القانونية:**

يتم الاحتفاظ بالأرشيف القانوني الخاص بـ **(جهة 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.

.7.4.3 **السجلات الشخصية:**

- ملفات الموظفين وما يتضمنه من المستندات الشخصية والوظيفية تحفظ بشكل دائم حتى بعد إنهاء علاقة عمل الموظف بـ **(جهة العمل)**.
- السجلات الإدارية الوظيفية (وتشمل سجلات الحضور والانصراف، استمارة الطلبات، سجل تغيرات العمل، أوراق إنهاء الخدمة، نتائج الاختبارات، سجلات التدريب) يتم الاحتفاظ بها وفق الحاجة إليها وللمدة اللازمة وفق تقديرات **(جهة العمل)**.
- سجلات وأوراق امتحانات شغل الوظائف: تحتفظ **(جهة العمل)** بأوراق إجابة الامتحانات والسجلات والقوائم وسائر الوثائق المتعلقة بالامتحانات التي تجريها لمدة سنتين تبدأ من تاريخ اعتماد نتيجة الامتحان.

.8.4.3 **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.

.9.4.3 **إجراءات إتلاف الوثائق:**

.1.9.4.3 يجب عدم إزالة أو إتلاف السجلات الا ان كانت مصنفة بذلك او عند انتهاء مدة الاحتفاظ بها.

.2.9.4.3 عند الاحتفاظ بالسجلات خلال الفترة المحددة لها في جداول الاحتفاظ، يتم إعدادها للإتلاف.

3.9.4.3. الوثائق المالية يجب إتلافها والتخلص منها وفق الإجراءات المحددة بلائحة الميزانية والحسابات والمخازن.

4.9.4.3. الوثائق المالية و سجلات المتعلقة بالموظفين يجب إتلافها بوسيلة تضمن إتلاف المستندات إتلافا كلياً.

5.9.4.3. يجب التخلص من البيانات الإلكترونية المحتفظ بها في الوسائط الأخرى عن طريق الإتلاف المادي لتلك الوسائط.

6.9.4.3. يجب أن تتم عملية إتلاف السجلات بشكل آمن وكامل.

7.9.4.3. يجب تسجيل عملية الإتلاف في وثيقة رسمية لإتلاف البيانات داخل **(جهة العمل)**.

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:**

3.4.9.1. Records must not be removed or destroyed before retention period expiration.

3.4.9.2. Once records have been retained for the applicable period of time, set forth in the record retention.

3.4.9.3. Destruction of finance records should be in accordance to budget and accounts procedures.

3.4.9.4. Destruction of financial and personnel-related documents and all paper documents should be accomplished by a method that prevents retrieval of this data.

3.4.9.5. Electronic data contained on all other media should be destroyed by the physical destruction of that media.

3.4.9.6. Records must be destroyed securely and completely.

3.4.9.7. Recorded Destruction in formal documented processes, for data destruction within the **(Organization)**.

4. سياسة نشر البيانات

1.4. 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 المشاريع الأولية.
  - البيانات والمعلومات التي ترى **(جهة العمل)** ضرورة نشرها لاستخدامها أو لأخذ العلم بها.

2.4. 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)**.

3.4. النطاق

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

4.4. السياسة

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

2.4.4. البيانات التي تحتاج إلى الحماية يمكن الوصول إليها عن طريق الوصول المصرح به، مثل الموظفين أو الشركاء وفق مبدأ «الحاجة إلى المعرفة» لأغراض ذات الصلة بالأعمال. وينبغي منح هذا التصريح لفترة محددة وتحددها الإدارة الأعلى مستوى.

3.4.4. تقتصر البيانات السرية على مجموعة من الأشخاص في وظيفة معينة تتطلب طبيعة عملهم ضرورة الوصول إلى البيانات السرية التي تحتفظ بها **(جهة العمل)**.

4.4.4. البيانات المقيدة يتم الوصول إليها بموجب إجراءات رسمية ولأفراد متخصصين ومحددين على أساس الوظيفة.

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. سياسة الوصول للبيانات

1.5. مقدمة

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

2.5. 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.

3.5. النطاق

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

4.5. السياسة

1.4.5. الأفراد المصرح لهم فقط يمكنهم الوصول إلى البيانات المتوفرة بشكل كامل.

2.4.5. المستخدمين يُصرّح لهم الوصول للبيانات واستخدامها عند الطلب.

3.4.5. 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.

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.

6. سياسة الاستخدام المقبول

1.6. 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 الإلكتروني ومتصفحات شبكة الإنترنت 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.

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.

2.6. الغرض

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.

3.6. 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)**.

4.6. السياسة

1.4.6. الاستخدام العام والملكية:

1.1.4.6. تمتلك **(جهة العمل)** البيانات المحفوظة على أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى المملوكة أو المستأجرة من قبل المؤسسة، أو من طرف ثالث، ويجب التأكد

من خلال الوسائل القانونية أو التقنية أن معلومات الملكية محمية وفقًا لسياسات حماية البيانات.

2.1.4.6. يجب أن يدرك المستخدم بأنه تقع على عاتقه مسؤولية الإبلاغ عن سرقة أو فقدان أو كشف غير مصرح به عن معلومات الملكية المتعلقة بـ **(جهة العمل)**.

3.1.4.6. يُسمح بالوصول إلى أو استخدام أو مشاركة معلومات الملكية لـ**(جهة العمل)** فقط في حدود ما هو مصرح به وضروري للإيفاء بمتطلبات الوظيفة التي يتم التكليف بها.

4.1.4.6. كل موظف مسؤول عن تطبيق معايير الاستخدام الآمن 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.

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

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

2.4.6. معلومات الملكية:

1.2.4.6. كل الأجهزة المحمولة وأجهزة الكمبيوتر المملوكة لـ **(جهة العمل)** والتي تتصل بشبكة الإنترنت يجب أن تلتزم بسياسة التحكم في الوصول.

2.2.4.6. 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 .

3.2.4.6. 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.

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

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

3.4.6. 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.

6.3.4.1. 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)**.

6.3.4.2. 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.

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

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

6.3.4.5. 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.

6.3.4.6. استخدام أجهزة الكمبيوتر المملوكة لـ **(جهة العمل)** للانخراط بفاعلية في شراء أو نقل مواد تنتهك القانون.

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

6.3.4.8. 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 مراقبة تدفق البيانات داخل الشبكة Network Sniffing، وعمليات حجب «الحرمان» من الخدمة (DDOS "Distributed Denial of Service")، والتلاعب في الحزمة البيانات (Packet spoofing) ومعلومات التوجيه المزورة لأغراض خبيثة.

9.3.4.6. عدم إجراء عملية فحص أمني للمنافذ ports إلا بعد إبلاغ مسبق للمسؤول بـ **(جهة العمل)**.

10.3.4.6. 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.

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

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

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

14.3.4.6. 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) .

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

16.3.4.6. التدوين أو النشر الإلكتروني 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.

17.3.4.6. سياسة تصنيف المعلومات بـ**(جهة العمل)** تنطبق أيضاً على التدوين، حيث يُحظر على الموظفين الكشف عن أي معلومات حساسة خاصة بـ**(جهة العمل)**، وكذا الأسرار التجارية والمهنية أو أي مواد تحت مظلة سياسة تصنيف المعلومات عن الانخراط في عمليات التدوين أو النشر الإلكتروني.

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

19.3.4.6. على الموظفين عدم نسب تصريحات شخصية أو آراء أو معتقدات لـ**(جهة العمل)** عند الانخراط في عمليات تدوين أو نشر إلكتروني، وإذا قام موظف ما بالتعبير عن رأي ما أو معتقد خاص به فلا يمكنه بأي حال من الأحوال أن يتحدث بصفة موظف في **(جهة**

العمـل) أو ممثـلاً لهـا صراحـةً أو ضمنيـاً، كمـا يجـب عـلى الموظـف أن يضـع في الاعتبـار المخاطـرة الـتي تتضمنهـا عمليـة التدويـن /النشـر الإلكتـروني.

20.3.4.6. لا يجـوز اسـتخدام العلامـات التجاريـة والشـعارات وأيـة ملكيـة فكريـة أخـرى خاصـة بـ**(جهـة العمـل)** فيمـا يتعلـق بـأي نشـاط تدويـن أو نشـر إلكتـروني .

6. Acceptable Use Policy

6.1. 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.

6.2. 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.

6.3. 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.

6.4. Policy

6.4.1. General Use and Ownership

6.4.1.1. **(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 Privacy Policies.

6.4.1.2. Users have to be aware that they are responsible to report the theft, loss or unauthorized disclosure of **(Organization)** proprietary information.

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

6.4.1.4. 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.

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

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

6.4.2. Security and Proprietary Information

6.4.2.1. All mobile and computing devices that connect to the internal network must comply with the Access Control Policy.

6.4.2.2. 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.

6.4.2.3. 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.

6.4.2.4. Postings by employees from **(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.

6.4.2.5. 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.

6.4.3. 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.

6.4.3.1. 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)**.

6.4.3.2. 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.

6.4.3.3. Accessing data, a server or an account for any purpose other than conducting **(Organization)** business, even with an authorized access, is prohibited.

6.4.3.4. 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.

6.4.3.5. 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.

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

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

6.4.3.8. 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.

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

6.4.3.10. 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.

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

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

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

6.4.3.14. 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.

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

6.4.3.16. 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.

6.4.3.17. **(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.

6.4.3.18. 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.

6.4.3.19. 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.

6.4.3.20. **(Organization)**'s trademarks, logos and any other **(Organization)** intellectual property must not be used in connection with any blogging activity.

7. سياسة كلمة السر/المرور

1.7. 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 للولوج إلى الأجهزة ولمصادقة 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.

2.7. الغرض من السياسة

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

3.7. 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.

4.7. السياسة

1.4.7. **فرض كلمة مرور قوية:** يجب ان تكون كلمة المرور قوية ولا تتضمن في تركيبها الكلمات التي يسهل على الآخرين إيجادها.

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

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

3.1.4.7. يجب أن لا يقل عدد رموز كلمة السر/المرور عن 12 رمزاً.

4.1.4.7. لا يجب استعمال اسم المستخدم في كلمة السر.

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

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

7.1.4.7. يفضل أن تكون كلمة المرور «جملة مرور» لا يفهمها إلا المستخدم، مُكونة من تركيبة الأحرف والأرقام والرموز.

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

2.4.7. **تخزين كلمة المرور:** يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها.

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

2.2.4.7. 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.

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

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

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

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

1.3.4.7. 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.

2.3.4.7. يجب أخذ الحذر من الأشخاص المتطفلين عند طباعة لكلمة السر/المرور أثناء عملية الولوج.

3.3.4.7. يمنع إرسال كلمة المرور عبر البريد الإلكتروني أو من خلال أي وسيلة عبر الإنترنت.

4.3.4.7. يجب تغيير كلمات المرور إذا ظهر أي مؤشر على احتمال اختراق للنظام أو لكلمة المرور.

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

6.3.4.7. لا يجب استخدام نفس كلمة المرور لحسابات المسؤولين المتعددة.

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

8.3.4.7. يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والأجهزة داخل **(جهة العمل)** والحسابات والأجهزة الأخرى خارجها.

4.4.7. **كلمات المرور الأولية (المؤقتة):** يجب تغيير كلمات المرور الأولية للمستخدمين وفرض مدة

انتهاء لصلاحيتها لإجبار المستخدم على تغييرها.

7.4.4.1. 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.

7.4.4.2. 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) .

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

7.4.4.4. يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقتة.

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

7.4.4.6. 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.

7.4.4.7. يجب على المستخدم في حالة أن اشتبه أو لاحظ وجود مشكلة أمنية أو أن كلمة المرور الخاصة به قد تعرضت للاختراق الإبلاغ عن الحادث وتغيير جميع كلمات المرور.

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

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

7. Password Policy

7.1. 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.

7.2. Purpose

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

7.3. 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.

7.4. Policy

7.4.1. **Enforce strong passwords:**

- 7.4.1.1. Passwords should be at least 12 positions in length.
- 7.4.1.2. 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.
- 7.4.1.3. Users shouldn't use popular, easily predictable passwords, such as names, birthdays, or phone numbers.
- 7.4.1.4. Users shouldn't use their username in the password.
- 7.4.1.5. Password shouldn't be repeated numbers or characters such as (3333 or AAAA).
- 7.4.1.6. In case of using a common word, users should mix the characters, so it doesn't give a clear meaning.
- 7.4.1.7. Implement strict controls for system-level and shared service account passwords.

7.4.2. **Passwords must be stored in a secure manner to ensure not to be detected:**

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

7.4.2.2. 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.

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

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

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

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

7.4.3.1. 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.

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

7.4.3.3. Users shouldn't send passwords via email or any other media via the Internet.

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

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

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

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

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

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

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

7.4.4.2. 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.

7.4.4.3. Users should acknowledge receipt of initial passwords.

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

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

7.4.6. 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.

7.4.7. 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.

7.4.8. 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.

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

8. سياسة استعمال البريد الإلكتروني

1.8. 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.

2.8. الغرض من السياسة

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

3.8. النطاق

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

4.8. السياسة

1.4.8. حساب البريد الإلكتروني:

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

2.1.4.8. 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.

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

4.1.4.8. 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.

2.4.8. استخدام البريد الإلكتروني:

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

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

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

8.2.4.4. 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.

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

8.2.4.6. 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.

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

8.2.4.8. يجب أن تحدد **(جهة العمل)** إجراءً مفصلاً وبوضوح للتعامل مع حساب البريد الإلكتروني في الحالات التالية (الاستقالة، الفصل/الطرد، الإيقاف).

8.2.4.9. يجب على من يتعرف على أو يلاحظ وجود مشكلة أمنية فعلية أو مشتبه بها، الاتصال على الفور بإدارة/ قسم أمن المعلومات في **(جهة العمل)** والإبلاغ بشكل فوري.

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

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

8.4.3. الاستخدام الغير مقبول للبريد الإلكتروني:

8.3.4.1. تعد الممارسات التالية غير مقبولة عند استخدام البريد الإلكتروني الخاص بـ**(جهة العمل)**

8.3.4.2. 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.

8.3.4.3. 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.

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

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

6.3.4.8. إرسال رسائل بريد إلكتروني غير مرغوب فيها بما في ذلك إرسال «بريد غير هام» JUKE MAIL ، أو مواد إعلانية إلى أفراد لم يطلبوها تحديداً كـ (رسائل البريد الإلكتروني المزعج SPAM).

7.3.4.8. استخدام غير مصرح به لمعلومات البريد الإلكتروني أو تزويرها .

8.3.4.8. إنشاء أو إجراء تحويل لـ (سلسلة رسائل chain letters)، (بونزي Ponzi)، أو أي أشكال هرمية من أي نوع .

8. Email Usage Policy

8.1. 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.

8.2. 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.

8.3. Scope

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

8.4. Policy

8.4.1. **Email Account:**

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

8.4.1.2. 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.

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

8.4.1.4. 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.

8.4.2. **Use of email:**

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

8.4.2.2. **(Organization)** email accounts should be used only for **(Organization)** business-related purposes to help employees in their job duties, and not to be used for personal purposes.

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

8.4.2.4. 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.

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

8.4.2.6. 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.

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

8.4.2.8. **(Organization)** must set out a clearly detailed procedure to handle Email account in the following cases (resignation, dismissal, suspension).

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

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

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

8.4.3. **Unacceptable Use of E-Mail:**

8.4.3.1. The **(Organization)** email system should 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)**'s employee should report the matter to their supervisor immediately.

8.4.3.2. 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.

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

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

8.4.3.5. 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).

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

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

9. سياسة استخدام الإنترنت

1.9. 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/أو 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.

2.9. الغرض

تهدف هذه السياسة إلى 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.

3.9. النطاق

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

4.9. السياسة

1.4.9. استخدام الموارد:

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

2.1.4.9. يجب أن تقوم إدارات **(جهة العمل)** بمراجعة متطلبات وصول المستخدمين إلى الإنترنت بشكل دوري لضمان استمرار احتياجهم لهذه المتطلبات.

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

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

2.4.9. **الاستخدام المسموح:** يجب أن يكون المستخدمين على دراية بما يُسمح به لاستخدام موارد الإنترنت في **(جهة العمل)**

1.2.4.9. التواصل بين الموظفين وغير الموظفين لأغراض العمل.

2.2.4.9. تنزيل التحديثات البرامج والتصحيحات الموافق عليها من إدارة / قسم تكنولوجيا المعلومات.

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

4.2.4.9. التزود بالمراجع للمعلومات التنظيمية أو الفنية المتعلقة بالعمل.

5.2.4.9. إجراء الأبحاث.

3.4.9. **الاستخدام الشخصي:**

1.3.4.9. لا يجب استخدام أجهزة كمبيوتر **(جهة العمل)** للوصول إلى الإنترنت لأغراض شخصية دون موافقة مدير المستخدم وقسم تكنولوجيا المعلومات.

2.3.4.9. يجب أن يكون جميع المستخدمين 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.

3.3.4.9. يجب أن يدرك المستخدمون الذين يختارون تخزين أو نقل المعلومات الشخصية مثل المفاتيح الخاصة أو أرقام بطاقات الائتمان أو الشهادات أو الاستفادة من «محافظ» الإنترنت بأنهم 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.

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

5.3.4.9. يجب على المستخدمين التواصل بقسم / إدارة أمن المعلومات [أو القسم المكافئ له] في **(جهة العمل)** والإبلاغ بشكل فوري في حالة التعرف أو ملاحظة وجود مشكلة أمنية فعلية أو مشتبه بها.

4.4.9. **الاستخدام المحظور:** يجب أن يدرك المستخدمين أن استخدام الإنترنت في الأفعال التالية محظور:

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

2.4.4.9. لا يجوز انتحال شخصية الآخرين أو جهاز آخر.

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

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

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

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

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

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

9.4.4.9. لا يجوز استخدام الإنترنت بشكل يؤثر سلباً على المستخدمين الآخرين، أو على أداء الأجهزة والشبكات.

9.4.4.10. يمنع استخدام الإنترنت 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.

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

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

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

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

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

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

9. Internet Usage Policy

9.1. 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.

9.2. 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

9.3. Scope

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

9.4. Policy

9.4.1. **Resource Usage:**

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

9.4.1.2. User's Internet access requirements should be reviewed periodically by **(Organization)** departments to ensure that continuing needs exist.

9.4.1.3. 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.

9.4.1.4. **(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.

9.4.2. **Allowed Usage:** Users should be aware of the allowed usage of **(Organization)**'s Internet resources.

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

9.4.2.2. Downloading software upgrades and patches supported from IT technical.

9.4.2.3. Review of possible vendor web sites for product information.

9.4.2.4. Reference regulatory or technical information.

9.4.2.5. Research

9.4.3. **Personal Usage:**

9.4.3.1. Users must not use **(Organization)** computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department.

9.4.3.2. All users 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.

9.4.3.3. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" must be aware that they 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.

9.4.3.4. Users must be aware that they are fully responsible for their computer devices and the use of them, and they have to be aware of the security and preserve of IT resources.

9.4.3.5. Users must contact the Information Security Department and report immediately if recognizing or noticing an actual or suspected security issue.

9.4.4. **Prohibited Usage:** Users must be aware that the following activities are prohibited.

9.4.4.1. 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.

9.4.4.2. Impersonation of others or devices is forbidden.

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

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

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

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

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

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

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

9.4.4.10. 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.

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

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

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

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

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

9.4.4.16. 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.

10. سياسة أمان محطات العمل (الكمبيوتر وملحقاته)

1.10. 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.

2.10. الغرض من السياسة

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

3.10. النطاق

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

4.10. السياسة

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

2.4.10. يجب أن يدرك المستخدم بأنه تقع عليه المسؤولية الكاملة للاستخدام الملائم لجميع الموارد المخصصة له بما فيها من أجهزة الكمبيوتر وملحقاتها أو برمجيات الأجهزة.

3.4.10. لا يسمح للمستخدمين بالوصول إلى الشبكة باستخدام الحواسيب الشخصية واللوحية والهواتف الذكية الا بتصريح من قسم / إدارة تكنولوجيا المعلومات.

4.4.10. لا يجب محاولة الوصول إلى أجزاء ممنوعة الوصول من الشبكة، مثل نظام التشغيل الرئيسي، برامج الأمان وغيرها دون الموافقة من الإدارة المختصة.

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

6.4.10. يجب أن يدرك المستخدم بأنه 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).

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

8.4.10. يجب الحصول على موافقة خاصة من قسم / إدارة تكنولوجيا المعلومات قبل تنصيب أي برامج أو تركيب أجهزة خاصة على أنظمة **(جهة العمل)**.

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

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

11.4.10. لا يقوم موظفو قسم / إدارة تقنية المعلومات بالدخول (login) للأجهزة الشخصية لأعمال الصيانة إلا بعد أخذ الإذن من صاحب العلاقة مباشرة.

12.4.10. يجب أن يدرك المستخدم بأن أجهزة الكمبيوتر وملحقاتها موجودة لخدمة الموظفين والمستخدمين لأداء الأعمال بطريقة أفضل، وعليه فإنه ليس من الممكن استغلالها لأغراض شخصية تحت أي ظرف من الظروف.

13.4.10. يحظر على موظفي **(جهة العمل)** استخدام 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.

14.4.10. يمنع إضافة معدات الشبكة غير المصرح بها لشبكة **(جهة العمل)**، حيث يؤثر إضافة هذه المعدات على استقرار الشبكة، وقد يؤدي إلى حدوث مشكلات يصعب تشخيصها.

15.4.10. يجب على المستخدم عند الدخول على جهاز الكمبيوتر استخدام اسم المستخدم وكلمة المرور الخاص به، وعند ترك الجهاز ولو لفترة وجيزة يجب قفل شاشة الجهاز بكلمة المرور.

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

17.4.10. لا يسمح لأي شخص من خارج **(جهة العمل)** باستخدام أجهزة كمبيوتر **(جهة العمل)** إلا بإذن كتابي رسمي.

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

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

10. Workstation Security Policy

10.1. 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)**.

10.2. 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)**.

10.3. Scope

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

10.4. Policy

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

10.4.2. Users must be aware that they should be fully responsible for the proper use of all resources allocated to them, including computer devices, peripherals and software.

10.4.3. Users are not allowed to access network using personal computers, tablets and smartphones, unless authorized by IT department.

10.4.4. Users must 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.

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

10.4.6. Users must be aware that 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.).

10.4.7. 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.

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

10.4.9. 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 must be aware that they are responsible for any data they leave on the laptop when it is returned to the **(Organization)**.

10.4.10. 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.

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

10.4.12. Users must be aware that computers and peripherals are available to serve employees and users to perform better work, therefore cannot be used for personal purposes under any circumstances.

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

10.4.14. It's prohibited to add unauthorized network gear to **(Organization)**'s network, that may affects network stability and can potentially result in hard-to-diagnose problems.

10.4.15. Users must logging computer using their username and password, and when leaving the device even for a short period of time, they must lock screen with password.

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

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

10.4.18. Users should not disable Anti-virus 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.

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

11. سياسة الحماية من البرمجيات الخبيثة

1.11. 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)**.

2.11. الغرض

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

3.11. النطاق

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 إنترنت.
- الأشخاص الآخرين العاملين للمؤسسة والأفراد والجهات المنخرطين في أي عمل ما معها والمستعملين لمعدات وشبكات **(جهة العمل)**.
- أياً أحد أعطى له الحق في الدخول على شبكة **(جهة العمل)**.

4.11. السياسة

1.4.11. **مسؤوليات المستخدم:**

1.1.4.11. 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.

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

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

4.1.4.11. يمنع تحميل الملفات من مصادر غير معروفة أو مشبوهة.

5.1.4.11. يجب تجنب المشاركة المباشرة على قرص التخزين بصلاحيات القراءة والكتابة ما لم يكن

هناك حاجة ضرورية لذلك وتلبية لمتطلبات العمل التي لا يمكن تحقيقها بطريقة أخرى.

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

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

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

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

10.1.4.11. 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.

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

12.1.4.11. إبلاغ فريق تقنية المعلومات بـ**(جهة العمل)** على الفور.

13.1.4.11. إطفاء الجهاز.

14.1.4.11. ضمان ألا يستعمل الجهاز موظفين آخرين.

15.1.4.11. أن يكون مستعداً لاطلاع فريق تقنية المعلومات على أي إجراء قام به قد يكون سبب العدوى.

2.4.11. مسؤوليات فريق تقنية المعلومات بـ(جهة العمل):

1.2.4.11. 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)**

2.2.4.11. 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.

3.2.4.11. 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.

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

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

6.2.4.11. 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 الأخصائيين للتحقيق في الأمر.

7.2.4.11. 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.

8.2.4.11. 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.

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

10.2.4.11. 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.

11. Malware Protection Policy

11.1. 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)**.

11.2. 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.

11.3. 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.

11.4. Policy

11.4.1. User's Obligations

11.4.1.1. 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.

11.4.1.2. 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.

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

11.4.1.4. Never download files from unknown or suspicious sources.

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

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

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

11.4.1.8. 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).

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

11.4.1.10. 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.

11.4.1.11. 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.

11.4.2. Organization's IT Department Obligations

11.4.2.1. 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.

11.4.2.2. 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.

11.4.2.3. 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 **(Organization)** network then updates will be installed from the secondary server.

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

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

11.4.2.6. 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.

11.4.2.7. 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)** Cybersecurity Senior Staff.

11.4.2.8. 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.

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

11.4.2.10. 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.

