مؤسسة الـــروَّاد
للتعاون والتنمية
Al-Rowad Foundation
for Cooperation and Development

RCD-4-9

سياسة أمن المعلومات

Information Security Policy

رقم الإصدار Version No	:	V01
تاريخ الإصدار Issue Date	:	01/06/2026

تحرص مؤسسة الرواد للتعاون والتنمية على إرساء بيئة تنظيمية تقوم على مبادئ الحوكمة، الشفافية، المساءلة، والكفاءة، بما يعزز من جودة الأداء المؤسسي ويضمن تحقيق الأهداف الاستراتيجية للمؤسسة.

وفي هذا السياق، تأتي هذه السياسة كجزء من مجموعة السياسات واللوائح الداخلية التي تنظم العمل في مختلف مجالات المؤسسة، وتحدد الأدوار والمسؤوليات وآليات التنفيذ والرقابة، بما يتماشى مع القيم والمبادئ الأساسية التي تتبناها المؤسسة.

تهدف هذه السياسة إلى توحيد الإجراءات والممارسات، وضمان الالتزام بالمعايير القانونية والتنظيمية والأخلاقية، مع تعزيز ثقافة العمل المؤسسي وتطوير الأداء المستدام.

تم إعداد الإصدار الأول من سياسة أمن المعلومات لمؤسسة الرواد للتعاون والتنمية من قبل مجلس الأمناء، وتم اعتمادها رسمياً من المدير التنفيذي للمؤسسة

1. التعريف بسياسة أمن المعلومات في مؤسسة الرواد للتعاون والتنمية:

تشكل سياسة أمن المعلومات دعامة مهمة في حماية وتأمين البيانات والمعلومات المخزنة عبر مجموعة من المبادئ والتوجهات والإجراءات التي تهدف إلى حماية المعلومات في المؤسسة من التهديدات المحتملة. تشمل هذه السياسة تحديد المسؤوليات وتوضيح كيفية التعامل مع البيانات والمعلومات لضمان سريتها وسلامتها وتوافرها.

2. السياسات:

2.1. سياسة كلمة المرور:

تعد كلمات المرور جانبًا مهمًا من جوانب أمان الكمبيوتر. قد تؤدي كلمة المرور المختارة بشكل سيئ إلى الوصول غير المصرح به و / أو استغلال معلومات وموارد الرواد.

يتحمل جميع المستخدمين، بمن فيهم موظفي الإدارة المركزية وموظفي المراكز ومشاريع المؤسسة والمتطوعين وأصحاب المصلحة الذين لديهم إمكانية الوصول إلى أنظمة ومعلومات الرواد، مسؤولية اتخاذ الخطوات المناسبة على النحو المبين أدناه لاختيار كلمات المرور الخاصة بهم وتأمينها.

إرشادات عامة حول إنشاء كلمة المرور:

- يجب تغيير جميع كلمات المرور على مستوى المستخدم (مثل البريد الإلكتروني وحسابات التطبيقات وجهاز كمبيوتر وما إلى ذلك) كل ثلاثة أشهر على الأقل.
- **استخدم تطبيقاً لإدارة كلمات المرور**: مثل Kaspersky Password Manager المزايا الرئيسية لاستخدام مدير لكلمات المرور تشمل تشفير كلمات المرور وإمكانية الوصول إليها من أي مكان به إنترنت. بعض التطبيقات بها أدوات مدمجة لإنشاء كلمات المرور ولفحص قوة كلمة المرور.
- **تنشيط المصادقة ثنائية العوامل** على جميع الحسابات المهمة التي يتم استخدامها. هذه طريقة أمان إضافية تلي إدخال كلمة المرور بنجاح، كما أنها تستخدم طرقًا لا يملك الوصول إليها إلا المستخدم، مثل البريد الإلكتروني أو الرسائل النصية القصيرة أو البيانات الحيوية (مثل بصمة الإصبع أو بصمة الوجه) أو مفتاح USB تتميز المصادقة ثنائية العوامل بأنها تبقي المستخدم بأمان من المحتالين والمتطفلين، حتى لو تم سرقة كلمة المرور.
- يجب عدك مشاركة كلمات المرور مع أي شخص، بما في ذلك مسؤولي النظام (القسم التقني) أو السكرتارية ما لم يكن هناك مهمة محددة مصرح لهم بها. جميع كلمات المرور يجب أن يتم التعامل معها على أنها معلومات حساسة وسرية
- يجب أن يكون جميع الموظفين والمتطوعين على دراية كافية بكيفية اختيار كلمات مرور قوية. كلمات المرور القوية لها الخصائص التالية:
  - تتكون كلمة المرور على الأقل من 8-10 أحرف وكلما كانت أطول كانت أفضل.
  - أن تكون صعبة التخمين: أن تتجنب الأرقام أو الحروف المتتالية مثل 12345 أو (abcde) تجنب كذلك الكلمات الشائعة مثل ("password1") او أنماط الكلمات والأرقام مثل aaabbb و qwerty و 123321 وما إلى ذلك.
- تحتوي على ثلاثة على الأقل من فئات الأحرف الخمسة التالية:
  - أحرف "خاصة" (مثل @ # $ % ^ & * () _ + | ~ - = \ ` {} [] :" ; ' <> / etc)
  - علامات ترقيم
  - أعداد
  - الأحرف الكبيرة
  - الأحرف الصغيرة
- استخدام قاعدة يصعب على الكمبيوتر تخمينها مثال على ذلك: عبارة تتكون من ثلاث كلمات كل كلمة من 4 حروف مع استبدال أول حرفين من كل كلمة بأرقام ورموز، أي يمكن أن تكون مثلا 4?ee#2ge?6ng بدلاً من"treecagesing" .
- استخدام كلمة مرور مختلفة لكل حساب فاستخدام كلمة مرور واحدة لعدة حسابات يعرض كل هذه الحسابات للخطر.
- يمكن تذكرها: عند تعيين كلمة مرور، احرص على أن تكون لها معنى في رأسك حتى تستطيع تذكرها لكن من الصعب. على الكمبيوتر تخمينها. يمكن تذكر كلمات المرور التي تتكون من حروف وكلمات عشوائية بتدريب الذاكرة عليها وربطها بشيء سهل تذكره، فلا تضع كلمة مرور في غاية الصعوبة لدرجة أنك تنساها بسهولة ولا تتمكن من الوصول إلى حسابك.
- عدم استخدام كلمة مرور شائعة الاستخدام مثل: أسماء العائلة والحيوانات الأليفة والأصدقاء وزملاء العمل والشخصيات الخيالية، تاريخ الميلاد وغيرها من المعلومات الشخصية مثل العناوين وأرقام الهواتف.
- عدم استخدام كلمة مرور موجودة في قاموس (عربي أو أي لغة أخرى).

أخيرًا، على الموظف أن يعلم أنه إذا كانت كلمة المرور سهلة بالنسبة له، فغالبًا ما تكون سهلة بالنسبة للمخترقين أيضًا. كلمات المرور المعقدة هي الطريقة الأفضل لحماية نفسه وجميع حساباته.

2.2. سياسة الاستخدام المقبول:

الإنترنت والأجهزة والأنظمة ذات الصلة بالإنترنت، بما في ذلك أجهزة الكمبيوتر والبرامج وأنظمة التشغيل ووسائط التخزين وحسابات الشبكة وموقع ويب الرواد وصفحات التواصل الاجتماعية وقواعد البيانات، هي ملك للرواد وبالتالي يجب استخدامها للأغراض المتعلقة بالعمل.

يعرّض الاستخدام غير الملائم الرواد لمخاطر مثل هجمات الفيروسات واختراق أنظمة وخدمات الشبكة.

الاستخدام العام والملكية:

- يجب أن يدرك مستخدمو شبكة وحسابات الرواد أن البيانات التي ينشئونها على أنظمة المؤسسة تظل ملكًا لـ الرواد ولا يمكن للإدارة أن تضمن سرية المعلومات الشخصية المخزنة على أي جهاز شبكة ينتمي إلى المؤسسة.
- الموظفون مسؤولون عن ممارسة الحكم الصائب فيما يتعلق بمدى معقولية الاستخدام الشخصي أما قسم تكنولوجيا المعلومات مسؤول عن وضع المبادئ التوجيهية المتعلقة بالاستخدام الشخصي لأنظمة الإنترنت والأجهزة.
- يجب تشفير أي معلومات يعتبرها المستخدمون حساسة أو ضعيفة.
- لأغراض الأمان وصيانة الشبكة، يجوز للأفراد المصرح لهم داخل الرواد مراقبة المعدات والأنظمة وحركة مرور البيانات في أي وقت.
- تحتفظ الرواد بالحق في تدقيق الشبكات والأنظمة على أساس دوري لضمان الامتثال لهذه السياسة.

الاستخدام غير المقبول:

البنود أدناه ليست شاملة بأي حال من الأحوال، ولكنها تحاول توفير إطار للأنشطة التي تندرج في فئة الاستخدام غير المقبول.