12. سياسة التوعية والتدريب

1.12. مقدمة

التوعية بأمن المعلومات تساعد بشكل كبير في حماية البيانات الشخصية والملكية الفكرية والمالية والمعلومات الحساسة والسرية والأنظمة الشبكية والتطبيقات التي تستخدمها **(جهة العمل)**، وذلك عبر تقديم مفاهيم عامة حول المخاطر والتهديدات و أفضل الممارسات في مجال أمن المعلومات. على الرغم من اعتبار الإنسان في معظم الأوقات الحلقة الأضعف في الدفاعات الإلكترونية لـ **(جهة العمل)**، إلا أنه قد يكون في الواقع أقوى درع يمكن لها الاستفادة منه ضد الهجمات الإلكترونية من خلال التوعية والتدريب المناسبين، حيث يمكن لـ **(جهة العمل)** تحويل القوى العاملة إلى أفضل خط دفاع ضد مجرمي الفضاء السيبراني.

وفي حين أن «التوعية» تشير إلى فهم أساسيات مجموعة من الموضوعات المتعلقة بأمن المعلومات، يولي»التدريب» اهتمامًا مفصلاً ومحدداً بتلك الموضوعات، حيث يُمكِّن التدريب على أمن المعلومات الأفراد من اتخاذ قرارات أفضل، ليس فقط في كيفية التعرف على الهجمات الإلكترونية المحتملة والاستجابة لها، ولكن أيضًا للتأكد من أنهم لا يعرضون البيانات عن غير قصد للخطر في عملهم اليومي. توفر التوعية المستوى الأساسي للمعرفة والفهم المناسب للتدريب للبناء عليه، لذا فإن الوعي والتدريب بأمن وسلامة المعلومات نهجان مكملان لبعضهما.

تحدد هذه السياسة الشكل العام لبرنامج للتوعية والتدريب بأمن المعلومات الهادف لتثقيف وتحفيز جميع العاملين بـ **(جهة العمل)** فيما يتعلق بمخاطر المعلومات والأمن والخصوصية والالتزامات ذات الصلة.

2.12. الغرض

الغرض من هذه السياسة هو رفع مستوى الوعي بأمن و سلامة المعلومات و تحديد مسؤوليات العاملين فيما يتعلق بمتطلبات أمن المعلومات و التزاماتهم تجاهها.

3.12. النطاق

تنطبق هذه السياسة على جميع الموظفين والموظفين المؤقتين بالإضافة لجميع الأشخاص المرتبطين بـ **(جهة العمل)**، والذين لديهم إمكانية الوصول إلى معلوماتها وأجهزة الكمبيوتر والأنظمة التي يتم تشغيلها أو صيانتها نيابة عنها.

4.12. السياسة

1.4.12. **التوعية بأمن المعلومات:**

1.1.4.12. يجب إبلاغ جميع الموظفين بالمواضيع الشائعة لأمن المعلومات وذات الصلة بالعمل، وتحفيزهم على الالتزام بأداء واجباتهم المتعلقة بأمن المعلومات حيالها .

2.1.4.12. يجب على إدارة/ قسم أمن المعلومات [أو قسم مكافأ له] تنظيم أربع ورش عمل (على

الأقل) في السنة، ويُلزم كل موظف بالحضور ويتم إبلاغ رئيسه بذلك.

12.1.4.3. يجب على جميع الموظفين الذين يتمتعون بإمكانية الوصول إلى موارد المعلومات لـ **(جهة العمل)** إكمال البرنامج التدريبي الخاص بأمن المعلومات خلال 30 يوم من تاريخ التوظيف. و يجب إكمال التدريب المستمر لأمن المعلومات بشكل سنوي .

12.1.4.4. يجب على إدارة/ قسم أمن المعلومات استخدام الكتيبات والملصقات وشاشات التوقف وغيرها من الوسائل، للمساعدة في زيادة الوعي بأمن المعلومات في **(جهة العمل)**.

12.1.4.5. يجب تقديم كتيب خاص بالتوعية الأمنية لكل موظف والصفحة الأخيرة على أن تكون موقعة من قبله.

12.1.4.6. يجب الأخذ في الاعتبار المعرفة بالسياسات الأمنية أثناء تقييم الموظف.

12.1.4.7. يجب دمج السياسات والإجراءات في ممارسات **(جهة العمل)** للحفاظ على مستوى عالٍ من التوعية الأمنية الذي يتطلب تدريبًا منتظمًا لجميع الموظفين والمتعاقدين مع **(جهة العمل)**.

12.1.4.8. يجب إجراء برامج التوعية الأمنية بصفة مستمرة لضمان أن لا تكون التوعية والتدريب كنشاط سنوي فحسب، بل يتم استخدامها للحفاظ على مستوى عالٍ من الوعي الأمني على أساس يومي.

12.1.4.9. يجب على إدارة/ قسم أمن المعلومات تشكيل فريق التوعية الأمنية، بحيث يكون هذا الفريق مسؤول عن تقديم وتطوير برنامج التوعية الأمنية. يوصى بتكوين الفريق من موظفين من إدارات وأقسام مختلفة من **(جهة العمل)** وبمسؤوليات مختلفة تمثل قطاعًا عرضيًا لـ **(جهة العمل)**.

12.1.4.10. يجب على إدارة/ قسم أمن المعلومات تحديد الأدوار في برنامج التوعية الأمنية، بحيث يوفر هذا البرنامج القائم على الوظيفة لـ **(جهة العمل)** مرجعًا لتدريب الموظفين على المستويات المناسبة بناءً على وظائفهم. يمكن توسيع نطاق التدريب – أو تجميع أو إزالة الموضوعات - وفقًا لمستويات المسؤولية والأدوار المحددة في **(جهة العمل)**.

12.1.4.11. يجب على فريق التوعية تحديد المقاييس لتقييم التوعية والتدريب: حيث تعد أداة فعالة لقياس نجاح برنامج التوعية الأمنية، ويمكنها أيضًا توفير معلومات قيمة للحفاظ عليه محدثًا وفعالًا. وستختلف المقاييس المحددة المستخدمة لقياس نجاح برنامج التوعية الأمنية لكل مؤسسة بناءً على اعتبارات مثل الحجم والمجال ونوع التدريب.

12.1.4.12. يجب أن يكون لدى فريق التوعية قائمة مرجعية لبرنامج التوعية الأمنية لتساعد **(جهة العمل)** على تخطيط وإدارة برنامجها التدريبي،يمكن استخدام قائمة التحقق الخاصة بالهيئة للمساعدة في التدريب على الوعي الأمني.

12.4.2. التدريب حول أمن المعلومات:

12.4.2.1. يجب أن تحدد إدارة/ قسم أمن المعلومات عناصر برنامج تدريبي للتوعية بأمن المعلومات. ويضمن الآليات المناسبة لتنفيذه.

12.4.2.2. يجب أن يُطلب تدريب إضافي على برامج التوعية بناءً على مهام الموظفين الذين تتطلب مسؤولياتهم صلاحية و إمكانيات الوصول للمعلومات السرية على النحو المحدد في سياسة تصنيف البيانات الخاص بـ **(جهة العمل)**، ويجب إكمال التدريب بشكل سنوي أو دوري.

12.4.2.3. يجب أن يتضمن برنامج التدريب تدريبًا عاماً إلزاميًا سنويًا، واستطلاعات مجدولة دورياً، وتقييمات التوعية الدورية غير مجدولة لضمان الامتثال للتدريب، واستطلاعات الرأي لتحسين برنامج التدريب والتثقيف التوعوي.

12.4.2.4. يجب حفظ شهادات إتمام التدريب ونتائجها في ملف الموظف بالموارد البشرية .

12. Security Awareness & Training Policy

12.1. Overview

Formal information security awareness will aid in the protection of data, personal, intellectual property, financial, or restricted and sensitive information, networked systems, and applications entrusted to and utilized by the **(Organization)**, by providing a broad understanding of information security threats, risks and best practices.

Humans, while most of the times considered the weakest link in an organization's cyber defenses, are could be in reality, the most powerful shield an **(Organization)** can leverage against cyber-attacks. With the right training and support, they can turn the workforce into the best line of defense against cyber criminals.

Whereas "awareness" implies a basic level of understanding about a board range of information security matters, "training" implies more narrowly-focused and detailed attention to one or more specific topics. Information security training empowers individuals to make better decisions, not only in how to recognize and respond to potential cyber-attacks, but also to be sure they aren't inadvertently putting data at risk in their day-to-day work. Awareness provides the foundation level of knowledge and understanding for training to build upon security awareness and training are complementary approaches.

This policy specifies an information security awareness and training program to inform and motivate all workers regarding their information risk, security, privacy and related obligations.

12.2. Purpose

The purpose of this policy is to raise the awareness of information security, and to inform and highlight the responsibilities employees have regarding their information security obligations.

12.3. Scope

This policy applies to all **(Organization)**'s employees, temporaries, and all **(Organization)**-Related Persons with access to its Information or computers and systems operated or maintained on behalf of the **(Organization)**.

12.4. Policy

12.4.1. **Information Security Awareness:**

12.4.1.1. All employees must be informed about relevant, current information security matters, and motivated to fulfill their information obligations.

12.4.1.2. Information Security Department [or equivalent department] must organize at least four workshops per year and it is mandatory to attend of every employee and his/her respective manager will be informed.

12.4.1.3. All employees with access to **(Organization)** information resources must complete security awareness training within the first 30 days from date of hire. Information Security training must be completed annually.

12.4.1.4. Information Security Department must take help of brochures, Posters, Screen Savers to increase the Information Security awareness at the **(Organization)**.

12.4.1.5. A Security Awareness Booklet and Brochure should be given to every employee. The last page needs to be signed by the employee.

12.4.1.6. Knowledge of security policies is one of the areas that must be assessed during appraisal of the employee.

12.4.1.7. The policies and procedures must be incorporated into **(Organization)** practice to maintain a high level of security awareness which demands regular training of all employees and contractors.

12.4.1.8. Security awareness must be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis.

12.4.1.9. Information Security Department must assemble the Security Awareness Team: this team is responsible for the delivery development, of the security awareness program. It is recommended the team be staffed with personnel from different areas of the **(Organization)**, with differing responsibilities representing a cross-section of the **(Organization)**.

12.4.1.10. Determine Roles for Security Awareness: Role-based security awareness must provide the **(Organization)** a reference for training personnel at the appropriate levels based on their job functions. The training can be expanded upon—and subject areas combined or removed—according to the levels of responsibility and roles defined in the **(Organization)**.

12.4.1.11. The awareness team must define metrics to assess Awareness and Training: metrics can be an effective tool to measure the success of a security awareness program, and can also provide valuable information to keep the security awareness program up-to-date and effective. The particular metrics used to measure the success of a security awareness program will vary for each organization based on considerations such as size, industry, and type of training.

12.4.1.12. The awareness team must have a Security Awareness Program checklist to help **(Organization)** plan and manage their security awareness training program. NISSA Checklist may be used to assist with security awareness training.

12.4.2. Information Security Training

12.4.2.1. Information Security Department must define and ensure the implementation of an information security awareness training program.

12.4.2.2. Additional role-based security awareness training must be required for employees whose responsibilities require Elevated Access, including access to Regulated or Confidential Information, as defined in the **(Organization)**'s Information Classification Policy. Role-based training must be completed on an annual or periodic basis.

12.4.2.3. Training program must include Annual mandatory training, Scheduled awareness surveys, Periodic unscheduled awareness assessments to assure compliance with the training. And Feedback surveys to improve our awareness training and education program.

12.4.2.4. Training completion certificates and results must be maintained in the individuals Human Resources personnel file, as part of the permanent record.

13. سياسة الوسائط القابلة للإزالة

1.13. مقدمة

الوسائط القابلة للإزالة هي مجموعة من أجهزة التخزين المختلفة وغير المثبتة داخل أجهزة الكمبيوتر، والتي تستخدم لنقل البيانات أو للنسخ الاحتياطي ويمكن إزالتها من جهاز الكمبيوتر أثناء تشغيل النظام. تشمل الوسائط القابلة للإزالة الأقراص المضغوطة CDs وأقراص DVD وأجهزة الذاكرة الصلبة بما في ذلك بطاقات الذاكرة وذاكرة فلاش (USB) والأقراص المرنة.

تعد الوسائط القابلة للإزالة مصدرًا معروفًا لانتشار البرامج الضارة بين الأجهزة، حيث يمكن باستخدامها نقل البرامج الضارة من بيئة إلى أخرى، كما قد تم ربطها مباشرةً بفقدان البيانات السرية والحساسة في العديد من المؤسسات. وحيث انه من السهل جدًا فقدها، فقد يؤدي ذلك إلى كشف كم كبير من البيانات المخزنة بها، مما يُحدث بدوره ضرراً كبيراً في السمعة، حتى مع عدم وجود دليل على ما تم فقده بالضبط.

وضعت هذه السياسة للتحكم في استخدام أجهزة الوسائط القابلة للإزالة من قبل جميع المستخدمين الذين لديهم إمكانية الوصول إلى المعلومات وأنظمة البيانات ومعدات تكنولوجيا المعلومات لأغراض إدارة الأعمال الرسمية.

2.13. الغرض

الغرض من هذه السياسة هو تحديد المسؤوليات والضوابط التنظيمية حول استخدام الوسائط القابلة للإزالة للحفاظ على سلامة البيانات، وذلك بالعمل على التقليل إلى الحد الأدنى من خطر فقدان البيانات السرية والحساسة التي تحتفظ بها **(جهة العمل)**، وتقليل خطر الإصابة بالبرمجيات الضارة لأجهزة الكمبيوتر بها، ولمنع الكشف غير المصرح به أو تعديل أو إزالة أو إتلاف أصول المعلومات بـ **(جهة العمل)** والذي قد يؤدي إلى تأخير أو توقف الأعمال.

3.13. النطاق

تنطبق هذه السياسة على جميع الموظفين والشركاء في **(جهة العمل)**، وعلى الأطراف الثالثة المتعاقدة معها والتي يمكنها الوصول إلى بياناتها، وتغطي جميع الأجهزة التي تملكها أو تُشغِلها **(جهة العمل)** وأي وسائط قابلة للإزالة وتستخدم مع هذه الأجهزة.

4.13. السياسة

1.4.13. شراء واستخدام الوسائط القابلة للإزالة:

1.1.4.13. يجب شراء الوسائط قابلة للإزالة والتي تستخدم لنقل أو تخزين بيانات **(جهة العمل)** عبر الطرق المعتمدة.

2.1.4.13. يجب شراء وتثبيت جميع أجهزة الوسائط القابلة للإزالة وأي معدات وبرامج مرتبطة بها بواسطة إدارة/ قسم تكنولوجيا المعلومات [أو قسم مكافأ له].

3.1.4.13. لا يجب استخدام الوسائط القابلة للإزالة في **(جهة العمل)** إلا في الحالات التي لا يوجد فيها بديل مناسب (مثل: مشاركة الشبكة / التخزين السحابي).

4.1.4.13. لا يجب توصيل الوسائط القابلة للإزالة المملوكة لـ **(جهة العمل)** في أجهزة الكمبيوتر التي لا تملكها أو تستأجرها دون موافقة وتصريح من قبل إدارة/ قسم تكنولوجيا المعلومات [أو قسم مكافأ له].

5.1.4.13. يجب على الموظفين استخدام الوسائط القابلة للإزالة المملوكة لـ **(جهة العمل)** فقط في أجهزتهم التابعة لـ **(جهة العمل)**. يجب عدم استخدام أجهزة الوسائط القابلة للإزالة التي لا تمتلكها **(جهة العمل)** لتخزين أي بيانات يتم استخدامها لإجراء الأعمال الرسمية لها، ويجب ألا تُستخدم مع أي من أجهزة تكنولوجيا المعلومات المملوكة أو المستأجرة لـ **(جهة العمل)**.

6.1.4.13. لا يجب استخدام أجهزة الوسائط القابلة للإزالة لأرشفة أو تخزين البيانات والسجلات كبديل لأجهزة التخزين الأخرى.

7.1.4.13. لا يجب حفظ بيانات **(جهة العمل)** المستخدمة أثناء عملية النسخ أو النقل في الوسائط القابلة للإزالة فقط. يجب أن تظل نُسخ أي بيانات مخزنة على الوسائط القابلة للإزالة موجودة على نظام المصدر على الكمبيوتر المتصل بالشبكة حتى يتم نقل البيانات بنجاح إلى كمبيوتر أو نظام آخر .

2.4.13. حماية البيانات:

1.2.4.13. يجب توفير مستوى الأمان المناسب للبيانات المخزنة على الوسائط القابلة للإزالة أثناء عمليات النقل أو التخزين وذلك حسب تصنيف البيانات وحساسيتها. يجب تشفير البيانات أو وضع كلمة السر على ملفات البيانات إلا في حالة لم يكن هناك خطر على **(جهة العمل)** من فقد البيانات أثناء نقلها أو تخزينها.

2.2.4.13. يجب تشفير جميع بيانات **(جهة العمل)** المخزنة على أجهزة الوسائط القابلة للإزالة حيثما أمكن ذلك. وفي حالة عدم إمكانية تشفيرها جميعاً، فيجب تشفير البيانات السرية و الحساسة.

3.2.4.13. تخزين المعلومات السرية والحساسة على الوسائط القابلة للإزالة يجب أن يكون فقط عند الضرورة لاستخدامها في أداء أعمال معينة، ويجب تشفيرها عند تخزينها وفقًا لسياسة التشفير المقبول لـ **(جهة العمل)**. كما يجب توفير إرشادات حول التشفير بما في ذلك الأجهزة والبرامج الموصى بها للموظفين.

4.2.4.13. يجب استخدام برنامج فحص الفيروسات والبرمجيات الضارة عند توصيل الوسائط القابلة للإزالة بأي جهاز آخر.

5.2.4.13. يجب توخي الحذر بشكل خاص لحماية جهاز الوسائط القابلة للإزالة والبيانات المخزنة

بها من الضياع أو السرقة أو التلف أو العطل الكهربائي. يجب تخزين جميع وسائط التخزين في بيئة آمنة بشكل مناسب من أجل التقليل من هذه المخاطر المادية.

3.4.13. مسؤوليات المستخدم:

1.3.4.13. يجب على مديري ومالكي أصول المعلومات التأكد من أن استخدام الوسائط القابلة للإزالة يتم التحكم فيه بشكل مناسب في نطاق مسؤوليتهم بما يتماشى مع أهداف هذه السياسة. كما يجوز لهم طلب تطبيق الضوابط التقنية لمنع استخدام الوسائط القابلة للنقل في ظروف معينة.

2.3.4.13. يجب أن يعلم موظفي **(جهة العمل)** الذين هم في حاجة لاستخدام الوسائط القابلة للإزالة في أعمالهم أنهم مسؤولين عن حصولهم على تصريح لاستخدامهم لها.

3.3.4.13. لا يجوز استخدام الوسائط الشخصية القابلة للإزالة لنقل أو تخزين بيانات **(جهة العمل)**.

4.3.4.13. يجب على من يستخدم أجهزة الوسائط القابلة للإزالة لنقل البيانات أن يهتم باختيار الطريقة المناسبة لنقل الجهاز، وأن يكون قادرًا وحريصًا على تجنب الأضرار أو الخسائر أثناء استخدامها ونقلها.

5.3.4.13. يجب أن يكون استخدام الوسائط القابلة للإزالة من قبل المتعاقدين والأطراف الثالثة مصرح به من **(جهة العمل)**، ووفقاً لسياسة حماية البيانات وسياسة الأطراف الثالثة.

6.3.4.13. التخلص من أجهزة الوسائط القابلة للإزالة

7.3.4.13. يجب عدم استخدام أجهزة الوسائط القابلة للإزالة المعطوبة أو التالفة. يجب على جميع المستخدمين إخطار قسم تكنولوجيا المعلومات [أو القسم المكافئ له] في هذه الحالة.

8.3.4.13. عندما تصل الوسائط القابلة للإزالة إلى نهاية عمرها الافتراضي، يجب التخلص منها عن طريق التدمير المادي بشكل آمن وكامل.

13. Removable Media Policy

13.1. Overview

Removable media refers to any type of computer storage devices that are not fixed inside a computer which used for backup or transportation of data, they can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs, Solid state memory devices including memory cards, flash memory (USB), as well as diskettes.

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations, it is very easy to lose, which can, and does, result in the compromise of large volumes of information. The loss of media can result in significant reputational damage, even if there is no evidence of what exactly has been lost. It can be utilized by attackers to transport malicious software from one environment to the other.

This policy made to control the use of removable media devices by all users who have access to information, information systems and IT equipment for the purposes of conducting official business.

13.2. Purpose

The purpose of this policy is to outline organizational responsibilities and controls around the use of removable media, to maintain the integrity of data, by minimizing the risk of loss or exposure of sensitive information maintained by **(Organization)**, and reducing the risk of acquiring malware infections on computers operated by **(Organization)**, and to prevent unauthorized disclosure, modification, removal or destruction of **(Organization)**'s information assets, and disruption to business activities.

13.3. Scope

This policy applies to all employees and partners of the **(Organization)**, and to contractual third parties who have access to **(Organization)** information, and covers all devices owned or operated by **(Organization)**, and any removable media used with those devices.

13.4. Policy

13.4.1. **Procurement & Use of Removable Media:**

13.4.1.1. Any removable media used to transport or store any **(Organization)** data should be purchased via approved channels.

13.4.1.2. All removable media devices and any associated equipment and software must only be purchased and installed by IT Department [or equivalent department].

13.4.1.3. The use of removable media within the **(Organization)** should only be used in cases where no suitable alternative exists (e.g. sanctioned network shares/cloud storage).

13.4.1.4. **(Organization)**'s removable media may not be connected to or used in computers that are not owned or leased by the **(Organization)** without explicit permission of **(Organization)**'s IT Department [or equivalent department].

13.4.1.5. Staff must only use **(Organization)**'s removable media in **(Organization)**'s devices. Non-**(Organization)** owned removable media devices must not be used to store any information used to conduct official **(Organization)** business, and must not be used with any **(Organization)** owned or leased IT equipment.

13.4.1.6. Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.

13.4.1.7. Removable media should not be the only place where data obtained for **(Organization)** purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

13.4.2. **Protection of Data:**

13.4.2.1. While in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the **(Organization)** from the data being lost while in transit or storage.

13.4.2.2. All **(Organization)**'s data stored on removable media devices must be encrypted where possible. If not, then all Confidential and Sensitive data held must be encrypted.

13.4.2.3. Confidential and Sensitive information must be stored on removable media only when required in the performance of assigned duties, and it must be encrypted in accordance with the **(Organization)** Encryption Policy. Guidance on encryption including recommended hardware and software should be available to staff.

13.4.2.4. Virus and malware checking software must be used when the removable media device is connected to a machine.

13.4.2.5. Special care must be taken to physically protect the removable media device and stored data from loss, theft, electrical corruption or damage. All storage media must be stored in an appropriately secure and safe environment in order to minimize physical risk.

13.4.3. **User Responsibility:**

13.4.3.1. Managers and information asset owners must ensure that use of removable media is suitably controlled within their area of responsibility in line with the objectives of this policy, and they may request technical controls to be implemented to prevent the use of removable media in certain circumstances.

13.4.3.2. **(Organization)** staff within professional services electing to use removable media, must be aware that they are responsible for having authorized permission to do so.

13.4.3.3. Personally owned removable media must not be used for the purposes of transporting or storing **(Organization)**'s data.

13.4.3.4. Staff using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

13.4.3.5. Use of removable media by a third party or contractor must be authorized, and in accordance with **(Organization)** Data Protection policy and Third-Party policy.

13.4.3.6. Disposing of Removable Media Devices

13.4.3.7. Damaged or faulty removable media devices must not be used. Users must contact IT Department [or equivalent department] in these cases.

13.4.3.8. When removable media has reached the end of its lifetime, it must be destroyed by the physical destruction of that media securely and completely.

14. سياسات جهاز التوجيه ومبدل الشبكة

1.14. المقدمة

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

2.14. الغرض

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

3.14. 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.

4.14. السياسة

1.4.14. **يجب أن يستوفي كل جهاز توجيه / مبدل معايير التهيئة التالية:**

1.1.4.14. 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.

2.1.4.14. يجب استخدام كلمة السر (enable secret) بدلاً من تمكين كلمة المرور (enable password).

3.1.4.14. يجب الحفاظ على كلمة السر (enable secret) مشفرة و مؤمنة على جهاز التوجيه أو المبدل.

4.1.4.14. 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.

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

1.2.4.14. نيابة عن (وكيل) بروتوكول حل العناوين (Proxy-ARP).

2.2.4.14. رسائل (ICMP) الغير قابلة للوصول.

3.2.4.14. التبديل السريع (Fast switching) والتبديل الذاتي (autonomous switching).

4.2.4.14. التخزين المؤقت للمسار متعدد البث (Multicast).

5.2.4.14. بروتوكول عمليات الصيانة (MOP).

3.4.14. **يجب ضبط الخدمات التالية:**

1.3.4.14. تشفير كلمة المرور.

2.3.4.14. مزامنة الوقت (NTP). يجب مزامنة جميع ساعات الشبكة مع مصدر زمن مشترك.

4.4.14. جميع تحديثات التوجيه (Routing) يجب ان تتم باستخدام تحديثات التوجيه الآمن.

5.4.14. استخدام نصوص SNMP الموحدة لـ**(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.

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

7.4.14. **يجب أن يحتوي كل جهاز توجيه (Router) على إشعار 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 كان محلياً أو عن بعد:

يحظر الدخول لهذا الجهاز لغير المصرح لهم.
يجب أن يكون لديك إذن صريح للدخول إلى هذا الجهاز أو ضبطه. أي إجراء 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

8.4.14. لا يجوز أبداً استخدام بروتوكول Telnet عبر أي شبكة لإدارة جهاز توجيه، ما لم يكن هناك نفق آمن يحمي مسار الاتصال بالكامل ، الإصدار 2 من بروتوكول (SSH) هو بروتوكول الإدارة المفضل.

9.4.14. ينبغي وضع أجهزة التوجيه والمبدلات في مكان يقتصر فيه الدخول على الأشخاص المرخص لهم فقط.

10.4.14. 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.

11.4.14. يجب أن يقوم المبدل بتوليد رسائل (SNMP TRAP) إذا وقع الاتصال وتم إعادة توليده في حال توفرت هذه الميزة.

12.4.14. 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.

13.4.14. **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:

1.13.4.14. متابعة ومراقبة لقوائم التحكم في الوصول لبروتوكول الإنترنت (IP Access List Accounting).

2.13.4.14. تسجيل وتوثيق أحداث الجهاز (Device logging).

3.13.4.14. 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.

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

1.14.4.14. رسم تخطيطي للشبكة.

2.14.4.14. ضوابط النظام (System configurations).

3.14.4.14. قواعد الجدار الناري.

4.14.4.14. عناوين بروتوكولات الإنترنت (IP Addresses).

5.14.4.14. قوائم التحكم في الوصول.

14. Router and Switch Security Policy

14.1. 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.

14.2. 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.

14.3. 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.

14.4. Policy

14.4.1. **Every router/switch must meet the following configuration standards:**

14.4.1.1. 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.

14.4.1.2. The enable secret must be used instead of enable password.

14.4.1.3. The enable secret on the router or switch must be kept in a secure encrypted form.

14.4.1.4. 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 discov-

ery protocols

14.4.2. **Routers and switches and/or interfaces should disallow the following:**

14.4.2.1. Proxy-ARP.

14.4.2.2. ICMP unreachable messages.

14.4.2.3. Fast switching and autonomous switching.

14.4.2.4. Multicast route caching.

14.4.2.5. Maintenance Operation Protocol (MOP).

14.4.3. **The following services must be configured:**

14.4.3.1. Password-encryption

14.4.3.2. Time syncing (NTP). All network clocks should be synced to a common time source.

14.4.4. All routing updates shall be done using secure routing updates.

14.4.5. 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.