- لا يحق لموظف الرواد تحت أي ظرف من الظروف الانخراط في أي نشاط غير قانوني بموجب القوانين المحلية أو الدولية أثناء استخدام موارد الرواد.
- انتهاكات حقوق أي شخص أو شركة محمية بموجب حقوق النشر أو الأسرار التجارية أو براءات الاختراع أو حقوق الملكية الفكرية الأخرى أو القوانين أو اللوائح المماثلة، بما في ذلك، على سبيل المثال لا الحصر، تثبيت أو توزيع منتجات البرامج "المقرصنة" أو غيرها من المنتجات غير مرخصة.
- النسخ غير المصرح به للمواد المحمية بحقوق الطبع والنشر بما في ذلك، على سبيل المثال لا الحصر، رقمنة وتوزيع الصور من المجلات أو الكتب أو المصادر الأخرى المحمية بحقوق الطبع والنشر، والموسيقى المحمية بحقوق الطبع والنشر، وتثبيت أي برنامج محمي بحقوق الطبع والنشر لا تملك الرواد أو المستخدم النهائي ترخيصًا نشطًا له. يمنع منعا باتا.
- إدخال برامج ضارة إلى الشبكة أو الخادم (على سبيل المثال، الفيروسات والديدان وأحصنة طروادة وقنابل البريد الإلكتروني وما إلى ذلك).
- الكشف عن كلمة مرور حساب الموظف للآخرين أو السماح للآخرين باستخدام حسابه، وهذا يشمل العائلة وأفراد الأسرة الآخرين عندما يتم العمل في المنزل.
- استخدام أصول وأجهزة المؤسسة للمشاركة بنشاط يتضمن شراء أو نقل المواد التي تروج للتحرش الجنسي أو كافة أشكال الإساءة الجنسية.
- تقديم عروض احتيالية للمنتجات أو العناصر أو الخدمات من أي حساب من حسابات الرواد.
- الإدلاء ببيانات حول المؤسسة، صراحةً أو ضمنًيا، ما لم يكن جزءًا من واجبات الوظيفة العادية او بتصريح رسمي.
- إحداث خروقات أمنية أو تعطل اتصال الشبكة. تشمل الانتهاكات الأمنية، على سبيل المثال لا الحصر، الوصول إلى البيانات التي لا يكون الموظف الوصول لها أو تسجيل الدخول إلى خادم أو حساب غير مصرح للموظف صراحة بالوصول إليه، ما لم تكن هذه الواجبات ضمن نطاق المهام العادية. لأغراض هذا القسم، يشمل "التعطيل" ، على سبيل المثال لا الحصر ، رفض الخدمة ، ومعلومات التوجيه المزورة لأغراض ضارة.
- يُحظر صراحة فحص المنافذ أو الفحص الأمني ما لم يتم إخطار قسم تكنولوجيا المعلومات في الرواد مسبقًا.
- تنفيذ أي شكل من أشكال مراقبة الشبكة الذي سيعترض البيانات غير المخصصة للموظف، ما لم يكن هذا النشاط جزءًا من الوصف الوظيفي للموظف.
- التحايل على مصادقة المستخدم، أو أمان أي مضيف، أو شبكة أو حساب. استخدام أي برنامج / نص / أمر، أو إرسال رسائل من أي نوع بقصد التدخل في الأنظمة والحسابات، عبر أي وسيلة، محليًا أو عبر الإنترنت.

2.3. 3. سياسة التدوين ووسائل التواصل الاجتماعي:

يخضع التدوين واستخدام تطبيقات التواصل الاجتماعي من قبل الموظفين، سواء باستخدام موارد وأنظمة الرواد أو أنظمة الكمبيوتر الشخصية، أيضًا للشروط والقيود المنصوص عليها في هذه السياسة.

من المقبول الاستخدام المحدود لأنظمة الرواد للمشاركة في التدوين، شريطة أن يتم ذلك بطريقة مهنية ومسؤولة، والتي لا تنتهك سياسة الرواد، لا تضر بمصالح الرواد الفضلى، ولا تتداخل مع واجبات العمل للموظف العادي.

- تنطبق سياسة حماية المعلومات للرواد أيضًا على التدوين واستخدام وسائل التواصل الاجتماعي. على هذا النحو، يُحظر على الموظفين الكشف عن أي معلومات سرية، أو ملكية، أو أسرار تجارية، أو أي مواد أخرى تغطيها شروط السرية في دليل الموارد البشرية.
- لا يجوز للموظفين المشاركة في أي مدونات أو صفحات أو مجموعات قد تضر أو تشويه الصورة وسمعة وحسن النية للرواد أو أي من موظفيها. يُحظر على الموظفين أيضًا تقديم أي تعليقات تميزية، أو مستهلكة، أو تشهيرية، أو مضايقة عند التدوين.
- لا يجوز للموظفين أيضًا أن يعزو البيانات الشخصية أو الآراء أو المعتقدات إلى مؤسسة الرواد عند المشاركة في التدوين. إذا كان الموظف يعبر عن معتقداته أو آرائه الشخصية في وسائل التواصل الاجتماعي، فلا يجوز للموظف، صراحة أو ضمنية، أن يمثل أنفسهم كموظف أو ممثل للمؤسسة.
- لا يتم استخدام اللوغو الخاص بالمؤسسة والشعارات وأي ملكية فكرية أخرى للرواد بشكل غير مصرح به في وسائل التواصل الاجتماعي.