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

14.4.7. **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 disci-
plinary 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.
```

14.4.8. 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.

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

14.4.10. 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.

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

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

14.4.13. **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:

14.4.13.1. IP access list accounting

14.4.13.2. Device logging

14.4.13.3. 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.

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

14.4.14.1. Network diagram

14.4.14.2. System configurations

14.4.14.3. Firewall rule set

14.4.14.4. IP Addresses

14.4.14.5. Access Control Lists

15. سياسة الاتصالات اللاسلكية

1.15. 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 العمل)** 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.

2.15. الغرض

الغرض من هذه السياسة هو تأمين وحماية أصول المعلومات التي تملكها **(جهة العمل)**. تمنح **(جهة العمل)** الوصول إلى هذه الموارد كامتياز 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 العمل)**، بحيث لا تتم الموافقة إلا على أجهزة البنية التحتية اللاسلكية التي تفي بالمعايير المحددة في هذه السياسة أو تلك التي تم منحها استثناء من قبل إدارة أمن المعلومات للاتصال بشبكة **(جهة العمل)**.

3.15. النطاق

تنطبق هذه السياسة على جميع أجهزة البنية التحتية اللاسلكية المتصلة بشبكة **(جهة العمل)** أو تكون موجودة ضمن موقع **(جهة العمل)** 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 العمل)**، كما تشمل جميع الموظفين التابعين لأطراف ثالثة والموكل لها إدارة أجهزة البنية التحتية اللاسلكية بالنيابة عن **(جهة العمل)**.

4.15. السياسة

1.4.15. **جميع أجهزة البنية التحتية اللاسلكية:** الموجودة في موقع **(جهة العمل)** والمتصلة بشبكتها، أو التي توفر الوصول إلى معلومات مصنفة على أنها سرية يجب عليها ما يلي:

1.1.4.15. الالتزام بالمعايير المحددة في معيار الاتصالات اللاسلكية.

2.1.4.15. استخدام بروتوكولات المصادقة والبنية التحتية المعتمدة من قبل **(جهة العمل)**.

3.1.4.15. استخدام بروتوكولات التشفير المعتمدة لدى **(جهة العمل)**.

4.1.4.15. الحفاظ على العناوين المادية للأجهزة (MAC) التي يمكن تسجيلها وتتبعها.

2.4.15. **للحد من احتمال إساءة استخدام الشبكة اللاسلكية:**

1.2.4.15. ينبغي أن تكون هناك مصادقة سليمة للمستخدم مع الاستبدال المناسب لآلية WEP وتتبع الشذوذ (Anomaly Tracking) على الشبكة المحلية اللاسلكية.

2.2.4.15. 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.

3.4.15. **بروتوكولات التشفير اللاسلكية:**

يفضل استخدام بروتوكول حماية الوصول للواي فاي الاصدار 3 (WAP3) كبروتوكول تشفير للشبكات اللاسلكية في حالة ما إذا كان الموجه (Router) او نقطة الوصول (Access point) تدعم هذه التقنية , و استخدام بروتوكول حماية الوصول للواي فاي الاصدار 2 (WPA2-AES) كبديل في حالة كان الموجه او نقطة الوصول لا تدعمWPA3 وذلك لأنه يوفر خوارزمية أمان أقوى وتشفيرًا متقدمًا كما يتحقق من صحة الرسالة وتكاملها.

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

1.4.4.15. رسم تخطيطي للشبكة.

2.4.4.15. ضوابط النظام (System configurations).

3.4.4.15. قواعد الجدار الناري.

4.4.4.15. عناوين بروتوكولات الانترنت (IP Addresses).

5.4.4.15. قوائم التحكم في الوصول.

15. Wireless Communication Policy

15.1. 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.

15.2. 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.

15.3. 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.

15.4. Policy

15.4.1. **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:

15.4.1.1. Abide by the standards specified in the Wireless Communication Standard.

15.4.1.2. Use **(Organization)** approved authentication protocols and infrastructure.

15.4.1.3. Use **(Organization)** approved encryption protocols.

15.4.1.4. Maintain a hardware address (MAC address) that can be registered and tracked.

15.4.2. **To stop the possible abuse of wireless network:**

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

15.4.2.2. 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

15.4.3. Wireless encryption protocols

15.4.3.1. WAP3 (Wi-Fi Protected Access version 3) is preferred as a wireless encryption protocol in case it is supported by the Router or the Access point, otherwise use WAP2-AES (Wi-Fi Protected Access version 2), because It offered a much stronger security algorithm and advanced level encryption with message authenticity and integrity validation.

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

15.4.4.1. Network diagram

15.4.4.2. System configurations

15.4.4.3. Firewall rule set

15.4.4.4. IP Addresses

15.4.4.5. Access Control Lists

16. سياسة الشبكة الافتراضية الخاصة (VPN)

1.16. 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.

2.16. الغرض

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

3.16. النطاق

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

4.16. السياسة

1.4.16. 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 العمل)** عبر وصلات الـ(VPN) الخاصة بهم.

2.4.16. 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)).

3.4.16. عندما يكون الاتصال بشبكة **(جهة العمل)** 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.

4.4.16. 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 الإنترنت الغير آمن إلى الشبكة المؤمنة باتصال بتقنية الـ(VPN).

5.4.16. بوابات الشبكات الافتراضية الخاصة (VPN gateways) يتم إعدادها وإدارتها من قبل موظفي القسم

الخاص بعمليات الشبكة لـ**(جهة العمل)**.

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

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

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

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

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

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

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

1.12.4.16. رسم تخطيطي للشبكة.

2.12.4.16. ضوابط النظام (System configurations).

3.12.4.16. قواعد الجدار الناري.

4.12.4.16. عناوين بروتوكولات الانترنت (IP Addresses).

5.12.4.16. قوائم التحكم في الوصول.

16. Virtual Private Network (VPN) Policy

16.1. 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.

16.2. 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.

16.3. 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.

16.4. Policy

16.4.1. 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.

16.4.2. 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.

16.4.3. 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.

16.4.4. 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.]

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

16.4.6. 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.

16.4.7. 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.

16.4.8. (Pings or other artificial network processes are not to be used to keep the connection open.)

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

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

16.4.11. 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.

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

16.4.12.1. Network diagram

16.4.12.2. System configurations

16.4.12.3. Firewall rule set

16.4.12.4. IP Addresses

16.4.12.5. Access Control Lists

17. سياسة جدار الحماية/الناري (Firewall)

1.17. 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 الإنترنت، حيث أنه من الضروري حماية الشبكات الخاصة الداخلية ومرافق الاتصالات الخاصة بـ**(جهة العمل)**.

2.17. 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.

3.17. 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)**.

4.17. السياسة

1.4.17. مراجعة مجموعة القواعد للتأكد من اتباعها للترتيب كما يلي:

1.1.4.17. مرشحات مكافحة الانتحال (حجب العناوين الخاصة والعناوين الداخلية التي تظهر من الخارج).

2.1.4.17. قواعد تصريح المستخدم (على سبيل المثال، السماح بـ HTTP إلى خادم الويب العام).

3.1.4.17. قواعد تصريح الإدارة (مثل رسائل تنبيه (SNMP traps) لخادم إدارة الشبكة).

4.1.4.17. الرفض والتنبيه (تنبيه مسؤولي الأنظمة حول حركة المرور المشبوهة).

5.1.4.17. الرفض والتوثيق (حفظ سجل حركة المرور للتحليل).

2.4.17. جدار الحماية القائم على التطبيق:

1.2.4.17. 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.

2.2.4.17. التأكد من مراقبة المسؤولين لأية محاولات لانتهاك سياسة الأمن باستخدام سجلات التدقيق التي تم إنشاؤها بواسطة جدار الحماية على مستوى التطبيق.

3.2.4.17. ضمان أن هناك آلية لتحديث وسد ثغرات الجدار الناري على مستوى التطبيقات والتحقق

بأنها محدثة لسد آخر الثغرات.

4.2.4.17. تأكد من وجود عملية لتحديث البرنامج بأحدث بصمات الهجوم.

5.2.4.17. في حالة تنزيل التواقيع من موقع الموردين والشركات المصنعة، يجب التأكد بأنها من موقع موثوق.

6.2.4.17. 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.

7.2.4.17. يجب حظر الأوامر التالية لـ SMTP في جدار الحماية على مستوى التطبيق:

- EXPN (التوسيع - expand)
- VRFY (تحقق- verify)
- DEBUG
- WIZARD

8.2.4.17. يجب حظر الأمر التالي لـ FTP:

- PUT

9.2.4.17. مراجعة وحظر العناوين (URL's) (والتأكد بانها ملائمة، فعلى سبيل المثال. يجب حظر أي عنوان URL لمواقع المخترقين.

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

3.4.17. **تفحص بحالة الاتصال (Stateful Inspection):**

1.3.4.17. مراجعة جداول الحالة (State Tables) للتأكد من إعداد القواعد المناسبة من حيث عناوين المصدر والوجهة ومنافذ المصدر والوجهة والمهلة.

2.3.4.17. تأكد من أن المهلة مناسبة حتى لا تعطي المتسلل الكثير من الوقت لشن هجوم ناجح.

- **بالنسبة لعناوين URL**

3.3.4.17. 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).

4.3.4.17. إذا كان الترشيح على عناوين MAC مسموح به، فيجب مراجعة المرشحات للتأكد من أنها مقتصرة على عناوين MAC المناسبة لـ **(جهة العمل)**.

4.4.17. **تسجيل الأحداث:**

1.4.4.17. تأكد من تفعيل خاصية تسجيل الأحداث وأن يتم مراجعة السجلات لتحديد أي أنماط محتملة قد تشير إلى وجود هجوم.

2.4.4.17. 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

5.4.17. **التصحيحات والتحديثات:**

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

2.5.4.17. إذا تم تنزيل التصحيحات والتحديثات تلقائيًا من مواقع الويب الخاصة بالموردين، فتأكد من استلام التحديث من موقع موثوق به.

3.5.4.17. 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.

6.4.17. **تقييم / اختبار الضعف:**

1.6.4.17. يجب التحقق ما إذا كان هناك إجراء لاختبار المنافذ المفتوحة باستخدام (NMAP)، وما إذا كانت المنافذ غير الضرورية مغلقة.

2.6.4.17. 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.

7.4.17. **الالتزام بسياسة الأمن:**

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

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

1.8.4.17. عناوين خاصة (RFC 1918)

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

2.8.4.17. عناوين محجوزة

- 240.0.0.0

3.8.4.17. عناوين غير قانونية

- 0.0.0.0

4.8.4.17. echo UDP

5.8.4.17. بث (RFC 2644) (ICMP)

17.4.9. الوصول عن بعد:

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

17.4.10. نقل الملفات:

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

17.4.11. حركة البريد الإلكتروني:

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

17.4.12. حظر حركة ICMP غير المرغوب فيها (ICMP 8, 11, 3):

17.4.12.1. تأكد من وجود قاعدة تمنع طلبات ورسائل ارتداد ICMP.

17.4.12.2. تأكد من وجود قاعدة تمنع إرسال رسائل تجاوز الوقت (Time Exceeded) ورسائل الإبلاغ عن عدم القدرة عن وصول للهدف (Unreachable).

17.4.13. الخوادم الحرجة والحساسة (Critical Servers):

17.4.13.1. 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).

17.4.14. جدران الحماية الشخصية:

17.4.14.1. 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.

17.4.14.2. 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.

17.4.14.3. 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.

15.4.17. **جدران الحماية الموزعة:**

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

2.15.4.17. التأكد من وجود ضوابط كافية لضمان سلامة السياسة أثناء النقل، على سبيل المثال، IPsec لتشفير السياسة عند النقل.

3.15.4.17. تأكد من وجود ضوابط كافية لمصادقة المضيف المناسب.

4.15.4.17. مرة أخرى يمكن استخدام IPsec للمصادقة مع شهادات التشفير.

16.4.17. **استمرار توافر جدران الحماية:**

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

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

1.17.4.17. رسم تخطيطي للشبكة.

2.17.4.17. ضوابط النظام (System configurations).

3.17.4.17. قواعد الجدار الناري.

4.17.4.17. عناوين بروتوكولات الانترنت (IP Addresses).

5.17.4.17. قوائم التحكم في الوصول.

17. Firewall Policy

17.1. Introduction

When a user connects to an insecure, open network, such as the Internet, he/she 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.

17.2. 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.

17.3. 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)**.

17.4. Policy

17.4.1. **Review the rulesets to ensure that they follow the order as follows:**

- 17.4.1.1. anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)
- 17.4.1.2. User permit rules (e.g. allow HTTP to public web-server)
- 17.4.1.3. Management permit rules (e.g. SNMP traps to network management server)
- 17.4.1.4. Deny and Alert (alert systems administrator about traffic that is suspicious)
- 17.4.1.5. Deny and log (log remaining traffic for analysis)

17.4.2. **Application based firewall:**

- 17.4.2.1. 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.
- 17.4.2.2. Ensure that the administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall.
- 17.4.2.3. Ensure that there is a process to update the application level firewall's vulnerabilities checked to the most current vulnerabilities.
- 17.4.2.4. Ensure that there is a process to update the software with the latest attack signatures.
- 17.4.2.5. In the event of the signatures being downloaded from the vendors' site, ensure that it is a trusted site.

17.4.2.6. 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.

17.4.2.7. The following commands should be blocked for SMTP at the application level firewall:

- EXPN (expand)
- VRFY (verify)
- DEBUG
- WIZARD

17.4.2.8. The following command should be blocked for FTP:

- PUT

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

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

17.4.3. **Stateful inspection:**

17.4.3.1. 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.

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

- **For URL's**

17.4.3.3. 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).

17.4.3.4. If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's at **(Organization)**.

17.4.4. **Logging:**

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

17.4.4.2. 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.

17.4.5. **Patches and updates:**

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

17.4.5.2. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.

17.4.5.3. 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.

17.4.6. **Vulnerability assessments/ Testing:**

17.4.6.1. Ascertain if there is a procedure to test for open ports using (NMAP) and whether unnecessary ports are closed.

17.4.6.2. 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.

17.4.7. **Compliance with security policy:**

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

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

17.4.8.1. 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

17.4.8.2. Reserved addresses

- 240.0.0.0

17.4.8.3. Illegal addresses

- 0.0.0.0

17.4.8.4. UDP echo

17.4.8.5. ICMP broadcast (RFC 2644)

17.4.9. **Remote access:**

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

17.4.10. **File Transfers:**

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

17.4.11. **Mail Traffic:**

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

17.4.12. **Block Unwanted ICMP Traffic (ICMP 8, 11, 3):**

17.4.12.1. Ensure that there is a rule blocking ICMP echo requests and replies.

17.4.12.2. Ensure that there is a rule blocking outgoing time exceeded and unreachable messages.

17.4.13. **Critical servers:**

17.4.13.1. 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.

17.4.14. **Personal firewalls:**

17.4.14.1. 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.

17.4.14.2. 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.

17.4.14.3. Ensure that there is a procedure to update the software for any new attacks that become known.

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

17.4.15. **Distributed firewalls:**

17.4.15.1. Ensure that the security policy is consistently distributed to all hosts especially when there are changes to the policy.

17.4.15.2. 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.

17.4.15.3. Ensure that there are adequate controls to authenticate the appropriate host.

17.4.15.4. Again IPsec can be used for authentication with cryptographic certificates.

17.4.16. **Continued availability of Firewalls:**

Ensure that there is a hot standby for the primary firewall

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

17.4.17.1. Network diagram

17.4.17.2. System configurations

17.4.17.3. Firewall rule set

17.4.17.4. IP Addresses

17.4.17.5. Access Control Lists

18. سياسة التشفير

1.18. مقدمة

يعد تقليل التعامل مع البيانات الحساسة للمؤسسة قدر الإمكان هو أفضل طريقة لحمايتها. يجب التعامل مع البيانات الحساسة فقط أثناء الحاجة لذلك لا أكثر. التشفير يعد أكثر أدوات حماية المعلومات فعالية عندما نكون في حاجة لمعالجة البيانات الحساسة.

مالكي الأصول الرقمية والمسؤولين عنها يجب أن يعلموا أن تشفير البيانات ليس بديلاً لضوابط حماية المعلومات، مثل إدارة التحكم في الوصول والتحقق من الهوية والتخويل؛ وأن التشفير يجب أن يستخدم بالتوازي مع هذه الضوابط والأدوات؛ وأن طرق تطبيق التشفير يجب أن تكون متناسبة مع احتياجات التأمين وتصنيف البيانات.

2.18. الغرض

الغرض من هذه السياسة هو إرشاد عام يقصر استخدام خوارزميات ومعايير معينة للتشفير، وهي الطرق التي حصل عليها مراجعة وتدقيق عام والتي أثبتت قدرتها على العمل بفاعلية في الظروف التشغيلية العملية. كما تشمل هذه السياسة على توجيهات تضمن أن كل المتطلبات التنظيمية والتشريعية ذات العلاقة يتم اتباعها والالتزام بها.

3.18. النطاق

تنطبق هذه السياسة على جميع الموظفين والشركاء في **(جهة العمل)**. وفي حالة وجود أي استثناء يتوجب الحصول على موافقة مسبقة من الجسم المسؤول عن الأمن السيبراني بـ**(جهة العمل)**.

4.18. السياسة

1.4.18. متطلبات عامة:

1.1.4.18. على **(جهة العمل)** تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير مبنية على احتياجاتها العملية ونتائج تحليل المخاطر، كما يتوجب أن تكون متوافقة مع التشريعات والضوابط التنظيمية ذات العلاقة.

2.1.4.18. يجب تشفير البيانات أثناء تخزينها وخلال انتقالها بالتوافق مع التشريعات والضوابط التنظيمية ذات العلاقة النافذة.

3.1.4.18. كلما أمكن، يتوجب الاقتصار فقط على استخدام الإصدارات المحدثة من طرق وخوارزميات ومفاتيح وأجهزة التشفير.

2.4.18. متطلبات الخوارزميات:

1.2.4.18. الشيفرات المستخدمة يجب أن تتوافق مع أو تزيد عما هو مذكو في وثيقة كتالوج الشيفرات الصادر عن فريق عمل أبحاث الإنترنت (IETF/IRTF Cipher Catalog) أو أي

وثيقة تحل محله عند زمن التطبيق. ينصح بشدة باستخدام معيار التشفير المتقدم (Advanced Encryption Standard - AES) في التشفير التماثلي.

.2.2.4.18 الخوارزميات المستخدمة يجب أن تتبع الضوابط المنصوص عليها في وثيقة المعيار الدولي رقم: ISO/IEC 18033-3:2010، أو أي وثيقة تحل محله عند زمن التطبيق وتعتمدها الهيئة الوطنية لأمن وسلامة المعلومات. ينصح بشدة باستخدام كل من خوارزميات التشفير RSA , ECC في التشفير اللاتماثلي.

.3.2.4.18 خوارزميات التوقيع المعتمدة هي كل من:

الخوارزمية	أقل طول للمفتاح
ECDSA	P-256
RSA	2048
LDWM	SHA256

.3.4.18 **متطلبات دالة الاختزال (Hash Function):**

بشكل عام يتوجب على **(جهة العمل)** الالتزام بالتالي:

.1.3.4.18 SHA-1: على المؤسسات الحكومية التوقف عن استخدام دالة الاختزال من نوع: (SHA-1) لغرض توليد التوقيعات الرقمية أو أختام الزمن وأي تطبيق يتطلب أن يكون مقاوماً لحوادث تصادم الدوال وتكرارها (Collision Resistance). يسمح للمؤسسات الحكومية أن تستخدم النوع (SHA-1) في التطبيقات التالية: التحقق من تواقيع رقمية وأختام زمنية قديمة أو توليد أو التحقق من رموز التثبت من الرسائل (HMACs) أو دوال اشتقاق المفاتيح (KDFs) أو دوال توليد الأرقام العشوائية.

.2.3.4.18 SHA-2 (أي كل من SHA-224 و SHA-256 و SHA-384 و SHA-512 و 224/SHA-512 و 256/SHA-512): يمكن للمؤسسات الحكومية أن تستخدم أياً من دوال الاختزال هذه للتطبيقات التي تعتمد على خوارزميات اختزال آمنة في عملها. تشجع الهيئة مصممي البروتوكولات على اعتماد دالة الاختزال نوع: (SHA-256) كحد أدنى لأي تطبيق يتطلب أن يكون متوافقاً للعمل مع الغير.

.3.3.4.18 SHA-3 (أي كل من SHA3-224 وSHA3-256 وSHA3-384 وSHA3-512 وSHAKE128 و SHAKE256): يمكن للمؤسسات الحكومية أن تستخدم خوارزميات الاختزال من نوع SHA-3 ثابتة الطول في التطبيقات التي تستخدم خوارزميات اختزال آمنة.

.4.4.18 **التوافق على المفاتيح والتحقق من الهوية:**

.1.4.4.18 عملية تبادل المفاتيح يجب أن تستخدم أحد بروتوكولات التشفير التالية: ديفي-هيلمان (Diffie-Hellman) أو آي كي إي (IKE) أو ديفي-هيلمان بالمنحنى الإهليلجي (Elliptic curve Diffie-Hellman (ECDH)).

2.4.4.18. يجب التحقق من هوية أطراف الاتصال قبل البدء في تبادل المفاتيح الجلسات أو اشتقاقها.

3.4.4.18. المفاتيح العامة المستخدمة في تأسيس الثقة يجب التحقق منها قبل استخدامها.

4.4.4.18. يتوجب على كل خوادم التحقق من الهوية (مثل RADIUS أو TACACS) أن تكون مثبتة عليها شهادة صالحة موقعة من قبل مزود موثوق به.

5.4.4.18. يتوجب على كل الخوادم والتطبيقات التي تستخدم بروتكول SSL أو TLS أن يكون لديها شهادة صالحة موقعة من قبل مزود معروف وموثوق به.

5.4.18. **توليد المفاتيح:**

1.5.4.18. مفاتيح التشفير يجب أن تولد وتخزن بطريقة آمنة تحميها من الضياع أو السرقة أو للفضح.

2.5.4.18. يجب أن يعتمد توليد المفاتيح على مولد أرقام عشوائية يتبع معياراً معتمداً.

18. Encryption Policy

18.1. Overview

The most reliable way to protect the **(Organization)**'s sensitive data is to avoid as much as possible handling sensitive data. Sensitive data should be retained or handled only when required. Encryption can be an effective information protection control when it is necessary to possess sensitive data.

IT Owners and IT Custodians should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs and classification of the data.

18.2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that related regulations are followed.

18.3. Scope

This policy applies to all **(Organization)**'s employees and affiliates. Any exception to the policy must be approved by the Infosec team in advance.

18.4. Policy

18.4.1. **General requirements:**

18.4.1.1. The **(Organization)** should develop and document and adopt procedures and standards for the encryption based on business needs and risk analysis, and in accordance with all relevant regulations and standards.

18.4.1.2. Data must be encrypted in storage and while in transit and in accordance with all relevant regulations and standards.

18.4.1.3. As much as possible, only the updated versions of encryption methods, algorithms, keys and equipment are to be used.

18.4.2. **Algorithm Requirements:**

18.4.2.1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

18.4.2.2. Algorithms in use must meet the standards defined for use in ISO/IEC 18033-3:2010 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

18.4.2.3. Signature Algorithms:

Algorithm	Key Length (min)
ECDSA	P-256
RSA	2048
LDWM	SHA256

18.4.3. **Hash Function Requirements:**

In general, **(Organization)** should adheres to the following:

18.4.3.1. SHA-1: Government entities should stop using SHA-1 for generating digital signatures, generating time stamps and for other applications that require collision resistance. Government bodies may use SHA-1 for the following applications: verifying old digital signatures and time stamps, generating and verifying hash-based message authentication codes (HMACs), key derivation functions (KDFs), and random bit/number generation.

18.4.3.2. SHA-2 (i.e., SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256): Government entities may use these hash functions for all applications that employ secure hash algorithms. NISSA encourages application and protocol designers to implement SHA-256 at a minimum for any applications of hash functions requiring interoperability.

18.4.3.3. SHA-3 (i.e., SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 and SHAKE256): Government entities may use the four fixed-length SHA-3 algorithms—SHA3-224, SHA3-256, SHA3-384, and SHA3-512 for all applications that employ secure hash algorithms.

18.4.4. **Key Agreement and Authentication:**

18.4.4.1. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

18.4.4.2. End points must be authenticated prior to the exchange or derivation of session keys.

18.4.4.3. Public keys used to establish trust must be authenticated prior to use.

18.4.4.4. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

18.4.4.5. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

18.4.5. **Key Generation:**

18.4.5.1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

18.4.5.2. Key generation must be seeded from an industry standard random number generator (RNG).

19. سياسة أمان الحوسبة السحابية

1.19. مقدمة

خدمات الحوسبة السحابية هي تطبيقات وموارد البنية التحتية التي تُستخدم في مجموعة كبيرة من الأعمال المختلفة. ويتم تعريفها على أنها مصطلح يشير الي المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية وقدرات المعالجة البرمجية، كما يستطيع المشتركين بالخدمة التحكم في هذه الموارد عن بعد عبر الاتصال الشبكي كالإنترنت.

تقدم خدمات الحوسبة السحابية العديد من المزايا واهمها الأداء العالي مع انخفاض تكلفتها، وهي سهلة الاستخدام بشكل عام للأفراد والمؤسسات، ويمكن الوصول إليها عبر الإنترنت من خلال مجموعة من المنصات المختلفة (محطات العمل وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية). ولكن بدون وجود ضوابط كافية قد يعرض استخدامها الأفراد والمؤسسات للتهديدات عبر الإنترنت كفقدان البيانات أو السرقة، والوصول غير المصرح به إلى الشبكة، لذلك وجب أن يكون هناك بعض الإرشادات الخاصة بنوع بيانات **(جهة العمل)** المناسبة للتخزين والمشاركة باستخدام هذه الخدمات.

هناك عدد من المخاوف المتعلقة بأمن المعلومات وخصوصية البيانات عند استخدام خدمات الحوسبة السحابية في **(جهة العمل)**، وذلك يشمل الآتي:

- **(جهة العمل)** لا تقوم بحماية بياناتها أو تتحكم فيها، مما يؤدي إلى فقدان الأمن أو تدنيه أو عدم القدرة على الامتثال للوائح وقوانين حماية البيانات المختلفة وفقدان خصوصيتها، وربما يرجع ذلك إلى تجميع البيانات مع مستخدمين آخرين للخدمات السحابية.
- اعتماد **(جهة العمل)** على طرف ثالث في عمليات البنية التحتية الحيوية ومعالجة البيانات.
- مستوى الأمن والعيوب التكنولوجية في البنية التحتية التي يقدمها مورد السحابة.

2.19. الغرض

تحدد هذه السياسة أفضل الممارسات والعمليات المقبولة لاستخدام خدمات الحوسبة السحابية لـ**(جهة العمل)** لضمان تخزين البيانات بشكل آمن أو مشاركتها باستخدام الخدمات السحابية العامة و / أو مشاركة الملفات، وتهدف إلى إرشاد مزودي الخدمات السحابية لحماية المستخدمين وتقديم أفضل الخدمات لهم.

3.19. النطاق

تنطبق هذه السياسة على جميع الموظفين في **(جهة العمل)** من يملكون صلاحية الوصول واستخدام خدمات موردي الخدمات السحابية القادرة على تخزين أو نقل البيانات الإلكترونية التي تملكها **(جهة**

العمل)، وعلى اي أطراف ملزمة بموجب الاتفاقات والعقود بالتعامل مع البيانات التي تمتلكها **(جهة العمل)**.

كما تنطبق على جميع مزودي خدمات الحوسبة السحابية التي توفر الخدمات والأنظمة الأساسية والبنية التحتية التي توفر الدعم لمجموعة واسعة من الأنشطة التي تتضمن معالجة البيانات المؤسسية أو تبادلها أو تخزينها أو إدارتها.

4.19. السياسة

19.4.1. مستخدم الخدمات السحابية:

19.4.1.1. الالتزام الدائم بجميع الضوابط واللوائح والتعليمات والسياسات الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات وجميع التشريعات النافذة ذات العلاقة بالبلاد.

19.4.1.2. يتوجب على الجهات الحكومية أو تلك التي تصنف من المؤسسات التي تقع في نطاق مسؤوليتها بنى تحتية حيوية وحساسة ألا تشترك في خدمات حوسبة سحابية لا تقع داخل البلاد بما في ذلك كل الأنظمة المستخدمة لهذه الخدمة مثل التخزين والمعالجة ومراكز التعافي من الكوارث وأنظمة المراقبة والدعم. كما يتوجب عليها التحقق من التزام مزود الخدمة بهذه المتطلبات قبل البدء في الخدمة وأثناءها.

19.4.1.3. على الجهات الحكومية أو تلك التي تصنف من المؤسسات التي تقع في نطاق مسؤوليتها بنى تحتية حيوية وحساسة والتي تشترك في خدمات حوسبة سحابية داخل البلاد أن تتحقق من قيام مقدم الخدمة بعزل أنظمة الحوسبة السحابية الخاصة بهم عن غيرها من أنظمة المشتركين الآخرين.

19.4.1.4. العمل على مراقبة الشبكة الداخلية والخارجية لمقدم الخدمة للكشف عن أي نشاطات مشبوهة.

19.4.1.5. وضع آلية لمتابعة ومراقبة مدى التزام مقدم الخدمة بجميع الضوابط واللوائح والتعليمات والسياسات الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات وجميع التشريعات النافذة ذات العلاقة بالبلاد.

19.4.1.6. يجب عمل تقييم شامل لمخاطر استخدام خدمات الحوسبة السحابية ومراجعتها واعتماد توصياته من قبل الإدارة العليا لـ**(جهة العمل)** قبل بدء استخدامها وتحديد المستوى المقبول من المخاطر وإبلاغ مقدم الخدمة به.

19.4.1.7. يجب أن يكون استخدام الخدمات السحابية في أغراض العمل مصرحاً رسمياً من إدارة / قسم تكنولوجيا المعلومات، حيث انه المسؤول عن ضمان الأمن والخصوصية وجميع متطلبات تكنولوجيا المعلومات الأخرى للبيانات التي سيتم معالجتها وحفظها بشكل مناسب من قبل مزود الخدمات السحابية.

19.4.1.8. حصر وتوثيق جميع الخدمات السحابية وتقنيات المعلوماتية والاتصالات ذات العلاقة.

9.1.4.19. يجب مراجعة شروط الخدمة التي يفرضها موردو خدمات الحوسبة السحابية والتي تتطلب موافقة المستخدمين من قبل إدارة تكنولوجيا المعلومات قبل الموافقة عليها.

10.1.4.19. يتوجب على الجهات الحكومية أو تلك التي تصنف من المؤسسات التي تقع في نطاق مسؤوليتها بنى تحتية حيوية وحساسة القيام بتصنيف البيانات قبل استضافتها في السحابة فإذا كانت البيانات مصنفة على أنها سرية "مقيدة» أو حساسة «داخلية» (يجب أن تستضاف في السحابة الحكومية) أما البيانات المصنفة على أنها عامة يمكن أن تستضاف في السحابة التجارية.

11.1.4.19. يجوز تخزين البيانات المصنفة على أنها عامة و/أو حساسة في الخدمات السحابية المشتركة، ولا يجوز تخزين البيانات السرية و/أو المقيدة في هذا النوع من الخدمات الحوسبة السحابية.

12.1.4.19. يجب تطبيق آليات الإدارة المؤمنة للجلسات بحيث تشمل التحقق من صحة وموثوقية الجلسة وإقفالها وإنهاء المهلة المحددة لها.

13.1.4.19. اعتماد آلية التحقق من الهوية متعدد العناصر وخاصة للحسابات ذات الصلاحيات الحساسة والهامة.

14.1.4.19. تطبيق آليات كشف محاولات الدخول لغير المصرح لهم وإيقافها، كوضع حد أقصى لعدد مرات المحاولات الغير ناجحة (تكون ثلاثة للحسابات الحساسة) وإضافة مهلة إقفال متزايدة المدة بعد كل محاولة فاشلة.

15.1.4.19. يجب على الموظفين المصرح لهم استخدام الخدمات السحابية عدم مشاركة بيانات تسجيل الدخول مع زملاء العمل الآخرين.

16.1.4.19. يجب أن يتوافق استخدام الخدمات السحابية مع جميع السياسات التي تَحكُم التعامل مع أي بيانات تملكها أو تجمعها **(جهة العمل)**.

17.1.4.19. لا يجوز استخدام حسابات الخدمات السحابية الشخصية لتخزين أو معالجة أو تبادل البيانات المملوكة لـ**(جهة العمل)**.

18.1.4.19. يجب أن توفر حلول الحوسبة السحابية نفس مستويات الخدمة في **(جهة العمل)** أو أفضل منها لضمان استمرارية الأعمال وذلك بما يتماشى مع متطلبات الأعمال التي يتم تقديمها.

19.1.4.19. يجب أن تحمي الحوسبة السحابية أمن وخصوصية بيانات **(جهة العمل)**، وأن تمتثل لجميع متطلبات الأمن والخصوصية المناسبة.

20.1.4.19. عند اختيار الخدمات السحابية يجب مراعاة تأثير استخدامها على استقرار عمليات تشغيل الأنظمة الأساسية لـ**(جهة العمل)** وأداؤها.

19.1.4.21. يجب أن يمتثل مستخدمي الحوسبة السحابية لجميع السياسات المتبعة في **(جهة العمل)** أثناء تعاملهم مع البيانات المخزنة في السحابة.

19.1.4.22. العمل على حماية ووضع جميع آليات الأمان السيبراني اللازمة لتأمين قناة الاتصال الشبكي مع مقدم خدمة الحوسبة السحابية.

19.1.4.23. يتوجب التحقق من عدم احتواء الأجهزة المحمولة على أي بيانات ومعلومات مقيدة أو سرية عند إرجاعها أو التخلص منها أو إعادة استخدامها.

19.1.4.24. التحقق من وجود ضمانات من مقدم الخدمة بالعمل على حذف بيانات المشترك بطريقة آمنة عند انتهاء التعاقد.

19.1.4.25. تبني وسائل وآليات آمنة عند تصدير ونقل البيانات والأنظمة من منظومات الحوسبة السحابية لمقدم الخدمة.

19.1.4.26. يجب التحقق مما إذا كانت الخدمة السحابية المقترحة قد تم قبولها بالفعل من قبل الإدارة العليا لمنع الازدواج المحتمل في الجهد أو التكلفة الغير الضروري.

19.1.4.27. يجب تشفير البيانات المستخدمة في **(جهة العمل)**، سواء كانت ثابتة أو قيد الحركة، ضمن أي بيئة سحابية معتمدة.

19.1.4.28. في حالة وجوب تشفير البيانات المخزنة مع مورد الخدمة السحابية، فيجب القيام بذلك باستخدام مفاتيح التشفير التي تملكها وتعمل بها **(جهة العمل)**.

19.1.4.29. تحديد وتقييم المكتب الرئيسي لمورد خدمات الحوسبة السحابية وموقع التخزين والمعالجة للبيانات.

19.1.4.30. قد تعتبر تطبيقات الأجهزة المحمولة خدمات سحابية إذا كانت «تخزن أو تعالج أو تنقل معلومات **(جهة العمل)** خارج حدود شبكتها».

19.1.4.31. يجب التأكد من أن اتفاقية مستوى الخدمة وشروط الاستخدام مناسبة لغرض استخدامها وتتمثل للمتطلبات أمن المعلومات لـ**(جهة العمل)**.

19.1.4.32. يجب التأكد من أن مزود الخدمات السحابية يعمل بنظام تعريف للوصول مناسب (يعتمد على الوظيفة).

19.1.4.33. سيدرج قسم تكنولوجيا المعلومات استمرارية الأعمال والتعافي من الكوارث في ضوابط أمن السحابة الخاصة به.

19.1.4.34. يجب أن تحدد إدارة / قسم تكنولوجيا المعلومات كيفية الإبلاغ عن حوادث أمان السحابة وإدارتها.

19.1.4.35. يجب أن تقوم إدارة / قسم تكنولوجيا المعلومات، بالتعاون مع الإدارة القانونية لـ **(جهة العمل)**، بإعداد وتنفيذ اتفاقيات مستوى الخدمة المناسبة (SLAs) مع موفري الخدمات

السحابية لضمان أداء مقبول لموردي الخدمات السحابية.

36.1.4.19. يجب توثيق جميع التغييرات المقترحة على عمليات الأمن السحابي بالتفصيل.

37.1.4.19. يجب تحديد انتهاكات أمن السحابة التي قد تؤثر على عمليات تكنولوجيا المعلومات الخاصة بـ **(جهة العمل)** في نظام إدارة أمن المعلومات بها والخطط المرتبطة به.

38.1.4.19. يجب أن تحدد إدارة / قسم تكنولوجيا المعلومات عمليات وإجراءات أمان السحابة؛ تأمين واستخدام البرامج والأنظمة المتخصصة للحد من خطر اختراق الأمن السحابي، اختبار أمان محيط **(جهة العمل)** بانتظام ومحيط مزود الخدمات السحابية باستخدام اختبارات الاختراق وطرق التحليل الجنائي الأخرى، وتوثيق كافة الإجراءات والضوابط الخاصة بسحابة المعلومات.

39.1.4.19. ستضع إدارة / قسم تكنولوجيا المعلومات وتوثق عملية رسمية لتحديد الاختراق المحتمل في محيط الشبكة السحابية (على سبيل المثال، هجوم رفض الخدمة، والتصيد الاحتيالي)، وتقييم عملية الاختراق وتحديد طبيعتها وتأثيرها المحتمل، وإخطار إدارة **(جهة العمل)** بعملية الاختراق، والتقليل من تأثير الاختراق في أسرع وقت ممكن وتوثيق الخطوات المتخذة عند التعامل مع الحادث. ستنطبق هذه العملية على جميع البيئات السحابية، سواء كانت سحابية داخلية أو مختلطة و / أو عامة.

40.1.4.19. ستضع إدارة / قسم تكنولوجيا المعلومات وتوثق عملية رسمية لتحديد الاختراق الداخلي المحتمل لأمن السحابة (على سبيل المثال، سرقة المعلومات، والهندسة الاجتماعية، والوصول غير المصرح به إلى الأنظمة)، وتقييم عملية الاختراق وتحديد طبيعتها وتأثيرها المحتمل، وإخطار إدارة **(جهة العمل)** بعملية الاختراق والتقليل من تأثير الاختراق في أسرع وقت ممكن، وتوثيق الخطوات المتخذة عند التعامل مع الحادث.

41.1.4.19. إجراء عملية تقييم ومعالجة الثغرات للخدمات السحابية المشترك بها مرة واحدة كل ستة أشهر على الأقل.

42.1.4.19. القيام بمعالجة والتعامل مع ما يبلغ عنه من ثغرات من قبل مزود الخدمة.

43.1.4.19. العمل على تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني وتأمينها للأصول ذات العلاقة بالخدمات السحابية والقيام بالمراقبة المستمرة لها ومتابعتها ومراجعتها بشكل دوري.

44.1.4.19. الالتزام بسياسة التعامل مع حوادث الأمن السيبراني الصادرة عن الهيئة الوطنية لأمن المعلومات، وإلزام مقدمي الخدمة بها.

45.1.4.19. الالتزام بسياسات وضوابط التعافي من الكوارث واستمرارية الأعمال الصادرة عن الهيئة الوطنية لأمن المعلومات، وإلزام مقدمي الخدمة بها.

19.2.4. مقدم الخدمات السحابية:

19.2.4.1. الالتزام الدائم بجميع الضوابط واللوائح والتعليمات والسياسات الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات وجميع التشريعات النافذة ذات العلاقة بالبلاد.

19.2.4.2. يجب أن يحدد مزودي الخدمات السحابية للمستخدمين الخدمات التي سيتم تقديمها للمشتركين ومتطلبات الأمن السيبراني لديهم.

19.2.4.3. ضرورة عزل خدمات الحوسبة السحابية المقدمة للجهات الحكومية أو تلك التي تصنف من المؤسسات التي تقع في نطاق مسؤوليتها بنى تحتية حيوية وحساسة عن الخدمات الحوسبة السحابية المقدمة للمؤسسات الأخرى.

19.2.4.4. حصر جميع الأصول الخاصة بتقنيات المعلوماتية والاتصالات ذات العلاقة والتابعة لمقدم الخدمة، كما يجب تحديد ملاك لتلك الأصول وحفظ كل هذه المعلومات وتحديثها بشكل دائم ضمن قاعدة بيانات أو آلية أخرى مناسبة.

19.2.4.5. يجب على مزودي الخدمات السحابية الحفاظ على سرية وسلامة وحماية البيانات بما في ذلك النسخ الاحتياطية وفترات الاحتفاظ بها، فلا يجوز لهم معالجة البيانات أو تغييرها أو تعديلها أو نقلها بين الأنظمة لديهم.

19.2.4.6. يجب على مزودي الخدمات السحابية ابلاغ المستخدمين مقدماً وأخذ موافقتهم في حالة سيتم نقل أو تخزين أو معالجة المحتوى الخاص بهم.

19.2.4.7. ضرورة الفصل بين الشبكات الخاصة بالحوسبة السحابية وعزلها عن الشبكات الأخرى الداخلية لمقدم الخدمة والخارجية والعمل على تأمينها بالوسائل التقنية الملائمة.

19.2.4.8. تطبيق آليات الحماية من هجمات حجب الخدمة بنوعيها (DoS and DDoS).

19.2.4.9. ضرورة تشفير البيانات أثناء انتقالها عبر شبكات مقدم الخدمة بما في ذلك بيانات عمليات إدارة الأنظمة السحابية.

19.2.4.10. تطبيق آليات التحكم في الوصول بين أجزاء الشبكات المختلفة.

19.2.4.11. وضع ضمانات عدم حصول تداخل في بيانات المستخدمين وعزلها بشكل تام عن بعضها.

19.2.4.12. الالتزام باتباع مبدأ الحد الأدنى من الوظائف المطلوبة لتنفيذ العمل ليس أكثر.

19.2.4.13. تطبيق آليات التعامل بطريقة آمنة مع التحقق من المدخلات والاستثناءات وحالات الفشل (Input Validation, Exceptions and Failures).

19.2.4.14. ضرورة العمل على الفصل بين آليات وتقنيات الأمن السيبراني وعزلها عن باقي التطبيقات والتقنيات الخاصة بخدمة الحوسبة السحابية.

15.2.4.19. توفير آليات خاصة بالأمن السيبراني التي يمكن للمشتركين الاستفادة منها وعرضها عليهم، وتحديد مستوى معين خاص للمشتركين الحكوميين يتم إلزامهم به بشرط أن يحصل مقدم خدمة الحوسبة السحابية على اعتماد لهذه الخدمات الإلزامية من الهيئة الوطنية لأمن وسلامة المعلومات بالخصوص.

16.2.4.19. يجب على مزودي الخدمات السحابية توفير خطة الاستجابة والتعافي من الكوارث وخطة استمرارية الأعمال والدعم الفني.

17.2.4.19. يجب على مزودي الخدمات السحابية توضيح مواقع حفظ البيانات الجغرافية للمشتركين.

18.2.4.19. يجب على مزودي الخدمات السحابية منح الحق للمستخدمين في تغيير مزود الخدمة والانتقال إلى مزود خدمات سحابية آخر.

19.2.4.19. يجب تطبيق آليات الإدارة المؤمنة للجلسات بحيث تشمل التحقق من صحة وموثوقية الجلسة وإقفالها وإنهاء المهلة المحددة لها.

20.2.4.19. اعتماد آلية التحقق من الهوية متعدد العناصر وخاصة للحسابات ذات الصلاحيات الحساسة والهامة.

21.2.4.19. تطبيق آليات كشف محاولات الدخول لغير المصرح لهم وإيقافها، كوضع حد أقصى لعدد مرات المحاولات الغير ناجحة (تكون ثلاثة للحسابات الحساسة) وإضافة مهلة إقفال متزايدة المدة بعد كل محاولة فاشلة.

22.2.4.19. عدم حفظ كلمات المرور للحسابات بمختلف أنواعها في هيئة نص غير مُشفّر، بل تعالج بطرق وخوارزميات تأمين تخزين كلمات المرور مثل دالة الاختزال (Hashing and Salting).

23.2.4.19. إخفاء بيانات التحقق من الهوية وبالأخص كلمة المرور أثناء عرضها للمستخدم لحمايتها من التلصص.

24.2.4.19. ضرورة الحصول على موافقة مبدئية واضحة وموثقة من مشترك الخدمة قبل الدخول إلى أي من الأصول والبيانات الخاصة بذاك المشترك.

25.2.4.19. حصر وتكوين قائمة جرد محدثة بشكل دائم لجميع الأجهزة المحمولة المصرح لها للعمل داخل أنظمة مقدم الخدمة. والعمل على إدارة آليات الأمان السيبراني للأجهزة المحمولة بشكل مركزي. كما يتوجب التحقق من عدم احتواء الأجهزة المحمولة على أي بيانات ومعلومات مقيدة أو سرية عند إرجاعها أو التخلص منها أو إعادة استخدامها.

26.2.4.19. تفعيل خاصية القفل الآلي لشاشة الأجهزة المحمولة حسب السياسات المتبعة والمعتمدة.

27.2.4.19. العمل على تزويد المشتركين بآليات وتقنيات وإجراءات أمنة لحفظ وتخزين البيانات

وكذلك لعملية حذفها وإتلافها. والعمل على إتلاف بيانات المشتركين المنتهية عقود خدمتهم بطريقة آمنة.

19.2.4.28. تيسير عملية نقل مشتركي الخدمة لبياناتهم وتصديرها بصيغة تمكنهم من نقلها لمزود آخر وتأمين هذه الخطوة.

19.2.4.29. ضمان أمان عملية الوصول وتخزين ونقل محتويات النسخ الاحتياطية لبيانات المشتركين والوسائط الموجودة عليها.

19.2.4.30. ضمان أمان عملية الوصول وتخزين ونقل محتويات النسخ الاحتياطية لأنظمة وتقنيات إدارة وعمل الخدمات السحابية الخاصة بالمشتركين.

19.2.4.31. إجراء عملية تقييم ومعالجة الثغرات للمكونات السحابية مرة واحدة كل ستة أشهر على الأقل.

19.2.4.32. إبلاغ المشترك بما يكتشف من ثغرات التي قد تؤثر عليه وتوضيح كيف يمكنه معالجتها.

19.2.4.33. القيام بعملية اختبار الاختراق للأنظمة السحابية والمكونات الأخرى الداعمة لها مرة واحدة فالسنة على الأقل.

19.2.4.34. العمل على تفعيل سجلات الأحداث (Event Logs) وآليات التدقيق (Audit Trails) لمكونات الحوسبة السحابية وضمان حمايتها وحفظها. وخاصة لجميع العمليات التي تجرى على الأنظمة السحابية للمشتركين.

19.2.4.35. العمل على تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني وتأمينها. والقيام بالمراقبة المستمرة ومتابعتها ومراجعتها بشكل دوري باستخدام تقنيات أو حلول إدارة أحداث ومعلومات الأمن السيبراني (SIEM).

19.2.4.36. الالتزام بسياسات وضوابط التعامل مع حوادث الأمن السيبراني الصادرة عن الهيئة الوطنية لأمن المعلومات.

19.2.4.37. وجوب تبليغ المشتركين فور حدوث حوادث الأمن السيبراني التي قد تؤثر عليهم ودعمهم في عملية التعامل معها.

19.2.4.38. ضرورة تفعيل سجلات أحداث محاولات الدخول (Login) وحفظها.

19.2.4.39. الالتزام بسياسات وضوابط التعافي من الكوارث واستمرارية الأعمال الصادرة عن الهيئة الوطنية لأمن المعلومات.

19. Cloud Computing Security Policy

19.1. Overview

Cloud computing services are application and infrastructure resources that are used in a wide range of business activities. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing services offers many advantages including low costs, high performance, and they are generally easy for people and organizations to use, they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones). However, without adequate controls, it also exposes individuals and organizations to Online threats such as data loss or theft, unauthorized access to corporate networks, and so on. There should be some guidelines for the type of **(Organization)**'s information that is appropriate for storing and sharing using these services.

There are a number of information security and data privacy concerns about the use of cloud computing services at the **(Organization)**. They include:

- **(Organization)** no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws Loss of privacy of data, potentially due to aggregation with data from other cloud consumers.
- **(Organization)** dependency on a third party for critical infrastructure and data handling processes.
- Potential security and technological defects in the infrastructure provided by a cloud vendor.

19.2. Purpose

This policy outlines best practices and approval processes for using cloud computing services at **(Organization)** to ensure that **(Organization)**'s protected or sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services, and it also guides the cloud service providers to give users a secure appropriate services.

19.3. Scope

This policy applies to all **(Organization)** staff who access and use cloud services that capable of storing or transmitting electronic data that are owned or leased by **(Organization)**, and to all parties who are contractually bound to handle data produced by **(Organization)**, and in accordance with **(Organization)** contractual agreements and obligations.

This also applies to all cloud computing resources that provide services, platforms, and infrastructure providing support for a wide range of activities involving the processing, exchange, storage, or management of institutional data.

19.4. Policy

19.4.1. **Cloud Services Users:**

19.4.1.1. Permanent adherence to all laws, regulations, instructions and policies issued by the National Information Security & Safety Authority (NISSA) and all issued legislation related to the country.

19.4.1.2. Government entities or those classified as institutions with critical infrastructure responsibility are obligated to refrain from subscribing to cloud computing services that are not located within the country, including all systems used for this service such as storage, processing, disaster recovery centers, monitoring and support systems. Said entities must also verify that the service provider complies with these requirements prior to launching and during the service.

19.4.1.3. All governmental entities and all organizations, that have any critical infrastructure under their purview that utilize cloud services, that are located on the Libyan territories, should verify that their cloud service provider has isolated their cloud from other subscribers' systems.

19.4.1.4. **(Organization)** must monitor the internal and external network of the service provider to detect any suspicious activities.

19.4.1.5. Establish a mechanism to follow up and monitor the service provider's commitment to all laws, regulations, instructions and policies issued by NISSA and all applicable legislation related to the country.

19.4.1.6. A comprehensive assessment of the risks pertaining to the usage of cloud computing services must be conducted, reviewed. Then approved by the senior management of the **(Organization)** before starting to use them, determining the acceptable level of risk beforehand and reporting it to the service provider.

19.4.1.7. The use of cloud services for business purposes must be officially authorized by the IT department, which is responsible for ensuring security, privacy and all other IT requirements in order for the data to be properly processed and saved by the cloud service provider.

19.4.1.8. An inventory of all cloud services and associated information and communication technologies must be conducted and documented.

19.4.1.9. Terms of service required by cloud computing service providers that require users' approval must be reviewed by the IT department before approval.

19.4.1.10. All governmental entities and all organizations, that have any critical infrastructure under their purview that utilize cloud services should have their data classified before being hosted in the cloud. If the data is classified as confidential "restricted" or sensitive "private", then such data must be hosted

in the government cloud. As for the data classified as "public", it can be hosted in the commercial clouds.

19.4.1.11. Data classified as public and/or sensitive may be stored in shared cloud services, and confidential and/or restricted data may not be stored in this type of cloud computing service.

19.4.1.12. The mechanisms of Secure Session Management must be implemented in a manner that ensures the validity and reliability of the session, as well as Lockout and their timeout.

19.4.1.13. Implement the multi-factor authentication mechanisms, especially for accounts classified as sensitive and important.

19.4.1.14. Implement mechanisms to detect and stop unauthorized access attempts, such as setting a maximum number of unsuccessful attempts (three for sensitive accounts) and adding an incremental lockout period after Unsuccessful Login.

19.4.1.15. Employees with authorization to use cloud services are under obligation not to share their login credentials with other co-workers.

19.4.1.16. Use of cloud services must comply with all policies that govern the handling of any data that are owned or being collected by **(Organization)**.

19.4.1.17. Personal cloud service accounts may not be used to store, process or exchange data owned by **(Organization)**.

19.4.1.18. Cloud computing solutions must provide the same or better levels of service in **(Organization)** to ensure business continuity in line with the requirements of the business being provided.

19.4.1.19. Cloud computing services must protect the security and privacy of **(Organization)**'s data, and comply with all appropriate security and privacy requirements.

19.4.1.20. When choosing cloud services, it should be taken into consideration the impact of their use on the stability and performance of the primary operational systems of **(Organization)**.

19.4.1.21. Cloud users must comply with all policies of their **(Organization)** when dealing with data stored in the cloud.

19.4.1.22. Ensure the protection and the integration of all the necessary cyber security mechanisms to secure the network communication channel with the cloud computing service provider.

19.4.1.23. Mobile devices must be inspected to verify that they do not contain any restricted or confidential data and information when they are returned, disposed of, or re-used.

19.4.1.24. Make sure that the service provider guarantees to delete the subscriber's data in a secure manner upon termination of the contract.

19.4.1.25. Adopting secure means and mechanisms when exporting and transferring data from the service provider's cloud computing systems.

19.4.1.26. The proposed cloud service should be checked to ensure it has already been accepted by top management to prevent potential duplication of effort or unnecessary cost.

19.4.1.27. The data used by the **(Organization)**, whether it is static or in motion, must be encrypted within any approved cloud environment.

19.4.1.28. If the data stored with the cloud service provider needs to be encrypted, it must be done using encryption keys that are owned and operated by the **(Organization)**.

19.4.1.29. It is essential to define and evaluate the cloud service provider's head office and data storage and processing location.

19.4.1.30. Mobile apps may be considered cloud services if they "store, process, or transmit the information of the **(Organization)** outside the boundaries of its network."

19.4.1.31. It must be ensured that the Service-level agreement and terms of use are appropriate for the purpose of their use and comply with the information security requirements of **(Organization)**.

19.4.1.32. It must be ensured that the cloud service provider is running an appropriate identity access management system (depending on the nature of work).

19.4.1.33. Business continuity and disaster recovery are to be included in the cloud security laws of the IT department.

19.4.1.34. The IT department/department must determine how cloud security incidents are reported and managed.

19.4.1.35. The IT department are to collaborate with the legal department of **(Organization)**, in order to prepare and implement appropriate Service Level Agreements (SLAs) with cloud service providers to ensure an acceptable performance of cloud service providers.

19.4.1.36. All proposed changes to the cloud security operations must be documented in detail.

19.4.1.37. All cloud security breaches that may affect the IT operations of **(Organization)** must be identified in their respective information security management system and associated plans.

19.4.1.38. The IT management/department must define cloud security processes and procedures; secure and use specialized software and systems to reduce the risk of cloud security breaches, as well as regularly test the security of the perimeter of **(Organization)** and the cloud service provider's perimeter using penetration tests and other forensic methods, and document all procedures and controls for the information cloud.

19.4.1.39. The IT management/department are to establish and document a formal process for identifying a potential breach in the cloud perimeter (e.g. denial-of-service attack, phishing), assessing the breach, determining its nature and potential impact, notifying **(Organization)** management of the breach, and mitigating the impact of the breach as quickly as possible and document the steps taken when dealing with the incident. This process will apply to all cloud environments, whether private, hybrid, and/or public.

19.4.1.40. The IT management/department are to establish and document a formal process for identifying a potential internal breach of cloud security (e.g., information theft, social engineering, unauthorized access to systems), assessing the breach, determining its nature and potential impact, and notifying the **(Organization)**'s management of the breach. Minimizing the impact of the breach as soon as possible, and documenting the steps taken when dealing with the incident.

19.4.1.41. Conduct a vulnerability assessment and repair process for the cloud services subscribed to at least once every six months.

19.4.1.42. Process and deal with the reported vulnerabilities by the service provider.

19.4.1.43. Activate cybersecurity related Event Logs and secure all cloud service-related assets. These assets must be continuously monitored and reviewed regularly.

19.4.1.44. Comply with the policy of dealing with cyber security incidents issued by the NISSA, and obligate service providers to it.

19.4.1.45. Comply with the policies and laws of disaster recovery and business continuity issued by the NISSA, and obligate service providers to them.

19.4.2. Cloud Services Providers

19.4.2.1. Permanent abidance by all laws, regulations, instructions and policies issued by the National Information Security & Safety Authority (NISSA) and all issued legislation related to the country.

19.4.2.2. Cloud service providers must specify to users the services to be offered to subscribers and their cyber security requirements.

19.4.2.3. The importance of isolating the cloud computing services provided to government agencies or those that are classified as institutions that are responsible for vital and sensitive infrastructures from the cloud computing services provided to other organizations.

19.4.2.4. Conduct an inventory of all relevant information and communications technology assets belonging to the service provider, and the owners of these assets must be identified and all such information kept and updated regularly via a database or another appropriate mechanism.

19.4.2.5. Cloud service providers must maintain the confidentiality, integrity and ensure protection of data, including backups and retention periods, and may not process, change, modify or transfer data between their systems.

19.4.2.6. Cloud service providers must inform users in advance and obtain their consent in the event that their content will be transferred, stored or processed.

19.4.2.7. The importance of separating cloud computing networks and isolating them from other internal and external networks of the service provider, and making sure to secure them by the appropriate technical means.

19.4.2.8. (DoS and DDoS) Implementation of protection mechanisms from both types of denial-of-service attacks.

19.4.2.9. The importance of encrypting data as it travels through the service provider's networks, including the data of cloud systems management operations.

19.4.2.10. Implementation of access control mechanisms between the different parts of the network.

19.4.2.11. Establish measures that guarantees there will be no interference with users' data and isolate each one completely from the rest.

19.4.2.12. Commit to follow the principle of the minimum number of jobs required to carry out the work and nothing more.

19.4.2.13. Implementation of safe handling mechanisms as well as checking inputs, exceptions and failures (Input Validation, Exceptions and Failures).

19.4.2.14. The importance of working on separating cyber security mechanisms and techniques and isolating them from the rest of the cloud computing service applications and technologies.

19.4.2.15. Provide cyber security mechanisms that subscribers can benefit from and showcase it to them, and specify a certain level for government subscribers that they are obligated to, provided that the cloud computing service provider obtains certification for these mandatory services from NISSA in particular.

19.4.2.16. Cloud service providers must provide a response plan, disaster recovery plan, business continuity plan, and technical support.

19.4.2.17. Cloud service provider should clarify in advance to their subscribers the geographical location of where their data is being kept.

19.4.2.18. Cloud service providers must give users the right to change service provider and switch to another cloud provider.

19.4.2.19. The mechanisms of secure management of sessions must be implemented, in a manner that includes validation and reliability of the session, closing and ending the deadline set for it.

19.4.2.20. Adopt a multi-factor identity verification mechanism, especially for sensitive and important accounts.

19.4.2.21. Implement mechanisms to detect and stop unauthorized access attempts, such as setting a maximum number of unsuccessful attempts (three for sensitive accounts) and adding an incremental lockout period after each failed attempt.

19.4.2.22. Abstain from saving passwords for accounts of all kinds in the form of unencrypted text, handled instead through encryption techniques and algorithms to guarantee a secure storage of passwords, such as the hashing and salting function.

19.4.2.23. Make sure the identity verification data stays hidden, especially the password, while showing only it to the user to protect it from spying.

19.4.2.24. It is necessary to obtain a clear and documented initial approval from the service subscriber before accessing any of the assets and data of that subscriber.

19.4.2.25. Compile and set up a regularly updated inventory of all mobile devices authorized to operate within the service provider's systems. And work on managing cyber security mechanisms for mobile devices. As well as verify that mobile devices do not contain any restricted or confidential data and information when they are returned, disposed of or re-used.

19.4.2.26. Activate the automatic screen lock feature for mobile devices according to the adopted and approved policies.

19.4.2.27. Work to provide subscribers with secure mechanisms, techniques and procedures for saving and storing data, as well as for the process of deleting and destroying it. And ensure to destroy the data of subscribers whose service contracts have ended in a safe manner.

19.4.2.28. Simplify the process of data transfer for service subscribers and exporting it in a form that enables them to transfer it to another provider and secure this step.