2.4. سياسة استخدام البريد الالكتروني:

تصف سياسة البريد الإلكتروني هذه القواعد والإرشادات التي تحكم إدارة واستخدام خدمات البريد الإلكتروني في مؤسسة الرواد.

2.4.1. الاستخدام المحظور:

لا يجوز استخدام نظام البريد الإلكتروني الخاص بالرواد لإنشاء أو توزيع أي رسائل تخريبية أو مسيئة، بما في ذلك التعليقات المسيئة حول العرق، أو الجنس، أو لون الشعر أو الإعاقة أو العمر أو المواد الإباحية أو المعتقدات والممارسات الدينية أو المعتقدات السياسية أو الأمن القومي. يجب على المستخدمين الذين يتلقون أي رسائل بريد إلكتروني تحتوي على هذا المحتوى من أي موظف في الرواد إبلاغ المشرف على الفور بالمسألة.

2.4.2. الاستخدام الشخصي:

يعد استخدام قدر معقول من موارد المؤسسة لرسائل البريد الإلكتروني الشخصية أمرًا مقبولاً، ولكن يتم حفظ البريد الإلكتروني غير المتعلق بالعمل في مجلد منفصل عن البريد الإلكتروني المتعلق بالعمل.

2.4.3. المراقبة:

يجوز لقسم تكنولوجيا المعلومات في الرواد مراقبة الرسائل دون إشعار مسبق بشرط وجود تفويض كتابي من المدير التنفيذي أو الامتثال للمتطلبات القانونية.

2.4.4. آداب البريد الإلكتروني العامة:

فيما يلي بعض النصائح لضمان استخدام نظام البريد الإلكتروني للرواد بكفاءة واحترافية:

- عند صياغة بريد إلكتروني جديد، يجب القيام فقط بتضمين المستلمين المعنيين. يجب أن يسترشد ذلك بمحتوى البريد الإلكتروني وبروتوكول الإبلاغ الخاص بالمنصب الوظيفي.
- عند الرد على رسالة بريد إلكتروني، يجب تمييز الفرق بين الرد والرد على الكل. الرد على الكل مفيد فقط في الحالات التي تكون فيها الملاحظات ضرورية وذات صلة بجميع مستلمي البريد.
- استخدم BCC و CC بشكل مناسب. يقوم كل من CC و BCC بإعادة توجيه نسخة من الرسالة إلى جميع المدرجين في القائمة. الاختلاف الرئيسي هو أنه مع BCC ، لا يتمكن المستلمون من الوصول إلى بعضهم البعض.
- يجب دائمًا تضمين موضوع ذي معنى. يمكن أن يؤدي عدم وجود موضوع ذي مغزى إلى جعل المستلم يتجاهل البريد الإلكتروني أو يصنفه على أنه بريد عشوائي / غير هام.
- يجب عدم الكتابة بأحرف كبيرة وتجنب تغميق الخط (bold)غير الضروري.
- ينصح بإعادة قراءة البريد الإلكتروني قبل إرساله لتجنب الأخطاء المطبعية.
- عدم القيام بإرفاق ملفات غير ضرورية، وعدم نسيان إرفاق ملفات إذا كان من المفترض أن يحتوي البريد الالكتروني عليها مع إعطاء المرفقات أسماء ذات مغزى.
- ينصح بعدم الافراط في استخدام خيار الأولوية العالية وتجنب الإفراط في الاستخدام العاجل والمهم.
- يجب الحذر عند استخدام الاختصارات والرموز التعبيرية ويجب استخدام لغة محايدة.

- يجب تجنب فتح رسائل البريد الإلكتروني العشوائية أو الرد عليها أو إعادة توجيهها. يشير البريد العشوائي إلى رسائل البريد الإلكتروني غير المرغوب فيها. والذي قد يطلب منك النقر فوق ارتباط من أجل: تنزيل بعض المحتوى، والمطالبة بمكافأة في المسابقات التي لم تشارك فيها، وإزالة فيروس من جهاز الكمبيوتر، والتحقق من البريد الإلكتروني وإلغاء حظره، إلخ.
- يقوم قسم تكنولوجيا المعلومات بتكوين البريد الإلكتروني للمؤسسة على الأجهزة الخاصة بالموظفين، ولكن المستخدمين مسؤولون عن الأنشطة المنبثقة عن الحساب الذي تم إنشاؤه.