19.4.2.29. Ensure the security of the process of accessing, storing and transferring the contents of the backup copies of the subscriber's data and the media on it.

19.4.2.30. Ensure the security of the process of accessing, storing and transferring the contents of the backup copies of the systems, technologies, management and works of the subscribers' cloud services.

19.4.2.31. Conduct a vulnerability assessment and patching for cloud components at least once every six months.

19.4.2.32. Inform the subscriber of any gaps that he discovers that may affect him and explain how he can address them.

19.4.2.33. Carry out penetration testing of cloud systems and other supporting components at least once a year.

19.4.2.34. Activate and maintain and secure all cloud service-related Event Logs and Audit Trails, especially those related to the subscribers' systems.

19.4.2.35. Activate and maintain and secure all cybersecurity-related Event Logs and Audit Trails, while keeping them under constant monitoring and regular revision using one of the Security Information and Event Management (SIEM) solutions.

19.4.2.36. Abide by the policies and controls for dealing with cyber security incidents issued by NISSA.

19.4.2.37. The obligation to inform subscribers as soon as cyber security incidents occur that may affect them and support them in the process of dealing with them.

19.4.2.38. It is important to set up and save logs of login attempts.

19.4.2.39. Abide by disaster recovery and business continuity policies and controls issued by NISSA.

20. سياسة الوصول للأطراف الثالثة

1.20. مقدمة

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

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 الأطراف الثالثة.

2.20. الغرض

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)**.

3.20. 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.

4.20. السياسة

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

1.1.4.20. لا 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 الآمن إلى مرافق شبكة **(جهة العمل)** من قبل الأطراف الثالثة.

2.1.4.20. تتطلب جميع طلبات الاتصال الجديدة بين الأطراف الثالثة و**(جهة العمل)** موافقة الطرف الثالث وممثل **(جهة العمل)** على الاتفاقية والتوقيع عليها.

2.4.20. **المتطلبات الأولية (قبل الاتفاق):** يجب أن تخضع عملية منح الوصول لمعدات تقنية المعلومات للمراجعة والتصديق من القسم المختص بذلك (قسم أمن المعلومات).

1.2.4.20. تجري المراجعة الأمنية للتأكد من أن أي توصيل يتطابق مع متطلبات العمل بأفضل طريقة ممكنة، وأنه يتبع مبدأ «أقل صلاحيات وصول».

2.2.4.20. 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.

3.2.4.20. 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)**.

3.4.20. إنشاء الاتصال:

1.3.4.20. يجب أن يستند كل اتصال قائم على مبدأ «أقل صلاحيات الوصول» وفقاً لمتطلبات العمل والمراجعة الأمنية المعتمدة.

4.4.20. تعديل أو تغيير الاتصال والوصول:

1.4.4.20. 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)**.

5.4.20. وصول الطرف الثالث المسموح به:

1.5.4.20. 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)**.

2.5.4.20. يجب السماح للطرف الثالث بالوصول فقط إلى المرافق والخدمات والبيانات التي تكون مطلوبة لتنفيذ المهام المحددة في العقد، وعلى النحو الذي تم توضيحه للمسؤولين على هذه المرافق والبيانات ضمن طلب الوصول الأصلي.

6.4.20. الأجهزة والمعدات (محطات العمل) الخاصة بالطرف الثالث:

1.6.4.20. 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.

7.4.20. وصول الأطراف الثالثة عن بعد:

1.7.4.20. 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.

2.7.4.20. 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.

8.4.20. **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)**.

9.4.20. **إنهاء الوصول:**

1.9.4.20. عندما انتهاء الحاجة إلى الوصول يجب أن يقوم المسؤول عن الاتصال داخل **(جهة العمل)** بإنهاء الوصول.

2.9.4.20. يجب أن يقوم المسؤولون عن كل اتصال بمراجعة هذه الاتصالات سنوياً للتحقق من وجود حاجة لاستمرارها، وأن نوع الوصول الحالي يلبي متطلبات الاتصال المرجوة.

3.9.4.20. يتم على الفور إنهاء جميع الاتصالات التي لم يعد لها فائدة أو حاجة في تنفيذ أعمال **(جهة العمل)**.

4.9.4.20. في حالة تم تعريفهم داخل نظام **(جهة العمل)**، يجب أن يكون لدى جميع الأطراف الثالثة والمستخدمين الخارجيين تاريخ صلاحية لحساباتهم.

21. القواعد الإرشادية لاتفاقية عدم الإفصاح

1.21. مقدمة

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

2.21. الغرض

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

3.21. النطاق

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

4.21. القواعد الإرشادية

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

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

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

4.4.21. 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.

5.4.21. يجب أن تحتوي اتفاقية عدم الإفصاح على الأقل على الآتي؛

1.5.4.21. أسماء الأطراف المتعاقدة.

2.5.4.21. 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.

21.5.4.3. تحديد ماهي المعلومات السرية في الاتفاقية.

21.5.4.4. مدة الالتزام بالاتفاقية بالسنوات.

21.5.4.5. مدة وشروط الحفاظ على سرية المعلومات بالسنوات.

21.5.4.6. المعلومات التي سيتم استبعادها من الاتفاقية، كالمعلومات التي تم معرفتها مسبقاً أو التي تتواجد ومتاحة للعموم، أو التي يُطّلع عليها لاحقاً من أطراف أخرى.

21.5.4.7. الشروط والقيود المتعلقة بطرق نقل المعلومات السرية.

21.5.4.8. الإجراءات التي ينبغي اتخاذها على المعلومات السرية عند نهاية الاتفاقية.

21.5.4.9. مسؤوليات استلام والتعامل مع المعلومات السرية:

- استخدام المعلومات للأغراض المتفق عليها فقط.
- الكشف عنها فقط للأشخاص الذين يحتاجون إلى معرفة المعلومات لأداء الأغراض 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 الأشخاص الذين تم الكشف لهم عن المعلومات يلتزمون بشروط تقييد الاستخدام وتقييد الإفصاح، وضمان حماية المعلومات.

21.5.4.10. نوع الإفصاح المسموح به – المعلومات اللازمة للوصول للهدف المطلوب في إطار القانون.

21.5.4.11. يجب أن يختار الطرفان القانون والقضاء المختص الذي يحكم تنفيذ الاتفاقية.

20. Third Party Access Policy

20.1. Introduction

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

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

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)

20.2. 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.

20.3. 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.

20.4. Policy

20.4.1. **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.

20.4.1.1. 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.

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

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

20.4.2.1. 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.

20.4.2.2. 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.

20.4.2.3. 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)**.

20.4.3. **Establishing Connectivity:**

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

20.4.4. **Modifying or Changing Connectivity and Access:**

20.4.4.1. 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.

20.4.5. **Permitted Third Party Access:**

20.4.5.1. 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.

20.4.5.2. 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.

20.4.6. **Third Party Workstations:**

20.4.6.1. 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.

20.4.7. **Remote Access by Third Parties:**

20.4.7.1. 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.

20.4.7.2. 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.

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

20.4.9. **Terminating Access:**

20.4.9.1. When access is no longer required, the responsible of access and connection in **(Organization)** must terminate the access.

20.4.9.2. 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.

20.4.9.3. Connections that are found to be depreciated, and/or are no longer being used to conduct **(Organization)** business, must be terminated immediately.

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

21. Non-disclosure / Confidentiality Agreement Guideline

21.1. 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.

21.2. 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.

21.3. Scope

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

21.4. Statement of Guidelines

21.4.1. 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 the agreement.

21.4.2. 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.

21.4.3. **(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.

21.4.4. 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.

21.4.5. The agreement should at least address the following;

21.4.5.1. The names of the contracting parties.

21.4.5.2. 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.

21.4.5.3. Defining what is to be confidential.

21.4.5.4. The term (in years) the agreement is binding.

21.4.5.5. The term and conditions (in years) of the confidentiality, i.e. the time period of confidentiality.

21.4.5.6. 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.

21.4.5.7. Restrictions regarding the transfer of confidential information.

21.4.5.8. Required actions that should be taken with the confidential information upon NDA's ending.

21.4.5.9. 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.

21.4.5.10. Types of allowed disclosure – such as those required by law or court order.

21.4.5.11. The parties should choose the law and jurisdiction that is governing their agreement.

22. سياسة الوصول عن بعد

1.22. مقدمة

يعد الوصول عن بُعد إلى شبكة **(جهة العمل)** ضروريًا للحفاظ على إنتاجيتها وسير الأعمال بها وذلك للموظفين الذين يؤدون أعمالهم من موقع بعيد عن **(جهة العمل)** مثل المنزل أو عند السفر أو في حالة عدم إمكانية تواجد الموظفين بها، ولكن في كثير من الحالات ينشأ هذا الوصول من شبكات في وضع أمني أقل بكثير من ذلك الموجود في شبكة **(جهة العمل)** أو قد تكون مخترقة بالفعل. يعد الوصول عن بعد بطبيعته مخاطرة أمنية حتى مع اتخاذ التدابير اللازمة لتأمين هذا النوع من الاتصال، وبالتالي فإن السياسات والمعايير والإجراءات مطلوبة لتقليل هذا الخطر.

2.22. الغرض

تهدف هذه السياسة إلى تحديد قواعد ومتطلبات الاتصال بشبكة **(جهة العمل)** من أي أجهزة خارجية عبر تقنية الوصول عن بُعد، وذلك لتقليل التعرض المحتمل لـ **(جهة العمل)** للأضرار التي قد تنجم عن الاستخدام غير المصرح به لمصادرها. حيث تشمل الأضرار فقدان البيانات الحساسة أو السرية، الملكية الفكرية، تلف الصورة العامة، وتلف الأنظمة الداخلية لـ **(جهة العمل)** الحرجة، وتتبعها المتطلبات المالية المتكبدة نتيجة لهذه الخسائر.

3.22. النطاق

تنطبق هذه السياسة على جميع الموظفين والشركاء في **(جهة العمل)** داخلها أو خارجها، بما في ذلك الموظفين التابعين للأطراف الثالثة والذين يستخدمون أجهزة **(جهة العمل)** أو أجهزتهم الشخصية للوصول إلى شبكة **(جهة العمل)** عن بُعد، كما تنطبق على اتصالات الوصول عن بعد المستخدمة للقيام بالعمل نيابة عن **(جهة العمل)**، بما في ذلك قراءة البريد الإلكتروني أو إرساله وعرض موارد الويب على الإنترنت. تنطبق هذه السياسة على جميع المعدات المملوكة أو المؤجرة أو المشغلة من قبل **(جهة العمل)**.

4.22. السياسة والمتطلبات

1.4.22. **السياسة:**

1.1.4.22. أثناء الاتصال بموارد الحوسبة لـ **(جهة العمل)**، يجب على مستخدمي الوصول عن بُعد اتباع سياسات **(جهة العمل)** في جميع الأوقات، بما في ذلك سياسة الاستخدام المقبول.

2.1.4.22. يجب على جميع الموظفين الذين يحتاجون إلى الوصول عن بُعد لأغراض العمل الخضوع لعملية تقديم طلب توضح سبب الحاجة إلى الوصول ومستوى الخدمة الذي يحتاجه الموظف. في حالة قبول طلبه، يجب الموافقة على اتفاقية الوصول عن بعد والتوقيع عليها من قبل المشرف أو رئيس قسم الموظف قبل تقديمها إلى

إدارة / قسم تكنولوجيا المعلومات، والتي بدورها ستقوم بتقديم الطلب إلى الإدارة العليا للموافقة النهائية.

22.1.4.3. يجب أن تحتوي جميع الأجهزة المستخدمة للوصول عن بعد على وسائل الحماية لتوفير الحماية الأمنية المناسبة. تشمل هذه الوسائل على سبيل المثال لا الحصر، استخدام أحدث برامج أمان الإنترنت (بما في ذلك برامج مكافحة الفيروسات وجدران الحماية/الناري وما إلى ذلك)، ويجب تطبيق أحدث تصحيحات أمان نظام التشغيل وتثبيت جدار حماية شخصي حيثما كان متاحًا.

22.1.4.4. تقع المسؤولية على المستخدمين المعتمدين/المصرح لهم (الموظفين والمتعاقدين والأطراف الثالثة الذين يتمتعون بامتيازات الوصول عن بُعد لشبكة جهة العمل) لـ**(جهة العمل)** ضمان إعطاء اتصال الوصول عن بُعد نفس الاعتبار والاحتياطات الذي يحظى به الاتصال الرئيسي في موقع **(جهة العمل)**.

22.1.4.5. سلوك المستخدم المقبول: يقتصر الوصول العام إلى الإنترنت من خلال شبكة **(جهة العمل)** على المستخدمين المصرح لهم. عند الوصول إلى شبكة **(جهة العمل)** من جهاز كمبيوتر شخصي، يكون المستخدمون المصرح لهم مسؤولين عن منع الوصول إلى موارد أو بيانات **(جهة العمل)** من قبل المستخدمين غير المخولين. يحظر أداء أي أنشطة غير قانونية من خلال شبكة **(جهة العمل)** من قبل أي مستخدم (مرخص أو غير ذلك). يتحمل المستخدم المصرح له مسؤولية ونتائج سوء استخدام وصول المستخدم المصرح له.

22.1.4.6. لا يجب أن يستخدم المصرح لهم بالوصول شبكات **(جهة العمل)** للوصول إلى الإنترنت لمصالح تجارية خارجية. يجب على المستخدمين المصرح لهم مراجعة السياسات التالية للحصول على تفاصيل حول حماية المعلومات عند الوصول إلى شبكة **(جهة العمل)** عبر طرق الوصول عن بعد والاستخدام المقبول لها:

- سياسة الاستخدام المقبول
- سياسة الشبكة الخاصة الافتراضية (VPN)
- سياسة الاتصالات اللاسلكية
- سياسة التشفير المقبولة

22.1.4.7. يجب إدارة جميع عمليات الوصول عن بُعد مركزيًا بواسطة مركز بيانات النظام (SDC) وستستخدم إجراءات الأمان المناسبة بناءً على متطلبات الوصول.

22.1.4.8. جلسات الوصول عن بعد للأطراف الثالثة: يجب العلم والإبلاغ بجميع جلسات الوصول الخاصة للأطراف الثالثة والالتزام بإجراءات تغيير الإدارة المناسبة «في حالة تغيير المستخدمين المصرح لهم بالوصول».

22.1.4.9. يوافق مستخدم الوصول عن بعد على إبلاغ المسؤولين على الفور بأي حادث أو

حوادث يشتبه بها في عملية وصول غير مصرح به و/أو الإفصاح عن موارد أو معلومات **(جهة العمل)**.

10.1.4.22. يخضع أي جهاز متصل بموارد الحوسبة لـ**(جهة العمل)** للمراقبة، والتي قد تشمل على مراقبة التاريخ والوقت ومدة الاتصال وتحديد نقطة النهاية وجميع حركة البيانات التي تمر عبر شبكة **(جهة العمل)**. لا يتم رصد الملفات الشخصية على المعدات التي لا تتبع **(جهة العمل)**.

2.4.22. **المتطلبات:**

1.2.4.22. يجب التحكم في الوصول الآمن عن بُعد بشكل صارم باستخدام التشفير (الشبكات الافتراضية الخاصة (VPNs)) وكلمات المرور القوية. سيتم فرض التحكم عبر مصادقة كلمة المرور لمرة واحدة أو المفاتيح العامة/الخاصة باستخدام عبارات مرور قوية.

2.2.4.22. يجب على المستخدمين المرخص لهم حماية معلومات تسجيل الدخول وكلمة المرور الخاصة بهم ولا يجب كشفها على اي أحد، وحتى على أفراد العائلة.

3.2.4.22. أثناء استخدام جهاز كمبيوتر مملوك لـ**(جهة العمل)** للاتصال بشبكة **(جهة العمل)** عن بُعد، يجب على المستخدمين المرخص لهم التأكد من أن المضيف المتصل عن بعد غير متصل بأي شبكة أخرى في نفس الوقت، باستثناء الشبكات الشخصية التي تقع تحت التحكم بالكامل لهم.

4.2.4.22. يجب أن تتم الموافقة مسبقاً على استخدام الموارد الخارجية لسير الأعمال بـ **(جهة العمل)** من قبل قسم أمن المعلومات والرئيس المباشر للمستخدم.

5.2.4.22. يجب على جميع المضيفين المرتبطين بالشبكات الداخلية **(جهة العمل)** عبر تقنيات الوصول عن بُعد استخدام أحدث برامج مكافحة الفيروسات، وهذا يشمل أجهزة الكمبيوتر الشخصية للمستخدمين. كما يجب أن تمتثل اتصالات الطرف الثالث للمتطلبات كما هو منصوص عليه في اتفاقية الطرف الثالث.

6.2.4.22. يجب أن تفي المعدات الشخصية المستخدمة للاتصال بشبكات **(جهة العمل)** بمتطلبات المعدات المملوكة لـ**(جهة العمل)** للوصول عن بُعد كما هو مذكور في معايير تكوين الأجهزة والبرامج للوصول البعيد إلى شبكة **(جهة العمل)**.

22. Remote Access Policy

22.1. Overview

Remote access to **(Organization)**'s network is essential to maintain its productivity for those employees who perform business from a remote location, such as home or when traveling, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than **(Organization)**'s network. While measures have been taken to secure this type of connection, remote access is inherently a security risk. Consequently, policy, standards and procedures are required to minimize this risk.

22.2. Purpose

This policy aims to define rules and requirements for connecting to **(Organization)**'s network from any external devices via remote access technology, and that is to minimize the potential exposure to **(Organization)** from damages which may result from unauthorized use of **(Organization)** resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical **(Organization)** internal systems, and financial liabilities incurred as a result of those losses.

22.3. Scope

This policy applies to all **(Organization)** employees, contractors, and other personnel in or out of **(Organization)**, including employees of affiliated third-party organization, who utilize **(Organization)** or personally-owned devices to remotely access the **(Organization)** network, and to remote access connections used to do work on behalf of **(Organization)**, including reading or sending email and viewing intranet web resources. This policy applies to all equipment that is owned, leased, operated, or maintained by **(Organization)**.

22.4. Policy and Requirements

22.4.1. **Policy:**

22.4.1.1. While connected to **(Organization)** computing resources, remote access users are required to follow **(Organization)** policies at all times, including the Acceptable Use Policy.

22.4.1.2. All employees requiring remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. The Remote Access Agreement must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the local IT department. The IT department will submit the application to the higher management for final review and approval.

22.4.1.3. All devises that used to remote access must have appropriate security protections enabled. These protections include but are not limited to, the use of up-to-date Internet security software (this includes Anti-Virus, Firewalls etc.), and all the most recent appropriate operating system security patches applied and a personal firewall installed where available.

22.4.1.4. It is the responsibility of **(Organization)** Authorized Users (employees, contractors, and third-parties with remote access privileges to **(Organization)**'s network) to ensure that their remote access connection is given the same consideration as the user's on-site connection to **(Organization)**.

22.4.1.5. Acceptable User Behavior: General access to the Internet use through the **(Organization)** network is strictly limited to **(Organization)** Authorized Users. When accessing the **(Organization)** network from a personal computer, Authorized Users are responsible for preventing access to any **(Organization)** computer resources or data by non-Authorized Users. Performance of illegal activities through the **(Organization)** network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

22.4.1.6. Authorized Users will not use **(Organization)** networks to access the Internet for outside business interests. Authorized Users must review the following policies for details of protecting information when accessing the **(Organization)** network via remote access methods, and acceptable use of **(Organization)**'s network:

- Acceptable Use Policy
- Virtual Private Network (VPN) Policy
- Wireless Communications Policy
- Acceptable Encryption Policy

22.4.1.7. All remote access must be centrally managed by System Data Center (SDC) and will use appropriate security measures based on access requirements.

22.4.1.8. Third Party Access Sessions: All third-party access sessions must be notified and the appropriate change management procedures must be adhered to.

22.4.1.9. Remote access user agrees to immediately report to (who is in charge) any incident or suspected incidents of unauthorized access and/or disclosure of **(Organization)** resources or information.

22.4.1.10. Any device connecting to **(Organization)** computing resources is subject to monitoring, which may include but is not limited to date, time, duration of access, identification of endpoint and all traffic which traverses **(Organization)** networks. Personal files on non-**(Organization)** equipment will not be monitored.

22.4.2. **Requirements:**

22.4.2.1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

22.4.2.2. Authorized Users must protect their login information and password from everyone, even from family members.

22.4.2.3. While using an **(Organization)**-owned computer to remotely connect to **(Organization)** 's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

22.4.2.4. Use of external resources to conduct **(Organization)** business must be approved in advance by information security department and the appropriate business unit manager.

22.4.2.5. All hosts that are connected to **(Organization)** internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.

22.4.2.6. Personal equipment used to connect to **(Organization)** 's networks must meet the requirements of **(Organization)** -owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to **(Organization)** Network.

23. سياسة الأمان المادي

1.23. 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.

2.23. 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.

3.23. 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.

4.23. السياسة

1.4.23. بند العقار:

1.1.4.23. 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 والأمطار الغزيرة والعواصف الرملية والفيضانات.

2.1.4.23. 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.

3.1.4.23. 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.

4.1.4.23. 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.

5.1.4.23. 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 مضائه بشكل جيد، ويجب ألا يكون هناك أي لوحات أو علامات إرشادية تبين أن المكان يخص مركز البيانات أو هوية **(جهة العمل)** المالكة.

1.5.1.4.23. 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.

2.5.1.4.23. 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.

3.5.1.4.23. 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.

6.1.4.23. غرف الخوادم:

1.6.1.4.23. 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.

2.6.1.4.23. البنية التحتية

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

3.6.1.4.23. 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).

4.6.1.4.23. 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.

23.1.4.7. المرافق:

23.1.7.1.4. أنظمة التبريد

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

23.1.7.2.4. 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.

23.1.7.3.4. 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.

23.1.7.4.4. 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.

23.1.4.8. التعافي من الكوارث:

23.1.8.1.4. 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.

2.8.1.4.23. 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 تدريبات اختبار جاهزية خطوات النسخ الاحتياطي.

2.4.23. بند ما يخص البشر:

1.2.4.23. الغير عاملين بمركز البيانات

1.1.2.4.23. الحراس

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

2.1.2.4.23. 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).

3.1.2.4.23. 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.

4.1.2.4.23. 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 إفصاح قبل دخول غرف الخوادم.

2.2.4.23. المستخدمين

1.2.2.4.23. 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.

2.2.2.4.23. السياسة

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

3.2.4.23. التعافي من الكوارث

1.3.2.4.23. 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.

2.3.2.4.23. 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.

3.3.2.4.23. 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 ظرف طارئ لأحد الموظفين مما يسهل عملية إحلال موظف مكان الأخر.

4.3.2.4.23. معلومات التواصل

يجب حفظ وتحديث بيانات التواصل الخاصة بكل موظفي مركز البيانات

5.3.2.4.23. 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.

23. Physical Security Policy

23.1. 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.

23.2. 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.

23.3. 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.

23.4. Policy

23.4.1. **Property Section:**

23.4.1.1. 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.

23.4.1.2. 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.

23.4.1.3. 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) pref-

erably 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.

23.4.1.4. 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.

23.4.1.4.1. 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.

23.4.1.4.2. 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.

23.4.1.4.3. 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.

23.4.1.4.4. 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.

23.4.1.5. Server Rooms

23.4.1.5.1. 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.

23.4.1.5.2. 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.

23.4.1.5.3. 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.

23.4.1.5.4. 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.

23.4.1.6. Facilities

23.4.1.6.1. 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.

23.4.1.6.2. 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.

23.4.1.6.3. 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.

23.4.1.6.4. 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.

23.4.1.7. Disaster Recovery

23.4.1.7.1. 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 back-up 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?

23.4.1.7.2. 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.

23.4.2. People Section:

23.4.2.1. Outsiders

23.4.2.1.1. 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.

23.4.2.1.2. 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.

23.4.2.1.3. 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.

23.4.2.1.4. 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.

23.4.2.2. Users

23.4.2.2.1. 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.

23.4.2.2.2. 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.

23.4.2.3. Disaster Recovery

23.4.2.3.1. 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.

23.4.2.3.2. 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.

23.4.2.3.3. 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.

23.4.2.3.4. Contact Information

A contact database must be maintained with contact information for all Data Center employees.

23.4.2.3.5. 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.

23.4.2.3.6. 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.

24. سياسة التعامل مع الحوادث

1.24. مقدمة

أصبحت المؤسسات والأفراد عرضة بشكل متزايد لهجمات الأمن السيبراني تزامناً مع تزايد تواجدها على الإنترنت تفضل معظم المؤسسات تجنب وتخفيف الأضرار الناجمة عن مثل هذه الهجمات من خلال وضع وتنفيذ سياسات وخطط أمن المعلومات.

سياسة التعامل مع الحوادث تتعامل مع آثار الحادث الأمني، بحيث تحدد من وأين وكيف يجب أن تستجيب للحادث. قد يتم تأخير الاستجابة للحادث في حالة عدم وجود هذه السياسة لدى المؤسسات، كذلك يمكن ضياع الأدلة التي تشير إلى سبب الحادث نهائيًا مما يؤدي الى تفاقم أثار الحادث ومنع المؤسسة من معالجة الحوادث المماثلة في المستقبل، كما تتطلب صياغة سياسة فعالة للاستجابة للحوادث الكثير من التخطيط والموارد.

2.24. الغرض

تحدد هذه الوثيقة السياسة الخاصة بمعالجة الحوادث الأمنية المتعلقة بأنظمة وعمليات **(جهة العمل)** من خلال الاستجابة المناسبة للحوادث. بالإضافة إلى ذلك فانها تهدف الى إنشاء مجموعة من المعايير التي يجب اتباعها عند وقوع حادثة أمن سيبراني.

3.24. النطاق

تنطبق هذه السياسة على جميع الموظفين والمتعاقدين والمستشارين والعاملين المؤقتين والشركاء والأطراف الثالثة لـ **(جهة العمل)**.

4.24. السياسة

1.4.24. تنظيم الاستجابة للحوادث:

1.1.4.24. خطة التعامل مع الحوادث: يجب أن تتضمن هذه الخطة الأدوار والمسؤوليات واستراتيجيات الاتصال في حالة حدوث أي حادث بما في ذلك إخطار الشركاء الخارجيين المعنيين.

2.1.4.24. فريق الاستجابة لحالات طوارئ أمن الكمبيوتر: يجب أن تقوم إدارة/ قسم تقنية المعلومات بتنظيم فريق الاستجابة لطوارئ أمن الكمبيوتر (CSIRT) أو أي فريق استجابة للحوادث مكافئ له وبنفس الأدوار ولمسؤوليات.

2.4.24. الأدوار والمسؤوليات:

1.2.4.24. توافرية الاستجابة للحوادث: يجب أن يكون فريق الاستجابة لحالات طوارئ أمن الكمبيوتر الخاص بـ **(جهة العمل)** متاحًا في جميع الأوقات للرد على التنبيهات التي تشمل على سبيل المثال لا الحصر، أدلة على نشاط غير مصرح به والكشف عن نقاط الوصول اللاسلكي غير المصرح بها وتنبيهات IDS الهامة، والتقارير تغييرات للأنظمة الحرجة الغير

مصرح بها او تغييرات على محتوى الملف.

.2.2.4.24 الشخص المحدد للاتصال لجميع الكوارث والأحداث الأمنية: يجب أن يكون لدى **(جهة العمل)** متحدث رسمي باسمها لا يجوز لأي موظف التحدث مع الصحافة أو أي أطراف خارجية أخرى حول الوضع الحالي لكارثة أو حالة طوارئ أو حدث أمني قد شُهد مؤخراً.

.3.2.4.24 مسؤوليات إدارة الحوادث: يجب تحديد الأفراد المسؤولين عن التعامل مع حوادث أمن أنظمة المعلومات بوضوح من قبل أكبر مسؤول أمن المعلومات، و يجب منح هؤلاء الأفراد صلاحيات تحديد الإجراءات والمنهجيات التي سيتم استخدامها للتعامل مع حوادث أمنية محددة.

.4.2.4.24 توفير المعلومات في الإجراءات القانونية: يُحظر على الموظفين تقديم أي سجلات خاصة بـ **(جهة العمل)** أو أي نسخ منها إلى جهات خارج **(جهة العمل)** أو إلى المسؤولين الحكوميين، سواء كان ذلك رداً على أمر استدعاء أو غير ذلك، ما لم يكن هنالك إذن مسبق تم الحصول عليه من كبير المستشارين القانونيين أولاً.