2.5. سياسة استخدام الإنترنت

بسبب الحاجة لاستخدام شبكة الإنترنت بشكل متزايد في عمل المؤسسة، هناك حاجة إلى توفير إرشادات أساسية تنظم استخدامها من أجل تجنب إساءة الاستخدام. في حين أنها أداة مهمة أدت إلى كفاءة وتحسين جودة الخدمة في العديد من المنظمات، إلا أنها قد تكون أيضًا مصدرًا لسوء أداء الموظفين إذا لم تتم إدارتها بشكل جيد. توضح هذه السياسة إرشادات الاستخدام للموظفين.

2.5.1. الاستخدام المسموح به:

يتم منح استخدام الإنترنت لغرض وحيد هو دعم الأنشطة اللازمة لتنفيذ وظائف العمل. يجب على جميع المستخدمين اتباع مبادئ الشركة فيما يتعلق باستخدام الموارد وممارسة الحكم السليم في استخدام الإنترنت. يمكن توجيه الأسئلة إلى قسم تكنولوجيا المعلومات.

قد يشمل الاستخدام المقبول للإنترنت لأداء وظائف العمل ما يلي:

- التواصل بين الموظفين داخليا او مع جهات خارجية كالمانحين لأغراض العمل.
- الدعم الفني لتكنولوجيا المعلومات عن طريق تنزيل ترقيات وتصحيحات البرامج وتنزيل التطبيقات اللازمة للقيام بالعمل.
- مراجعة مواقع الويب للموردين المحتملين للحصول على معلومات عن المنتجات.
- استخراج معلومات تنظيمية أو تقنية مرجعية.
- أغراض البحث الخاص بأمور العمل.

2.5.2. الاستخدام الشخصي:

المستخدمون الذين يختارون تخزين أو نقل المعلومات الشخصية مثل المفاتيح الخاصة أو أرقام بطاقات الائتمان أو الشهادات أو يستخدمون "محافظ" الإنترنت يفعلون ذلك على مسؤوليتهم الخاصة.

الرواد ليست مسؤولة عن أي فقدان للمعلومات، مثل المعلومات المخزنة في المحفظة، أو أي خسارة تبعية للممتلكات الشخصية.

2.5.3. الاستخدام المحظور:

يُحظر على وجه التحديد اقتناء وتخزين ونشر البيانات غير القانونية أو ذات الطبيعة الإباحية أو التي تصور بشكل سلبي العرق أو الجنس أو العقيدة.

إجراء مشروع تجاري أو نشاط سياسي أو الانخراط في أي شكل من أشكال جمع المعلومات الاستخبارية من مكاتب ومراكز الرواد أو الانخراط في أنشطة احتيالية أو نشر مواد كاذبة أو تشهيرية عن عمد.

تشمل الأنشطة الأخرى المحظورة تمامًا، على سبيل المثال لا الحصر:

- تنزيل أي برنامج وتثبيته على أجهزة الكمبيوتر الخاصة بالرواد أو تغيير التكوين على أي جهاز من دون موافقة قسم تكنولوجيا المعلومات.
- يجب أن تكون جميع البرامج المثبتة بواسطة قسم تكنولوجيا المعلومات مرخصة بشكل مناسب.
- يحظر على الموظفين عمل نسخ من أي برامج مملوكة لمؤسسة الرواد
- الوصول إلى معلومات الرواد التي لا تدخل في نطاق عمل الفرد. يتضمن ذلك القراءة غير المصرح بها لمعلومات الحساب والوصول غير المصرح به إلى معلومات ملف الموظفين، والوصول إلى المعلومات غير الضرورية للتنفيذ السليم لوظائف الوظيفة.
- إساءة استخدام المعلومات الشخصية أو الإفصاح عنها دون الحصول على إذن مناسب أو تغييرها. يتضمن ذلك إجراء تغييرات غير مصرح بها على ملف الموظفين أو مشاركة بيانات المستفيدين أو الموظفين الإلكترونية مع موظفين غير مصرح لهم.
- تعمد الإشارة أو الربط التشعبي لمواقع الويب الخاصة بـ الرواد إلى مواقع الإنترنت الأخرى التي قد يكون محتواها غير متوافق مع أو ينتهك أهداف أو سياسات المؤسسة.