.5.2.4.24 خطة إدارة الأزمات: يجب إعداد خطة إدارة الأزمات وتحديثها سنويًا، حيث تغطي هذه الخطة موضوعات مثل عملية إدارة الأزمة واستمرارية اتخاذ القرارات المتعلقة بالأزمات وسلامة الموظفين ومراقبة الأضرار والاتصالات مع جهات خارجية مثل وسائل الإعلام.

.3.4.24 تحضير فريق الاستجابة لحوادث طوارئ أمن الكمبيوتر (CSIRT):

.1.3.4.24 يجب الحصول على جميع الأجهزة والبرامج اللازمة للتحقيق في الحادث والاحتفاظ بها في مكان آمن.

.2.3.4.24 يجب الحفاظ على سلسلة النماذج ونماذج التقارير التي سيتم استخدامها لتوثيق الحوادث والإجراءات المستخدمة للتحقيق في الحادث والنتائج التابعة له.

.3.3.4.24 تحديد مجموعة من الموظفين للعمل في (CSIRT). يجب أن يحتوي الفريق على خبراء من جميع المجالات التقنية في **(جهة العمل)** على سبيل المثال (الشبكات، الاتصالات السلكية واللاسلكية، الدعم الفني، إدارة الخادم ،إلخ)، وبذلك سيكون الفريق مستعد للتعامل مع أي حادث أمني، بحيث يستجيب الأعضاء للحوادث التي تتعلق بمجالهم فقط. كما يجب تعيين عضو واحد من (CSIRT) ليكون المحقق الرئيسي ويكون مسؤولاً عن تنظيم وإدارة (CSIRT) عند وقوع حادث ما. كما يجب أن يتلقى جميع أعضاء (CSIRT) تدريبًا دوريًا على كيفية الاستجابة الصحيحة والمناسبة لأي حادث.

.4.4.24 التقارير:

.1.4.4.24 يجب أن تصف تقارير الحوادث تفاصيل الحدث بدقة ويجب كتابتها بلغة مفهومة للقُراء دون خلفية تقنية.

.2.4.4.24 يجب الإبلاغ عن حوادث الأمن السيبراني و / أو الأحداث الأمنية فور اكتشافها من خلال

طرق الإدارة المناسبة في أسرع وقت ممكن و المتمثلة في:

- المكالمات الهاتفية
- البريد الصوتي
- البريد الإلكتروني
- نموذج الموقع
- نظام التذاكر (Ticketing System)

24.4.4.3. الموظفون والمتعاقدون الذين يستخدمون أنظمة وخدمات معلومات **(جهة العمل)** مسؤولون عن ملاحظة أو الإبلاغ عن أي ضعف أو حادثة أمنية ملحوظة أو مشتبه بها في الأنظمة أو الخدمات أو أي انتهاكات للسياسة باستخدام إجراءات الإبلاغ المناسبة. وسيؤدي عدم الإبلاغ عن حادث إلى اتخاذ إجراء تأديبي ضد أي مستخدم اكتشف أو شهد على الحادث.

24.4.4.4. يجب الإبلاغ عن الحوادث الداخلية عن طريق الاتصال بمكتب الدعم الفني أو المسؤول الأعلى لأمن المعلومات (CISO). بالنسبة لجميع الحوادث التي يتم إبلاغ مكتب الدعم الفني بها يتعين على المسؤول الذي يتلقى المكالمة جمع معلومات حول طبيعة الحادث كما هو مفصل في نموذج الإبلاغ عن الحادث وإخطار (CISO) على الفور بالحادث، كما يجب عليه ألا يناقش الحادث مع أي شخص آخر ما لم يصدر أمر بذلك من (CISO).

24.4.4.5. يجب أخذ تقارير الحوادث المبلغ عنها من مصادر خارج **(جهة العمل)** على محمل الجد والتحقيق فيها للتأكد من صحتها. يتم التعامل مع نتائج التحقيق باستخدام السياسات المعمول بها.

24.4.4.6. فقدان أو الكشف عن المعلومات السرية و/أو الحساسة: في حالة فقدان المعلومات السرية و/أو الحساسة، أو الكشف عنها لأطراف غير مصرح لهم بمعرفتها، أو الاشتباه في ضياعها، يجب إخطار مالكها وإدارة / قسم أمن المعلومات [أو قسم مكافئ له] على الفور.

24.4.4.7. التضارب في الإبلاغ عن الانتهاك والمشكلات: أي محاولة للتدخل في أو منع أو إعاقة أو إثناء أحد الموظفين عن جهودهم للإبلاغ عن مشكلة أو انتهاك في أمن المعلومات محظورة تمامًا، وتتسبب في اتخاذ إجراءات تأديبية.

24.4.4.8. الإبلاغ عن نشاط غير مصرح به: يجب على مستخدمي نظم المعلومات داخل **(جهة العمل)** إبلاغ أكبر مسؤول أمن المعلومات على الفور بأي فقد أو تغيير غير مصرح به في البيانات، كما يجب الإبلاغ عن أي استخدام مشكوك فيه للملفات أو قواعد البيانات أو شبكات الاتصالات على الفور إلى نفس المسؤول.

24.4.4.9. الإبلاغ عن نقاط الضعف (الثغرات) في النظام: يجب على المستخدمين الإبلاغ على

الفور عن جميع تنبيهات أمان المعلومات والتحذيرات ونقاط الضعف المشتبه بها وما شابه ذلك إلى مكتب الدعم الفني. يُحظر على المستخدمين استخدام أنظمة **(جهة العمل)** لإعادة توجيه هذه المعلومات إلى مستخدمين آخرين، سواء كان المستخدمون الآخرون داخليين أو خارجيين.

10.4.4.24. مناقشة نقاط الضعف والثغرات الأمنية: يجب على الموظفين الذين يكتشفون وجود ثغرة أمنية أو ضعف في تدابير أمن المعلومات التي تستخدمها **(جهة العمل)** ألا يناقشوا هذه الأمور مع أي شخص آخر غير أكبر مسؤول أمن المعلومات أو مسؤول التدقيق الداخلي أو المحققين المعينين بواسطة أحد هذين المسؤولين.

11.4.4.24. الإبلاغ عن نقاط الضعف الأمنية: عند اكتشاف ثغرة أمنية جديدة وخطيرة في أمن نظم المعلومات مرتبطة بأجهزة أو برامج خاصة بمورد معين، يجب الإبلاغ عنها على الفور في الوسائل المناسبة للنشر العام.

12.4.4.24. الجدول الزمني للاستجابات للمشاكل الأمنية المبلغ عنها: يجب أن تعترف **(جهة العمل)** باستلام جميع نقاط الضعف المبلغ عنها لمنتجاتها أو خدماتها في غضون سبعة أيام، كما يجب أن تقدم رداً مفصلاً على الطرف المبلغ في غضون عشرة أيام من وقت استلام التقرير. و يجب أن تسعى أيضًا إلى الاتصال بالجهة المبلغة كل سبعة أيام أثناء تطوير عملية التصحيح أو الإصلاح كما يجب أن تسعى إلى حل مشكلة الثغرة او نقطة الضعف خلال ثلاثين يومًا، أو في أقرب وقت ممكن عمليًا.

13.4.4.24. يجب توثيق جميع خطوات التحقيق والاستنتاجات فور حدوثها.

14.4.4.24. يجب كتابة جميع التقارير باستخدام النموذج المخصص لنوع الحادث بإيجاز و وضوح.

15.4.4.24. يتم مراجعة جميع تقارير الحوادث من قبل (CISO)، ومن قبل مسؤول الحوادث.

16.4.4.24. يجب الاحتفاظ بجميع التقارير والأدلة المتعلقة بحادث لمدة لا تقل عن 10 سنوات.

5.4.24. الاستجابة الأولية:

قبل البدء في التحقيق، يحتاج (CSIRT) إلى التحقق من وقوع الحادث بالفعل. يجب أن يتخذ (CSIRT) الإجراءات التالية لتزويدهم بالمعلومات الكافية لاتخاذ هذا القرار:

1.5.4.24. مراجعة نموذج الإبلاغ عن الحوادث المملوءة من قبل أحد تقني مكتب الدعم الفني أو (CISO). يجب الاتصال بالمبلغ عن الحادث، إذا كانت هناك حاجة لمزيد من المعلومات أو التوضيح.

2.5.4.24. مراجعة سجلات النظام ذات الصلة لتحديد البيانات التي من شأنها أن تدعم وقوع الحادث فعلاً. والتحقيق مع موظفي **(جهة العمل)** -غير المتخصصين في تكنولوجيا المعلومات- الذين قد يكونوا قادرين على توفير وصف للحدث. يجب الأخذ في الاعتبار أنه قد لا تكون جميع الخطوات مطلوبة لأنواع معينة من الحوادث. يجب دائمًا الحذر

عند الحصول على سجلات النظام واستجواب الموظفين الذين ليسوا على علم بالحادث. في نهاية هذه المرحلة يجب على (CSIRT) معرفة ما إذا كان قد وقع حادث أم لا، وإذا كان الأمر كذلك فما هو نوع الحادث الذي وقع والأنظمة التي تتأثر به، والتأثير المحتمل على **(جهة العمل)**. حيث لا يجب استكمال التحقيق حتى يتم الرد على جميع الأسئلة السابقة من قبل (CSIRT).

24.4.6. مراقبة الأحداث الأمنية:

24.4.6.1. يجب تقييم الأحداث الأمنية ويجب تحديد ما إذا كانت ستصنف على أنها حوادث أمنية.

24.4.6.2. تنبيهات الحوادث – IDS: يجب أن تتضمن خطة الاستجابة للحوادث الإجراءات المطلوبة للتنبيهات من نظام كشف التسلل والاختراق.

24.4.6.3. تنبيهات الحوادث – IPS: يجب أن تتضمن خطة الاستجابة للحوادث الإجراءات المطلوبة للتنبيهات من نظام منع التسلل والاختراق.

24.4.6.4. تنبيهات الحوادث - أنظمة مراقبة سلامة الملفات : يجب أن تتضمن خطة الاستجابة للحوادث الإجراءات المطلوبة للتنبيهات من جميع أنظمة مراقبة سلامة الملفات.

24.4.7. إدارة خرق البيانات:

24.4.7.1. خطة استجابة خرق البيانات: يجب على إدارة **(جهة العمل)** إعداد واختبار وتحديث خطة استجابة خرق البيانات سنوياً، والتي تتناول سياسات وإجراءات الاستجابة في حالة حدوث خرق للبيانات السرية و/أو الحساسة.

24.4.8. جمع الأدلة:

24.4.8.1. مصادر الأدلة الرقمية: يجب على إدارة/ قسم أمن المعلومات تحديد مصادر الأدلة الرقمية لكل نظام كمبيوتر، والتي يمكن استخدامها في قضية ما أمام المحكمة. بعد ذلك يجب أن تخضع هذه المصادر لعملية تتبع معايير موحدة في الجمع والحفظ والإتلاف مماثلة لتلك المستخدمة للسجلات الحيوية والحساسة.

24.4.8.2. الشخص المسؤول عن إنتاج الأدلة الإلكترونية: تقوم **(جهة العمل)** بتعيين فرد واحد مسؤول عن تنسيق اكتشاف وتقديم الأدلة الإلكترونية التي قد تكون مطلوبة في قضية أمام المحكمة.

24.4.8.3. تصنيف البيانات الخاصة بالأدلة الإلكترونية المحتملة: يجب أن تنضوي بيانات **(جهة العمل)** التي قد تعتبر أدلة إلكترونية تحت تصنيف بيانات محدد.

24.4.8.4. يجب جمع البيانات الإلكترونية بطريقة جنائية رقمية سليمة. كلما أمكن يجب استخدام مجموعة أدوات جنائية رقمية مثل EnCase أو FTK. أما الأدلة التي لم تجمع باستخدام هذه الأدوات، فيجب على المحقق أو (المحققين) تدوين ملاحظات مفصلة عن كيفية جمعهم لهذه البيانات.

5.8.4.24. تؤخذ ملخصات Md5 لجميع البيانات التي تم جمعها مباشرة بعد الحصول على الأدلة.

6.8.4.24. يجب نسخ جميع الأدلة الإلكترونية إلى وحدة تخزين قابلة للإزالة ووضعها في خزنة أدلة مقفلة و آمنة بحيث لا يمكن إلا لـ (CISO)والعضو الرئيسي في (CSIRT) الوصول إليها. يجب أن يكون لكل دليل علامة دالة مرفقة.

7.8.4.24. بالنسبة للحوادث التي تتطلب أدلة غير إلكترونية (على سبيل المثال ، ملفات الموظفين والمقابلات مع الموظفين و/أو الشهود) ، يجب توثيق جميع المعلومات التي تم جمعها على الفور وتخزينها في مكان سري. ويجب عدم مشاركة بيانات الموظفين الشخصية المكشوفة من خلال هذه التحقيقات مع أي شخص خارج (CSIRT).

9.4.24. **التحقيق والتحاليل الجنائية:**

1.9.4.24. عملية التحليل الجنائية: أي عملية تحليل أو تحقيق باستخدام وسائط تخزين بيانات تحتوي على معلومات قد تصبح في مرحلة ما دليلاً مهماً على جريمة كمبيوتر أو محاولة لإساءة استخدام الكمبيوتر، يجب تنفيذها على نسخة بدلاً من الإصدار الأصلي. سيساعد هذا في منع العبث بالمعلومات الأصلية.

2.9.4.24. تقارير حالة التحقيق: يجب إبلاغ تقارير تحقيقات أمن المعلومات بشكل دوري إلى الإدارة فقط بواسطة المحقق الرئيسي أو ممثل إدارة فريق التحقيق.

3.9.4.24. معلومات التحقيق في جرائم الكمبيوتر: يجب إبلاغ كبير المستشارين القانونيين بجميع الأدلة والأفكار والافتراضات المتعلقة بجرائم الكمبيوتر التي تتعرض لها **(جهة العمل)**، بما في ذلك أساليب الهجوم المحتملة ونوايا الجاني، ومعاملتها كمعلومات مقيّدة وقيّمة قانونيًا.

4.9.4.24. فرق التحقيق في أمن المعلومات: يُمنع على أي شخص ذو معرفة شخصية بالمشتبه به أو يكون صديقًا له من المشاركة في فريق التحقيق في حادث أمن المعلومات وذلك لتفادي تضارب المصالح.

5.9.4.24. التحقيقات الداخلية والاستفسارات الرسمية: يجب على جميع العاملين بـ **(جهة العمل)** الشهادة أو الرد على الأسئلة المرتبطة بالتحقيقات الداخلية عندما يتم توجيهها إليهم من قبل كبير المستشارين القانونيين.

6.9.4.24. تفاصيل التحقيقات في عمليات تسلل واختراق النظام: يجب عدم إرسال التفاصيل المتعلقة بالتحقيقات في عمليات تسلل واختراق نظام المعلومات التي لا تزال جارية عبر البريد الإلكتروني. ولمنع وقوع مثل هذه المعلومات في أيدي المتسللين، يجب ألا يتم تخزين الملفات التي تصف التحقيق الجاري على الأنظمة التي يحتمل أن تكون معرضة للخطر أو في أي مكان على الشبكة ذات صلة حيث يُتوقع من المتسللين مشاهدتها.

7.9.4.24. أثناء عملية التحليل: يجب على المحقق (المحققين) تدوين الملاحظات خطوة بخطوة

لجميع الإجراءات التي اتخذت لجمع البيانات. يجب أن تكون هذه الملاحظات مفصلة ومكتوبة بوضوح بحيث يمكن فهمها وتكرارها بواسطة محقق طرف ثالث.

10.4.24. **مراجعة الحادث:**

1.10.4.24. تقييم خطة الاستجابة للحوادث - الدروس المستفادة: يجب تحديث خطة الاستجابة للحوادث بحيث تعكس الدروس المستفادة من الحوادث الفعلية.

2.10.4.24. تقييم خطة الاستجابة للحوادث - تطورات المجال: يجب تحديث خطة الاستجابة للحوادث لتعكس التطورات في المجال.

5.24. المصطلحات والتعاريف

1.5.24. **كبير مسؤولي أمن المعلومات (CISO):** هو المسؤول التنفيذي الأول داخل المؤسسة والمسؤول عن إنشاء والحفاظ على رؤية المؤسسة واستراتيجيتها وبرنامجها لضمان حماية أصول بياناتها وتقنياتها.

2.5.24. **CERT (فريق الاستجابة لحالات الطوارئ بالكمبيوتر) / CSIRT (فريق الاستجابة لحوادث أمان الكمبيوتر):** هو فريق مختار بعناية ومدرب جيدًا من خبراء أمن تكنولوجيا المعلومات الذي يتمثل عملهم الرئيسي في الاستجابة لحوادث أمن الكمبيوتر كما يوفر الخدمات اللازمة للتعامل معها ودعم مكوناتها للتعافي من الانتهاكات.

3.5.24. **خرق البيانات:** حادثة أمنية تؤثر بشكل مباشر على البيانات الشخصية أو المعلومات الشخصية الحساسة أو معلومات التعرف الشخصية.

4.5.24. **التعامل مع الحوادث:** إجراءات الكشف، الإبلاغ والتقييم والاستجابة الى والتعامل مع والتعلم من حوادث أمن المعلومات.

5.5.24. **الاستجابة للحوادث:** الإجراءات المتخذة لتخفيف أو حل حادث أمن المعلومات، بما في ذلك تلك المتخذة لحماية واستعادة ظروف التشغيل العادية لنظام المعلومات والبيانات المخزنة فيه.

6.5.24. **البرمجيات الخبيثة:** البرمجيات أو البرامج الثابتة التي تهدف إلى إجراء عملية غير مصرح بها والتي سيكون لها تأثير سلبي على سرية أو سلامة أو توفر نظام المعلومات. فيروس أو دودة أو حصان طروادة أو أي كيان آخر قائم على الكود يصيب المضيف.

7.5.24. **حدث أمني:** حدث محدد لنظام أو خدمة أو حالة شبكة تشير إلى حدوث اخترا محتمل لسياسة أمن المعلومات أو استغلال محتمل لضعف الأمن أو موقف غير معروف مسبقًا قد يكون ذا صلة بالأمن.

8.5.24. **حادثة أمنية:** حدث يهدد فعليًا أو يحتمل أن يهدد سرية أو سلامة أو توفر أي نظام معلومات أو البيانات التي يعالجها النظام أو يخزنها أو يرسلها، أو تشكل انتهاكًا أو تهديدًا وشيكًا بانتهاك سياسات

الأمن أو الإجراءات الأمنية أو سياسات الاستخدام المقبول.

9.5.24. **ثغرة أمنية:** نقطة ضعف أو تحكم موجودة يمكن استغلالها بواسطة تهديد واحد أو أكثر.

10.5.24. **الضعف الأمني:** نقطة ضعف تنتج عن عدم وجود تحكم ضروري.

6.24. الملحق

1.6.24. تصنيف الحدث:

هذه القائمة ليست شاملة ويمكن إضافة فئات أخرى للمساعدة في عملية إعداد التقارير. يجب تصنيف الأحداث الأمنية وفقًا للتأثير أو التهديد المحتمل على سرية وسلامة وتوافر نظم المعلومات و / أو المعلومات الإلكترونية الخاصة بـ **(جهة العمل)**. التصنيف ضروري من أجل تقييم المخاطر التي تهدد خدمات وعمليات **(جهة العمل)** ، ولتحديد الاستجابة المناسبة

1.1.6.24. أنواع الحوادث

النوع	الوصف
محاولة الاقتحام	محاولة اقتحام ملحوظة و / أو مستمرة تبرز فوق النشاط اليومي قد تؤدي إلى وصول غير مصرح به إلى المعلومات أو نظام المعلومات الإلكتروني المستهدف.
حجب الخدمة	حجب الخدمة عن قصد أو بدون قصد (المحاولات الناجحة أو المستمرة) التي تؤثر أو تهدد بالتأثير على خدمة حرجة أو تمنع الوصول إلى جميع أو جزء كبير أو أكثر من أجزاء شبكة **(جهة العمل)**
البرمجيات الخبيثة	جميع حالات الإصابة الناجحة أو المحاولات المستمرة للإصابة بأكواد خبيثة أو ضارة ، مثل الفيروسات أو أحصنة طروادة أو الدودة.
انتهاك السياسة	الوصول إلى أو استخدام نظم المعلومات أو المعلومات الإلكترونية الخاصة بالمؤسسة والتي تنتهك سياسات المنظمة وقد تشكل خطراً على نظم المعلومات أو المعلومات الإلكترونية الخاصة بالمنظمة.
نشاط الاستطلاع	مثل مسح المنافذ غير المصرح به ، وشم الشبكة ، وتحقيقات ومسح خرائط تعيين الموارد ، وغيرها من الأنشطة التي تهدف إلى جمع المعلومات حول الثغرات الأمنية في شبكة المنظمة وتعيين موارد الشبكة والخدمات المتاحة.
الهندسة الاجتماعية	هي مثيل (أو مثيلات) حيث يستخدم المهاجم تفاعلًا بشريًا للحصول على معلومات حول «المنظمة» أو موظفيها أو أنظمة المعلومات الخاصة بها.
استخدام بدون تخويل	أي نشاط غير معروف بأنه مرتبط بنشاط المؤسسة أو الاستخدام العادي

2.1.6.24. مستويات خطورة الحوادث

يُعد تقييم شدة الحادث مقياسًا شخصيًا لتهديده لعمليات أي منظمة. يساعد مستوى الخطورة في تحديد أولوية التعامل مع الحادث ، ومن يدير الحادث، وخطة الاستجابة للحادث.

العوامل التالية تساعد في تحديد مستوى الخطورة:

- أهمية نظام المعلومات.
- حساسية المعلومات المخزنة على أو الوصول إليها من خلال النظام أو الخدمة.
- احتمال الانتشار. هل الحادث موجود أم يمكن أن ينتشر خارج حدوده الحالية؟

2.6.24. معالجة الحوادث والإبلاغ عنها:

يجب أن يتضمن تقرير الحادث معلومات أساسية عن حادث أمن المعلومات، مثل متى وماذا وكيف ولماذا وقع الحادث ، وكذلك فئة الحادث وتأثيره ونتيجة لرد الفعل.

1.2.6.24. المعلومات الأساسية

1.1.2.6.24. تاريخ الحادثة

2.1.2.6.24. رقم الحادثة

3.1.2.6.24. الأحداث ذات الصلة و / أو أرقام الحوادث (إن وجدت)

2.2.6.24. الشخص المبلغ عن الحادثة

1.2.2.6.24. الاسم

2.2.2.6.24. معلومات الاتصال مثل العنوان والتنظيم والقسم والهاتف والبريد الإلكتروني

3.2.6.24. تفاصيل عضو CSIRT

1.3.2.6.24. الاسم

2.3.2.6.24. معلومات الاتصال مثل العنوان والتنظيم والقسم والهاتف والبريد الإلكتروني

4.2.6.24. وصف الحادث

1.4.2.6.24. ماذا حدث

2.4.2.6.24. كيف حدث

3.4.2.6.24. لماذا حدث

4.4.2.6.24. وجهات النظر الأولية حول المكونات / الأصول المتأثرة

5.4.2.6.24. أي ثغرة أمنية محددة

6.4.2.6.24. الموقع الفعلي لنظام المعلومات المتأثر.

5.2.6.24. تفاصيل الحادث

1.5.2.6.24. تاريخ ووقت وقوع الحادث

2.5.2.6.24. تاريخ ووقت اكتشاف الحادث

3.5.2.6.24. تاريخ ووقت وقوع الحادث

6.2.6.24. فئة الحادث

1.6.2.6.24. المكونات / الأصول المتأثرة

2.6.2.6.24. انعكاس تأثير ضرر الحادث على الأعمال

3.6.2.6.24. إجمالي تكلفة الاسترداد من الحادث

24.6.2.6.4. قرار الحادث

24.6.2.6.5. الشخص (الأشخاص) / مرتكب الجريمة (الأشخاص) المعنيون (إذا وقع الحادث بسبب أشخاص)

24.6.2.6.6. وصف الجاني

24.6.2.6.7. الإجراءات المتخذة لحل الحادث

24.6.2.6.8. الإجراءات المخطط لها لحل الحادث

24.6.2.6.9. الإجراءات المتميزة

24.6.2.6.10. الخاتمة

24. Incident Handling Policy

24.1. Overview

Simultaneously with their growing Online presence, organizations and individuals become increasingly susceptible to cybersecurity attacks. Most organizations prefer to avoid and mitigate the damage caused by such attacks by establishing and implementing information security policies and plans.

Incident handling policy deals with the aftermath of an information security incident. It outlines who, where, and how should respond to the incident. In case an organization lacks an incident response policy, a response to an incident may be delayed, and the evidence indicating the cause of the incident can be permanently lost. This, in turn, will increase the impact of the incident and prevent the organization from addressing similar incidents in the future. Drafting an effective incident response policy requires substantial planning and resources.

24.2. Purpose

This document defines the policy for addressing Security Incidents related to **(Organization)** information systems and operations through appropriate Incident Response. Additionally, the objective of this policy is to create a set of standards that should be followed whenever a cybersecurity incident occurs.

24.3. Scope

This policy applies to all employees, contractors, consultants and partners of **(Organization)** entities including, but not limited to, business units and subsidiaries.

24.4. Policy

24.4.1. **Incident Handling Organization:**

24.4.1.1. Incident Handling Plan: This plan must be drafted and should include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners.

24.4.1.2. Computer Security Incident Response Team: Information Technology Department management must organize and maintain a Computer Security Incident Response Team (CSIRT) or any equivalent qualified Incident Response Team (IRT) that has the same roles and responsibilities.

24.4.2. **Roles and Responsibilities:**

24.4.2.1. Incident Response Availability: **(Organization)** Computer Security Incident Response Team (CSIRT) must be available at all times to respond to alerts that include but are not limited to an evidence of unauthorized activity,

detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

24.4.2.2. Designated Contact Person for All Disasters and Security Events: Unless expressly recognized as an authorized spokesperson for **(Organization)**, no worker may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

24.4.2.3. Incident Management Responsibilities: The individuals responsible for handling information systems security incidents must be clearly defined by the most senior Information Security staffer. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

24.4.2.4. Providing Information in Legal Proceedings: Workers are prohibited from providing any **(Organization)** records, or any copies thereof, to third parties outside of **(Organization)** or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the Chief Legal Counsel has first been obtained.

24.4.2.5. Crisis Management Plan: Crisis management plan must be prepared and annually updated, it should cover topics such as a process for managing the crisis, crisis decision making continuity, the safety of employees, damage control, and communications with third parties such as the media.

24.4.3. **Prepare the CSIRT:** to prepare CSIRT **(Organization)** must:

24.4.3.1. Obtain all hardware and software needed to investigate an incident and keep it stored in a secure location.

24.4.3.2. Maintain a series of forms and report templates that will be used to document incidents, the procedures used to investigate the incident, and the subsequent findings.

24.4.3.3. Select a group of employees to serve on the CSIRT. This team should contain experts from all technical areas supported by **(Organization)**, such as (Network, telecommunications, technical support, server administration, etc.), so the team is prepared to handle any computer incident. Members of the CSIRT will only need to respond to incidents that pertain to their body of knowledge. However, one member of the CSIRT should be designated as the lead investigator and will be responsible for organizing and managing the CSIRT whenever an incident occurs. All members of the CSIRT must receive periodic training on how to properly respond to an incident.

24.4.4. **Reporting:**

24.4.4.1. Incident reports must accurately describe the details of an event and should be written in language that is understandable to readers without a technical background.

24.4.4.2. Cybersecurity incidents or/and Security Events, once discovered, must be promptly reported as quickly as possible through appropriate management channels

- Telephone calls
- Voice mail
- Email
- Website form
- Ticketing System

24.4.4.3. Personnel and contractors using the **(Organization)**'s information systems and services are responsible to note or report any observed or suspected security weakness or incident in systems or services and any violations of policy using the appropriate reporting procedures. Failure to report an incident will lead to disciplinary action against the user(s) who witnessed or detected the incident.

24.4.4.4. Internal incidents must be reported by contacting the Help Desk or the Chief Information Security Officer (CISO). For all incidents reported to the Help Desk, the technician receiving the call must gather information on the nature of the incident as detailed in the Incident Notification form and immediately notify the CISO of the incident. The Help Desk technician should not discuss the incident with anyone else unless instructed to do so by the CISO.

24.4.4.5. Incident reports originating from sources outside the **(Organization)** shall be taken seriously and investigated for validity. Discoveries from the resulting investigation should be handled using the established policies.

24.4.4.6. Loss or disclosure of sensitive information: If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Department [or equivalent department] must be notified immediately.

24.4.4.7. Violation And Problem Reporting Interference: Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action.

24.4.4.8. Reporting Unauthorized Activity: Users of **(Organization)** information systems must immediately report to the most senior Information Security staffer any unauthorized loss of, or changes to computerized production data.

Any questionable usage of files, databases, or communications networks must likewise be immediately reported to the same senior.

24.4.4.9. Reporting System Vulnerabilities: Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Systems Help Desk. Users are prohibited from utilizing **(Organization)** systems to forward such information to other users, whether the other users are internal or external to **(Organization)**.

24.4.4.10. Security Weaknesses and Vulnerability Discussion: Workers who discover a weakness or vulnerability in the information security measures used by **(Organization)** must not discuss these matters with anyone other than the most senior Information Security staffer, Internal Audit Manager, or trained investigators designated by one of them.

24.4.4.11. Reporting Security Vulnerabilities: When a new and serious information systems security vulnerability associated with a particular vendor's hardware or software is discovered, it must be immediately reported to appropriate public media for public dissemination.

24.4.4.12. Schedule for Responses to Reported Security Problems: **(Organization)** must acknowledge receipt of all reported vulnerabilities with its products or services within seven days. It must provide a detailed response to the reporting party within ten days from the time the report was received. It must also endeavor to contact the reporting party every seven days while a patch or fix is being developed, and it must endeavor to resolve the vulnerability within thirty days, or as soon as is practically feasible concisely and clearly.

24.4.4.13. All investigative steps and conclusions shall be documented as they occur.

24.4.4.14. All reports must be written using the existing template for the incident type.

24.4.4.15. All incident reports must be reviewed by the CISO, and by management for incidents

24.4.4.16. All reports and evidence pertaining to an incident shall be retained for a period of at least 10 years.

24.4.5. **Initial Response:**

24.4.5.1. Before starting an investigation, the CSIRT needs to verify that an incident has actually occurred. The following actions must be taken by the CSIRT to provide them with enough information to make this decision:

24.4.5.2. Review the Incident Notification form filled out by the Help Desk technician or the CISO. The incident reporter should be contacted if further information or clarification is needed.

24.4.5.3. Review relevant system logs to identify data that would support the belief an incident has occurred. Interview Organization personnel (non-IT) that

may be able to provide a context for the incident. Note that all steps may not be required for certain types of incidents. Discretion should always be used when acquiring system logs and questioning employees who are not aware of the incident. At the end of this phase, the CSIRT should know whether or not an incident occurred and if so what type of incident occurred, which systems are affected, and the potential impact to **(Organization)**. The investigation shall not proceed until all of the previous questions can be answered by the CSIRT.

24.4.6. **Security Event Monitoring:**

24.4.6.1. Security Events should be assessed and it must be decided if they are to be classified as Security Incidents.

24.4.6.2. Incident Alerts – IDS: The incident response plan must include actions required to alerts from the intrusion detection system.

24.4.6.3. Incident Alerts – IPS: The incident response plan must include actions required to alerts from the intrusion prevention system.

24.4.6.4. Incident Alerts - File Integrity Monitoring Systems: The incident response plan must include actions required to alerts from all file integrity monitoring systems.

24.4.6.5. Data Breach Management

24.4.6.6. Data Breach Response Plan: **(Organization)** management must be prepared, tested and annually updated, a Data Breach Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive data.

24.4.7. **Collection of Evidence:**

24.4.7.1. Sources of Digital Evidence: For every production computer system, the Information Security Department must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subject a standardized capture, retention, and destruction process comparable to that used for vital records.

24.4.7.2. individual person responsible for electronic evidence production: **(Organization)** will appoint an individual responsible for coordinating the discovery and presentation of electronic evidence that may be required in a court case.

24.4.7.3. Special Data classification for possible electronic evidence: **(Organization)** data that may be considered electronic evidence must have a specific data classification.

24.4.7.4. Electronic data must be collected in a forensically sound manner. Whenever possible, a forensics toolkit such as EnCase or FTK must be used. For evidence that is not collected via a forensics toolkit, the investigator(s) must take detailed notes of how the data was collected.

24.4.7.5. Md5 sums shall be taken of all collected data immediately following evidence acquisition.

24.4.7.6. All electronic evidences must be copied to removable storage and placed in a locked evidence cabinet or safe to which only the CISO and the lead member of the CSIRT have access. Every piece of evidences will have an accompanying evidence tag.

24.4.7.7. For incidents requiring non-electronic evidence (e.g., personnel files and interviews with employees and/or witnesses), all information gathered must be immediately documented and stored in a confidential location. Personal employee data learned through these inquiries by an investigator must not be shared with anyone outside of the CSIRT.

24.4.8. **Investigation and Forensics:**

24.4.8.1. Forensic Analysis Process: Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

24.4.8.2. Investigation Status Reports: The status of information security investigations must be communicated periodically to management only by the lead investigator or the management representative of the investigation team.

24.4.8.3. Computer Crime Investigation Information: All evidence, ideas, and hypotheses about computer crimes experienced by **(Organization)**, including possible attack methods and perpetrator intentions, must be communicated to the Chief Legal Counsel and treated as restricted and legally privileged information.

24.4.8.4. Information Security Investigation Teams: Any person who personally knows the suspects, or who is friendly with them, for conflict of interest reasons is barred from participating on an information security incident investigation team.

24.4.8.5. Internal Investigations and Official Inquiries: All **(Organization)** workers must testify or otherwise respond to questions associated with internal investigations when directed to do so by the Chief Legal Counsel.

24.4.8.6. Intrusion Investigations Details: Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of

intruders, files which describe an investigation now underway must not be stored on potentially compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

24.4.8.7. During the analysis process: the investigator(s) must take step by step contemporaneous notes of all actions that were taken to collect the data. These notes should be detailed and clearly written such that they could be understood and repeated by a third-party investigator.

24.4.9. **Incident Review:**

24.4.9.1. Incident Response Plan Evolution - Lessons Learned: The incident response plan must be updated to reflect the lessons learned from actual incidents.

24.4.9.2. Incident Response Plan Evolution - Industry Developments: The incident response plan must be updated to reflect developments in the industry.

24.5. Terms and Definitions

24.5.1. **CISO (Chief information security officer):** is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

24.5.2. **CERT (Computer Emergency Response Team) / CSIRT (Computer Security Incident Response Team):** is a carefully selected and well-trained team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches

24.5.3. **Data Breach:** A Security Incident that directly impacts Personal Data, Sensitive Personal Information or Personally Identifiable Information.

24.5.4. **Incident handling:** actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents

24.5.5. **Incident response:** Actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

24.5.6. **Malicious Code:** Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

24.5.7. **Security Event:** An identified occurrence of a system, service or network state indicating a possible breach of information security policy, a possible exploitation of a Security Vulnerability or Security Weakness or a previously unknown situation that can be security relevant.

24.5.8. **Security Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

24.5.9. **Security Vulnerability:** A weakness of an existing asset or control that can be exploited by one or more threats.

24.5.10. **Security Weakness:** A weakness that results from the lack of an existing, necessary control.

24.6. APPENDIX

24.6.1. **Event Categorization:**

This list is not comprehensive and other categories may be added to help with the reporting process. Security events must be categorized according to the potential impact or threat to the confidentiality, integrity, and availability of the **(Organization)**'s electronic information and/or information systems. Categorization is necessary in order to assess the risk to the **(Organization)**'s business services and operations, and to determine the appropriate response.

24.6.1.1. Incident Types

TYPE	DESCRIPTION
Attempted Intrusion	A significant and/or persistent attempted intrusion that stands out above the daily activity and could result in unauthorized access of the target electronic information or information system.
Denial of Service	Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of the **(Organization)**'s network.
Malicious Software	All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms.

Policy Violation	Access or use of the **(Organization)**'s electronic information or information systems that violates Rowan policies and may present a risk to the **(Organization)**'s electronic information or information systems.
Reconnaissance Activity	Instances of unauthorized port scanning, network sniffing, resourcing mapping probes and scans, and other activities that are intended to collect information about vulnerabilities in the **(Organization)**'s network and to map network resources and available services.
Social Engineering	An instance (or instances) where an attacker uses human interaction to obtain or compromise information about the **(Organization)**, its personnel, or its information systems.
Unauthorized Use	Any activity that is not recognized as being related to **(Organization)** business or normal use.

24.6.1.2. Incident Severity Levels:

Rating the severity of an incident is a subjective measure of its threat to any Organization's operations. The severity level helps determine the priority for handling the incident, who manages the incident, and the incident response plan.

The following factors help determine severity level:

- Criticality of the information system.
- Sensitivity of the information stored on or accessed through the system or service.
- Probability of propagation. Is the incident contained or can it spread beyond its current boundaries?

24.6.2. INCIDENT HANDLING AND REPORTING

The incident report must include basic information of the information security incident, such as when, what, how and why the incident occurred, as well as the incident category, impact, and result of incident response.

24.6.2.1. Basic information

24.6.2.1.1. Date of incident

24.6.2.1.2. Incident number

24.6.2.1.3. Related event and/or incident numbers (if applicable)

24.6.2.2. Reporting person

24.6.2.2.1. Name

24.6.2.2.2. Contact information such as address, organization, department, telephone and e-mail

24.6.2.2.3. CSIRT member details
24.6.2.2.4. Name
24.6.2.2.5. Contact information such as address, organization, department, telephone and e-mail

24.6.2.3. Incident description

24.6.2.3.1. What occurred
24.6.2.3.2. How occurred
24.6.2.3.3. Why occurred
24.6.2.3.4. Initial views on components/assets affected
24.6.2.3.5. Any vulnerability identified
24.6.2.3.6. Physical location of the affected information system.

24.6.2.4. Incident details

24.6.2.4.1. Date and time the incident occurred
24.6.2.4.2. Date and time the incident was detected
24.6.2.4.3. Date and time the incident was reported

24.6.2.5. Incident category

24.6.2.5.1. Components/assets affected
24.6.2.5.2. Adverse business impact/effect of incident
24.6.2.5.3. Total recovery cost from incident
24.6.2.5.4. Incident resolution
24.6.2.5.5. Person(s)/perpetrator(s) involved (if incident caused by people)
24.6.2.5.6. Description of perpetrator
24.6.2.5.7. Actions taken to resolve incident
24.6.2.5.8. Actions planned to resolve incident
24.6.2.5.9. Actions outstanding Conclusion

25. سياسة النسخ الاحتياطي

1.25. مقدمة

تفشل الأنظمة وأجهزة الكمبيوتر بشكل مفاجئ 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 ما يلي:

- 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 المخزنة في الوقت المناسب في حالة حدوث كارثة أو فشل في النظام.

2.25. 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.

3.25. 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.

4.25. السياسة

1.4.25. تحديد البيانات الهامة:

1.1.4.25. يجب أن 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.

2.1.4.25. البيانات التي يتم نسخها احتياطياً

سيتم الاحتفاظ بنسخة احتياطية من:

1.2.1.4.25. جميع البيانات التي تقرر أنها هامة وحساسة لأعمال (جهة العمل) و/أو وظيفة الموظف.

2.2.1.4.25. جميع المعلومات المخزنة على خادم الملفات التابعة لـ (جهة العمل). وتقع على عاتق المستخدم ضمان نقل أي بيانات ذات أهمية إلى

خادم الملفات.

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

2.4.25. تخزين النسخ الاحتياطي:

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

2.2.4.25. يجب الحفاظ على الفاصل 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.

3.2.4.25. 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.

4.2.4.25. يسمح بالنسخ الاحتياطي عبر الإنترنت (في السحابة) إذا كانت الخدمة تلبي المعايير المحددة في **(جهة العمل)**.

3.4.25. تكرار النسخ الاحتياطي:

1.3.4.25. يجب إجراء عملية النسخ الاحتياطي على فترات منتظمة.

2.3.4.25. الآلية التي يتم بها تكرار عملية النسخ الاحتياطي هي ما يضمن استعادة البيانات بنجاح، يجب 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.

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

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

5.3.4.25. 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 بدءاً 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.

4.4.25. الاحتفاظ بالنسخ الاحتياطي:

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

2.4.4.25. 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.

5.4.25. النسخ المخزنة:

1.5.4.25. النسخ المخزنة يجب أن تخزن مع وصف قصير يتضمن المعلومات التالية:

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

2.5.4.25. يجب الاحتفاظ بسجل للحركات المادية والإلكترونية لجميع النسخ الاحتياطية، يجب أن تشير الحركة المادية والإلكترونية للنسخ الاحتياطية إلى:

1.2.5.4.25. النسخة الاحتياطية الأولية وطريقة نقلها إلى التخزين.

2.2.5.4.25. أي حركة للنسخ الاحتياطية من موقع التخزين الخاص بها إلى موقع آخر.

3.5.4.25. 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:

1.3.5.4.25. تعبئة نموذج يوضح تفاصيل الطلب، بما في ذلك النسخة المطلوبة وأين ومتى يرغب مقدم الطلب في استلامها والغرض من طلب النسخة.

2.3.5.4.25. الإقرار بأن النسخة الاحتياطية سيتم إرجاعها أو إتلافها فور الانتهاء من استخدامها.

3.3.5.4.25. تقديم إيصال تسليم كدليل على أن النسخة الاحتياطية قد تم إرجاعها.

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

6.4.25. اختبار عملية استعادة البيانات:

1.6.4.25. يجب أن يتم فحص والقيام بإجراءات استعادة النسخ الاحتياطية بشكل منتظم لضمان

فعاليتها وللتحقق من إمكانية استكمال إجراءات عملية الاستعادة في الوقت المحدد والإبلاغ عن قدرتها على استعادة البيانات.

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

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

4.6.4.25. 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.

7.4.25. وسائط النسخ الاحتياطي:

1.7.4.25. 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:

1.1.7.4.25. أثبات هوية ذو صلة

2.1.7.4.25. إذن تخويل ذو صلة

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

1.2.7.4.25. استخدام أماكن تخزين (حاويات) آمنة.

2.2.7.4.25. التسليم باليد.

3.2.7.4.25. في الحالات الحرجة يتم تقسيم ما سيتم تسليمه إلى أجزاء يرسل كل جزء عبر طريق مختلفة عن غيره.

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

1.3.7.4.25. يجب تجهيز وسائط النسخ الاحتياطي للتخلص منها.

2.3.7.4.25. يجب أن لا تحتوي الوسائط على نسخ احتياطية يمكن إعادة استخدامها (فعالة).

3.3.7.4.25. يجب ضمان عدم الوصول لمحتويات الوسائط الحالية أو السابقة وقراءتها أو استرجاعها من قبل طرف غير مصرح له.

4.3.7.4.25. يجب العمل على أن تتلف وسائط النسخ الاحتياطي ماديا بحيث لا يمكن استعادة محتوياتها قبل التخلص منها.

4.4.7.4.25. 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.

25. Data Backup Policy

25.1. Introduction

Systems and computers fail periodically. Vital records, systems and work products may be irretrievably lost if they have only been stored on the failed computer or computer system. The resulting frustrations, lack of productivity and cost are few of the consequences. This policy is designed to prevent such occurrences by having alternative locations for these systems and data, so they can be restored.

Data backup is the process of copying, storing and restore and recovery of computer data. Simply stated data in whatever format it may be in.

The purpose data backup is as follows:

- To provide secure storage for data assets critical to the work flow at **(Organization)**.
- To prevent loss of data in the case of accidental deletion, corruption of data, system failure, or disaster.
- To permit timely restoration of archived data in the event of a disaster or system failure.

25.2. Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

25.3. Scope

This policy applies to all data stored on **(Organization)** systems, on all computers, both laptops and desktops, and to all servers owned by **(Organization)** and any other electronic devices that may have storage capacity and consists of relevant data.

25.4. Policy

25.4.1. **Identification of Critical Data:**

25.4.1.1. **(Organization)** must identify what data is most critical. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

25.4.1.2. Data to be Backed Up

25.4.1.3. All data determined to be critical to **(Organization)** operation and/or employee job function.

25.4.1.4. 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.

25.4.1.5. All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

25.4.2. **Backup Storage:**

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

25.4.2.2. 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.

25.4.2.3. 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.

25.4.2.4. Online backups (Cloud) are allowable if the service meets the criteria specified herein.

25.4.3. **Backup Frequency/Procedure:**

25.4.3.1. Backups must be carried out at regular intervals.

25.4.3.2. Backup frequency is critical to successful data recovery. **(Organization)** must 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.

25.4.3.3. 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)**.

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

25.4.3.5. 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.

25.4.4. **Backup Retention:**

25.4.4.1. **(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.

25.4.4.2. 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.

25.4.5. **Stored copies:**

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

25.4.5.2. 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.

25.4.5.3. 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.

25.4.5.4. Backup information must 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.

25.4.6. **Restoration Testing:**

25.4.6.1. 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.

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

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

25.4.6.4. 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.

25.4.7. **Backup Media:**

25.4.7.1. 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.

25.4.7.2. 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.

25.4.7.3. 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.

25.4.7.4. 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.

26. سياسة خطة التعافي من الكوارث

1.26. مقدمة

يتطلب العمل عدة موارد مختلفة من الموظفين والبنية التحتية والتكنولوجيا والتي بلا شك أحد أهم الجوانب الأساسية للنجاح، لذلك يجب أن تكون (جهة عمل) جاهزة لأى أحداث مفاجئة مثل الحرائق أو التخريب أو الإرهاب أو فشل النظام أو الكوارث الطبيعية والتي من شأنها أن تسبب اضطراب أو توقف في عمل التكنولوجيا وبالتالي (جهة عمل).

غالبًا ما تكون خطة التعافي من الكوارث جزءًا من خطة استمرارية الأعمال، وهي عملية استعادة خدمات التكنولوجيا الهامة المستخدمة لدعم عمليات المنظمة فور حدوث توقف أو اضطراب كبير بسبب حدث مفاجئ سواء أكان من صنع الإنسان أو كارثة طبيعية.

2.26. الغرض

الغرض من هذه السياسة هو توفير التوجيهات والقواعد العامة لتجهيز وتنفيذ ثم إدارة خطة التعافي من الكوارث (DRP) لـ (جهة عمل). وتحدد هذه السياسة المتطلبات الأساسية لخطة التعافي من الكوارث، والتي يمكن تطويرها من قبل (جهة عمل) حيث سيتم وصف عملية استرداد أنظمة تكنولوجيا المعلومات وتطبيقاتها وبياناتها من أي نوع من الكوارث التي تسبب توقف أو انقطاع كبير في الأعمال.

3.26. النطاق

تنطبق هذه السياسة على موظفي إدارة تكنولوجيا المعلومات والاتصالات في **(جهة العمل)** وهم المسؤولون عن تطوير الخطة واختبارها وتحديثها، كما يحتوي نطاق هذه السياسة على إجراءات خطة الاسترداد التي يجب تطويرها وتنفيذها في حالة الطوارئ أو الكوارث وذلك فيما يخص أى نظام يحتوي على معلومات مخزنة إلكترونياً، ويشمل ذلك النسخ الاحتياطي للبيانات والتخطيط لاسترجاعها وتفعيل وضع الطوارئ.

4.26. السياسة

على (جهة عمل) أن تنشأ خطة تعافي من الكوارث وتطورها وتنفذها عند اللزوم لضمان استرجاع البيانات التي فُقدت بسبب حدث طارئ كالحريق والتخريب المتعمد والتعرض لعملية إرهابية أو الكوارث الطبيعية بأشكالها.

1.4.26. يجب أن تكون خطة التعافي من الكوارث مُوثقة ومُخزنة بطريقة يسهل الوصول إليها من قبل الأشخاص المكلفين والمسؤولين على تنفيذها.

2.4.26. يجب تخزين نسخة من الخطة في موقع خارج (جهة عمل) أو على السحابة.

3.4.26. يجب مراجعة خطة التعافي من الكوارث واختبارها والموافقة عليها على بشكل سنوي.

4.4.26. نتائج اختبارات خطة التعافي من الكوارث يجب توثيقها ليتم استعمالها فيما بعد كجزء من عملية تحسين الخطة .

5.4.26. تنفيذ إجراءات خطة التعافي يجب أن يكون تحت قيادة الوحدة الإدارية المسؤولة عن أمن المعلومات (أو ما يكافئها)، ومع ذلك؛ يجب أن يتم مشاركة قسم الشؤون الإدارية في هذه العملية.

6.4.26. **يجب أن تحتوي خطة التعافي من الكوارث على الإجراءات التالية:**

1.6.4.26. تحليل لتقييم المخاطر (Risk Assessment).

2.6.4.26. استراتيجيات التخفيف من المخاطر والإجراءات الاحترازية اللازمة لتجنب الكوارث. هذه الإجراءات يجب أن تشمل التدابير الوقائية مثل إخماد الحرائق وإمدادات الطاقة الاحتياطية لضمان عدم الانقطاع (UPS) والحماية من زيادة التيار وتدابير بيئية لحماية المعدات الحساسة من الغبار أو درجة الحرارة أو الرطوبة.

3.6.4.26. النسخ الاحتياطية والتخزين المتعدد خارج الموقع.

4.6.4.26. إجراءات الإبلاغ عن الحوادث ، وتصعيد استجابة (جهة عمل) للكوارث.

5.6.4.26. يجب تصنيف البيانات المخزنة على الأنظمة وتفصيلها وفقًا لمدى أهميتها وسريتها.

6.6.4.26. يجب وصف / إدراج جميع المعدات وتطبيقات البرامج وأي متطلبات أخرى لإكمال خطة التعافي من الكوارث.

7.6.4.26. الأشخاص المسؤولون

1.7.6.4.26. يجب تكليف أشخاص معينين بقرارات الإعلان عن الكارثة.

2.7.6.4.26. يجب تكليف أشخاص مؤهلين يتمتعون بالمسؤولية والخبرة والكفاءة اللازمة لتنفيذ أنشطة التعافي من الكوارث، ويجب أن يتم وصف ذلك بوضوح في الخطة.

3.7.6.4.26. ينبغي وصف تسلسل المسؤولية، بمعنى أن كل فرد من أفراد الفريق الأساسي يجب أن يكون له شخص بديل يستطيع القيام بالمهام المطلوبة.

4.7.6.4.26. يجب إعداد خطة اتصال مناسبة متضمنة شجرة تشعب وتدرج اتصال واضحة.

8.6.4.26. النسخ الاحتياطي واسترجاع البيانات

يجب عمل نسخ احتياطي للبيانات بشكل منتظم وفقًا لسياسة النسخ الاحتياطي، لضمان أن (جهة عمل) لديها نسخة محدثة من جميع البيانات. بناءً على تصنيف سياسة البيانات، سيكون من السهل معرفة البيانات التي يجب استردادها أولاً، ومع ذلك يجب مراعاة ما يلي في الخطة:

1.8.6.4.26. يجب وضع إجراء لتحديد هدف نقطة الاسترداد (RPO) وهدف وقت

الاسترداد (RTO)، هذا الإجراء يجب الموافقة عليه من الإدارة العليا ومالكي البيانات.

.2.8.6.4.26 ينبغي وصف كيفية استعادة البيانات.

.3.8.6.4.26 يجب أن تنشئ إدارة / قسم تقنية المعلومات («IT») موقعًا بديلًا لمركز القيادة يكون آمنا ومناسبا لإدارة أنشطة الاسترداد.

.4.8.6.4.26 يجب مراقبة عمليات النسخ الاحتياطي والاستعادة لضمان إكمالها بنجاح، وقد يؤدي نقص المراقبة والمتابعة إلى فشل هذه العمليات.

26. Disaster Recovery Plan Policy

26.1. Overview

Business requires several different resources like staff, infrastructure, and technology, which is undoubtedly one of the core aspects of success. Therefore, **(Organization)** must be ready for any disturbances in technology that can happen due to unexpected events such as fire, vandalism, terrorism, system failure, or natural disaster.

The Disaster Recovery Plan (DRP) is often part of the Business Continuity Plan, and it is the process of restoring critical technology services used to support business operations immediately following a significant man-made or natural disruption ("disaster").

26.2. Purpose

The purpose of this policy is to provide directions and general rules for the creation, implementation, and management of the Disaster Recovery Plan (DRP) for **(Organization)**. This policy defines the requirements for a baseline disaster recovery plan to be developed and implemented by **(Organization)** that will describe the process to recover IT Systems, Applications, and Data from any type of disaster that causes a major outage.

26.3. Scope

This policy is directed to the Information and communication technology (ICT) Management Staff who is accountable to ensure the plan is developed, tested, and kept up to date. The scope of this policy contains procedures regarding a recovery plan that shall be developed and implemented in the event of an emergency, disaster, or other occurrences, when any system that contains electronically stored information is affected, including data backup, disaster recovery planning, and emergency mode operation plan.

26.4. Policy

Disaster Recovery Plan (DRP) must be created, developed, and implemented when needed to ensure recoverability from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, or natural disaster.

26.4.1. The Disaster Recovery Plan must be documented and easily available to the assigned personnel who are accountable to implement it.

26.4.2. A plan copy should be stored in a remote location.

26.4.3. The Disaster Recovery Plan must be reviewed, tested, and approved on an annual basis.

26.4.4. The tests results must be documented to be used as part of the ongoing improvement of the DRP.

26.4.5. The DRP Activities must be led by the Information Security department (or equivalent), however; the administration department should be involved.

26.4.6. **The DRP must include the following procedures:**

26.4.6.1. Risk assessment analysis

26.4.6.2. Risk mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as fire suppression, uninterruptible power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature, or humidity.

26.4.6.3. Backups and multiple offsite storages.

26.4.6.4. Procedures for reporting incidents and escalating the **(Organization)**'s response to a disaster.

26.4.6.5. Data stored on the systems should be classified and detailed according to its criticality and confidentiality.

26.4.6.6. All equipment, software applications, and any other requirements to complete the recovery plan successfully must be described/listed in the DRP.

26.4.6.7. Accountable personnel

26.4.6.7.1. Disaster declaration decisions should be assigned to a responsible person.

26.4.6.7.2. Proper communication plan should be prepared including a clear call tree.

26.4.6.7.3. The flow of responsibility when normal staff is unavailable to perform their duties should be described.

26.4.6.7.4. Qualified personnel with the necessary responsibility, experience, and competence should be assigned to implement the activities of the disaster recovery, and this should be clearly described in the DRP.

26.4.6.8. Backup and Data Recovery:

26.4.6.9. Data backup must be applied on regular basis according to Backup Policy, to ensure the **(Organization)** has an updated copy of all data. Based on data classification, it will be easy to know which data should be recovered first, However, the following must be considered in the DRP:

26.4.6.10. Procedure for recovery point objective (RPO) and recovery time objective (RTO) should be approved by senior management and data owners.

26.4.6.11. The method of recovering data should be described)how the data will be recovered(.

26.4.6.12. The Information Technology ("IT") Department shall establish an alternative command center location that provides secure and suitable facilities for the management of recovery activities.

26.4.6.13. The backup and recovery processes should be monitored to ensure successful completion; lack of monitoring and follow-up may cause the failure of these processes.

27. سياسة خصوصية بيانات العملاء

1.27. مقدمة

من الضروري أحياناً أن يقوم العملاء بإرسال بيانات مختلفة إلى خدمة دعم العملاء التابعة لـ **(جهة العمل)**، وحيث أن هذه البيانات قد تحتوي على معلومات سرية و/أو حساسة وجب التعامل معها بطريقة خاصة، يتم التعامل مع بيانات العميل بالطريقة الموضحة أدناه، ما لم يكن هناك توجيه بخلاف ذلك في اتفاقية عدم الإفصاح بينهم.

بيانات العميل هي معلومات خاصة بمشكلة أو مسألة محددة مقدمة من العميل في شكل إلكتروني لأغراض حل المشكلات المتعلقة بمنتج أو بخدمة معينة.

2.27. الغرض

تهدف هذه السياسة الى حماية بيانات العملاء السرية أو الحساسة التي يقدمونها في سياق المعاملات اليومية المتعلقة بأعمال **(جهة العمل)**. حيث أن حماية بيانات العملاء من متطلبات الأعمال الهامة مع ضرورة توفر المرونة للوصول إلى البيانات والعمل بفعالية بدون ان تتعرض هذه البيانات للخطر.

3.27. النطاق

تسري هذه السياسة على جميع الموظفين والأجهزة التي تتعامل مع بيانات العملاء في **(جهة العمل)**.

4.27. السياسة

1.4.27. يجب تصنيف جميع بيانات العملاء على أنها بيانات سرية أو مقيدة، وهي ليست مفتوحة المصدر ويجب التعامل على أنها سرية عندما استلامها فوراً. يقتصر الوصول إلى هذه المعلومات على عدد محدود من الموظفين وبأساس «الحاجة إلى المعرفة». (كما هو موضح في سياسة حماية البيانات).

2.4.27. **استخدام البيانات الشخصية:** يُحظر الكشف عن بيانات العملاء الشخصية أو استخدامها الا في الحالات الخاصة والمتفق عليها في اتفاقية عدم الإفصاح.

1.2.4.27. يجب كتابة استخدام المعلومات الشخصية في العقد المبرم بين **(جهة العمل)** والعملاء.

2.2.4.27. الموظفون المصرح لهم فقط في **(جهة العمل)** يمكنهم الوصول إلى بيانات العملاء الشخصية.

3.2.4.27. إذا استخدمت **(جهة العمل)** المعلومات الشخصية بطريقة مخالفة عن الغرض الذي حدد لها في العقد، فيجب على **(جهة العمل)** طلب الموافقة قبل هذا الاستخدام.

3.4.27. يجب الاحتفاظ ببيانات العميل بما في ذلك شفرة المصدر -إذا تم تقديمها- على خوادم **(جهة العمل)** لمدة 6 أشهر. بعد 6 أشهر يتم حذف بيانات مشروع العميل وشفرة المصدر تلقائيًا، باستثناء أي معلومات وصفية وإجرائية ليست خاصة بالعميل والتي تم استخدامها في المسائل المتعلقة بأعمال **(جهة العمل)**.

4.4.27. **الانتقال الآمن للبيانات:** قد تتعرض البيانات عند نقلها لمخاطر أمنية، لذلك يجب على الموظفين الآتي:

1.4.4.27. تجنب نقل البيانات الحساسة للعملاء إلى أجهزة أو حسابات أخرى ما لم يكن ذلك ضروريًا تمامًا. عند وجود حاجة لنقل جماعي لهذه البيانات، يجب على الموظفين أن يطلبوا المساعدة من إدارة/ قسم أمن المعلومات في **(جهة العمل)**.

2.4.4.27. مشاركة بيانات العملاء عبر شبكة / نظام **(جهة العمل)** وليس عبر شبكة Wi-Fi العامة أو اتصال خاص.

3.4.4.27. التأكد من أن مستلمي البيانات هم الأشخاص أو المؤسسات المصرح لهم بذلك ولديهم سياسات أمان كافية.

4.4.4.27. الإبلاغ عند التعرض لأي تحيل أو خروقات للخصوصية ومحاولات الاختراق.

5.4.27. **الرسائل الترويجية أو الإعلانات:** يجب إخطار العملاء بأن **(جهة العمل)** قد تستخدم معلومات الاتصال الخاصة بهم بإرسال رسائل أو رسائل بريد إلكتروني للتوصية بالمنتجات والخدمات التي قد تهمهم، أو العروض الخاصة أو لإعلامهم بالأحداث القادمة.

27. Customer Data Privacy Policy

27.1. Overview

It is necessary for customers to send different types of data to **(Organization)** Customer Support. Because this data may contain Confidential and / or Sensitive information, it is treated in a special way. Unless otherwise directed by a specific non-disclosure agreement, customer data is treated in the manner described below.

Customer data is problem-specific information provided by the customer in electronic form for purposes of resolving product-related issues.

27.2. Purpose

This policy aims to protect confidential or sensitive data provided by customers in the course of **(Organization)**'s everyday transactions. The protection of customer data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

27.3. Scope

This policy applies to all employees and devices which handles customer data at **(Organization)**.

27.4. Policy

27.4.1. All customer data must be classified as confidential or restricted data, and must be treated as confidential when it is received. Access to this information is restricted to a limited number of personnel on a "need to know" basis. (Including as described in Data Privacy Policy).

27.4.2. **Use of Personal Information:** It is prohibited to use or disclose personal customer data except in special cases that have been agreed on in the non-disclosure agreement.

- 27.4.2.1. Only authorized **(Organization)** employees have access to Personal Information.
- 27.4.2.2. The use of Personal Information must be written in the contract between **(Organization)** and customers.
- 27.4.2.3. If **(Organization)** use Personal Information in a manner different than the purpose for which it was mentioned in the contract, then **(Organization)** will ask for consent prior to such use.

27.4.3. Customer data including source code, if submitted, is held on **(Organization)** servers for 6 months. After 6 months, the customer project data and source code is automatically deleted, except for any descriptive and procedural information which is not customer-specific and which has been taken into use in business-related issues.

27.4.4. **Transfer data securely:** Transferring data introduces security risk. Employees must:

27.4.4.1. Avoid transferring customer sensitive data to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees must ask **(Organization)**'s Information Security Department for help.

27.4.4.2. Share customer data over the **(Organization)** network/ system and not over public Wi-Fi or private connection.

27.4.4.3. Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

27.4.4.4. Report scams, privacy breaches and hacking attempts.

27.4.5. **Promotional Messaging or Advertising:** Customers must be notified that the **(Organization)** may use their contact information send messages or emails to recommend products and services that might be of interest to them, or special offers or to notify them about upcoming events.