- أي سلوك من شأنه أن يشكل جريمة جنائية أو يشجع عليها، أو يؤدي إلى مسؤولية مدنية، أو ينتهك بأي شكل من الأشكال أي أنظمة ، أو قانون محلي ، أو حكومي ، أو وطني ، أو دولي.
- استخدام، أو نقل، أو نسخ أو استلام طوعي لمواد تنتهك حقوق الطبع والنشر أو العلامات التجارية أو الأسرار التجارية أو حقوق براءات الاختراع لأي شخص أو مؤسسة. افترض أن جميع المواد الموجودة على الإنترنت هي حقوق طبع ونشر و / أو براءة اختراع ما لم تنص إشعارات محددة على خلاف ذلك.
- نقل أي معلومات ملكية أو سرية أو غير ذلك من المعلومات الحساسة دون الضوابط المناسبة.
- إنشاء أو نشر أو نقل أو استلام طوعي لأي مواد غير قانونية أو مسيئة أو تشهيرية أو تهديدية أو مضايقة، بما في ذلك على سبيل المثال لا الحصر التعليقات القائمة على العرق أو الأصل القومي أو الجنس أو العمر أو الإعاقة أو الدين أو المعتقدات السياسية.
- أي شكل من أشكال القمار.
- تنزيل غير مصرح به لأية برامج أو ملفات تجريبية لاستخدامها دون إذن مسبق من قسم تكنولوجيا المعلومات.
- أي تسوق عبر الإنترنت للعناصر أو الخدمات.
- ممارسة الألعاب.
- إعادة توجيه الرسائل المتسلسلة.
- المشاركة في أي مسابقة عبر الإنترنت أو ترويج وقبول الهدايا الترويجية.

2.6. سياسة حماية سرية البيانات والبريد الالكتروني:

يجب على الموظفين الذين يستخدمون حسابات وأنظمة الرواد مراعاة حساسية المعلومات، بما في ذلك المعلومات الشخصية المحمية التي يمكن الوصول إليها وتقليل إمكانية الوصول غير المصرح به.

ستقوم الرواد بتنفيذ الضمانات المادية والتقنية لجميع أجهزة العمل التي تصل إلى المعلومات المحمية لتقييد الوصول إلى المستخدمين المصرح لهم.

تشمل التدابير المناسبة ما يلي:

- تقييد الوصول المادي إلى أجهزة العمل على الموظفين المصرح لهم فقط.
- تأمين أجهزة العمل (قفل الشاشة أو تسجيل الخروج) قبل مغادرة المنطقة لمنع الوصول غير المصرح به.
- تمكين شاشة توقف محمية بكلمة مرور مع مهلة قصيرة لضمان حماية أجهزة العمل التي تُركت غير آمنة
- الامتثال لجميع سياسات وإجراءات كلمات المرور المعمول بها.
- ضمان استخدام أجهزة العمل للأغراض المصرح بها فقط.
- يجب أن تكون جميع عمليات تثبيت البرامج في أجهزة العمل مصرحًا بها صراحةً من قبل قسم تكنولوجيا المعلومات.
- تخزين جميع المعلومات الحساسة، بما في ذلك المعلومات الشخصية المحمية على خوادم الشبكة المحمية
- إبعاد الطعام والشراب عن أجهزة العمل لتجنب الانسكابات العرضية.
- تأمين أجهزة الكمبيوتر المحمولة التي تحتوي على معلومات حساسة باستخدام أقفال الكابلات أو قفل أجهزة الكمبيوتر المحمولة في الأدراج أو الخزانات.
- التأكد من أن جميع الأجهزة المحمولة تستخدم تقنية التشفير
- التأكد من تأمين جميع أجهزة العمل باستخدام برنامج مكافحة الفيروسات المحدث.
- التأكد من وضع الشاشات بعيدًا عن العرض العام. إذا لزم الأمر، فقم بتثبيت فلاتر شاشة الخصوصية أو غيرها من الحواجز المادية أمام المشاهدة العامة.
- تثبيت جدران الحماية وأجهزة توجيه VLAN لمنع القرصنة.
- تثبيت برنامج مكافحة الفيروسات وتحديثه للسماح بمسح الرسائل الواردة والصادرة
- استخدم جدار حماية ثنائي الاتجاه، والذي يمنع حركة المرور الواردة والصادرة غير المرغوب فيها.
- تجنب خلط العديد من برامج جدار الحماية أو برامج مكافحة الفيروسات لأن هذا لن يعطي المزيد من الحماية.
- السماح بالتحديثات التلقائية لحل مشكلات الأمان بمجرد العثور عليها.
- عدم الثقة في تنبيهات الأمان المنبثقة أثناء تصفح الإنترنت
- التأكد من إغلاق أجهزة العمل بعد ساعات العمل.
- إذا تم استخدام الوصول إلى الشبكة اللاسلكية، فتأكد من أن الوصول آمن. يجب إخفاء SSIDs.
- الإجراءات التالية محظورة:

- إرسال رسائل بريد إلكتروني غير مرغوب فيها، بما في ذلك إرسال "بريد غير هام" أو مواد إعلانية أخرى إلى الأفراد الذين لم يطلبوا هذه المواد على وجه التحديد (البريد الإلكتروني العشوائي).
- أي شكل من أشكال المضايقات عبر البريد الإلكتروني والهاتف، سواء من خلال اللغة أو التردد أو حجم الرسائل.
- الاستخدام غير المصرح به أو تزوير معلومات البريد الإلكتروني.
- إنشاء أو إعادة توجيه "رسائل متسلسلة" أو "سبام" أو مخططات "هرمية" أخرى من أي نوع.
- نشر نفس الرسائل غير المتعلقة بالعمل أو ما شابه ذلك إلى عدد كبير من مجموعات أخبار (البريد العشوائي لمجموعة الأخبار).
- نسخ رسالة أو مرفق غير مصرح به.
- الرد على البريد العشوائي أو النقر على الروابط للمطالبة بجوائز في مسابقات لم تشارك فيها.

2.7. سياسة النسخ الاحتياطي:

يمكن للكوارث أن تضرب في أي وقت وتحتاج الرواد إلى تقليل المخاطر في مثل هذه الحوادث من خلال إنشاء إجراءات النسخ الاحتياطي للبيانات والحفاظ عليها. يضمن النسخ الاحتياطي المنتظم والدوري توفر نسخ من أنظمة المعلومات والبيانات في حالة حدوث أي كارثة أو مشكلة أو فشل في النظام.

تحدد هذه السياسة سياسة الرواد تجاه الاحتفاظ بنسخ احتياطية من أصول المعلومات الخاصة بها ، بما في ذلك تكرار النسخ الاحتياطية وتخزين المعلومات والاحتفاظ بها بالإضافة إلى إجراءات التوثيق واستعادة النسخ الاحتياطية.

- يجب إجراء النسخ الاحتياطي للمعلومات والبرامج التجارية الأساسية وفقًا لجدول زمني شامل وموثق جيدًا.
- يجب توفير مرافق احتياطية مناسبة لضمان إمكانية استرداد جميع المعلومات والبرامج الأساسية بعد وقوع كارثة أو فشل في الوسائط.
- يجب عمل نسخة احتياطية من جميع التطبيقات وأنظمة التشغيل والبيانات (بما في ذلك قواعد البيانات) ومعلومات تكوين المستخدم ومعلومات تكوين الأجهزة (إن أمكن) وفقًا لإجراءات النسخ الاحتياطي والاستعادة
- يجب تطوير إجراءات النسخ الاحتياطي والاستعادة الخاصة بالأنظمة الإضافية وفقًا لمتطلبات النظام وتوصيات البائع. يجب توثيق هذه الإجراءات وتنفيذها أثناء (وكجزء من) تنفيذ النظام.
- سيتم تحديد إجراء النسخ الاحتياطي والاستعادة من قبل قسم تكنولوجيا المعلومات بناءً على نوع النسخ الاحتياطية التي سيتم إجراؤها، وتواتر النسخ الاحتياطي أو جدوله، والحماية التي سيتم توفيرها لوسائط النسخ الاحتياطي.
- تتطلب استعادة النسخ الاحتياطية تفويضًا محددًا ومناسبًا ويجب إجراؤها وفقًا لإجراء النسخ الاحتياطي والاستعادة
- يجب فحص إجراءات الاستعادة بانتظام (على أساس سنوي على الأقل) واختبارها للتأكد من أنها فعالة وأنه يمكن إكمالها في غضون الوقت المخصص في الإجراءات التشغيلية للاسترداد
- يجب جدولة النسخ الاحتياطية الكاملة للخادم مرتين في الأسبوع بينما يجب نسخ التطبيقات المهمة احتياطيًا كل يوم.
- يجب تخزين أشرطة النسخ الاحتياطي للتخزين خارج الموقع في مكان آمن خارج الموقع بشكل دوري اعتمادًا على مدى أهمية البيانات حتى تكون متاحة بسهولة في حالة وقوع كارثة أو للتخزين طويل الأجل.
- يجب الاحتفاظ بنسخ احتياطية لجميع البيانات لمدة لا تقل عن 30 يومًا لضمان استعادة الأنظمة بالكامل.
- يجب تحديد فترة الاحتفاظ وأي شرط للاحتفاظ بنُسخ أرشيفية لفترات أطول (أو بشكل دائم) بشكل رسمي لمعلومات العمل الهامة وكذلك بناءً على أي متطلبات قانونية
- يجب أن تتضمن وثائق النسخ الاحتياطي تحديد جميع البيانات الهامة والبرامج والوثائق وعناصر الدعم التي ستكون ضرورية لأداء المهام الأساسية خلال فترة الاسترداد.
- يجب على مسؤولي الأنظمة إجراء عملية تحقق على بيانات النسخ الاحتياطي للتأكد من نسخها احتياطيًا بنجاح.
- يجب على مسؤولي الأنظمة إجراء نسخ احتياطي قبل وبعد تثبيت التصحيحات أو الترقيات أو إجراء أي تغييرات تكوين على النظام.
- يجب تخزين البيانات الاحتياطية السرية في شكل مشفر.
- يجب على مسؤولي الأنظمة التحقق من جودة وسائط النسخ الاحتياطي (الأشرطة ومفاتيح USB وأقراص DVD والأشرطة وما إلى ذلك) شهريًا والتأكد من أنها في حالة جيدة لإعادة استخدامها.
- بعد الانتهاء من اختبار النسخ الاحتياطي، يجب محو جميع البيانات بأمان من بيئة الاختبار.
- مسؤولو النظام مسؤولون عن اختبار برامج النظام والنسخ الاحتياطية للبيانات عن طريق استعادة عينة من النسخ الاحتياطية وفقًا لجدول رسمي في بيئة الاختبار.
- سيكون مدير قسم تكنولوجيا المعلومات مسؤولاً عن التحكم في اختبار النسخ الاحتياطي والإشراف عليه.

- يجب تخزين الحد الأدنى من المعلومات الاحتياطية، جنبًا إلى جنب مع السجلات الدقيقة والكاملة للنسخ الاحتياطية وإجراءات الاستعادة الموثقة، في مكان بعيد، على مسافة كافية من مكاتب مؤسسة الرواد ومرافق المعالجة الأخرى لتجنب الضرر الناجم عن كارثة في الموقع الرئيسي.
- يجب عمل نسختين على الأقل من الإصدارات القابلة للاسترداد بالكامل لجميع البيانات الهامة. يجب تخزين نسخة واحدة في مركز البيانات أو مرفق المعالجة الرئيسي بينما يجب تخزين النسخة الأخرى في موقع تخزين خارج الموقع.
- يجب تسمية كل وسائط نسخ احتياطي بشكل مناسب مع ذكر تفاصيل المالك والتاريخ وطبيعة النسخ الاحتياطي.
- يجب تكويد جميع وسائط النسخ الاحتياطي التي سيتم نقلها من مركز البيانات أو مرفق المعالجة الرئيسي إلى موقع خارج الموقع.
- يجب إنشاء خطة طوارئ لإجراءات استعادة وحماية المعلومات والأنظمة والبنية التحتية في حالة وقوع كارثة قد تتضمن ما يلي:
  - خطة الاستجابة للطوارئ الحاسوبية: التفاصيل - بمن يتم الاتصال به ومتى؟ وكيف؟ ما هي الإجراءات الفورية التي يجب اتخاذها في حالة حدوث ذلك؟
  - دراسة البيانات: تفصيل البيانات المخزنة في الأنظمة وأهميتها وصفاتها.
  - قائمة الخدمات: ضع قائمة بجميع الخدمات المقدمة وترتيب أهميتها. كما يشرح ترتيب الاسترداد في كل من الأطر الزمنية قصيرة الأجل وطويلة الأجل.
  - خطة النسخ الاحتياطي واستعادة البيانات: قم بتفصيل البيانات التي تم نسخها احتياطيًا، والوسائط التي تم حفظها بها، ومكان تخزين هذه الوسائط، وعدد مرات إجراء النسخ الاحتياطي. يجب أن يصف أيضًا كيفية استرداد هذه البيانات.
  - خطة استبدال المعدات: صِف المعدات المطلوبة لبدء تقديم الخدمات، واذكر الترتيب المطلوب، ولاحظ مكان شراء المعدات.
- بعد إنشاء خطط الطوارئ، يجب على الإدارة تخصيص وقت لاختبار تنفيذها بحيث يمكن اكتشاف المشكلات التي قد تتسبب في فشل الخطة وتصحيحها في بيئة لها عواقب قليلة
- في حالة وقوع كارثة، يمكن استخدام خطط الطوارئ ذات الصلة لإعادة الوضع إلى طبيعته.
- يُطلب من جميع المستخدمين قراءة سياسات ومعايير وإجراءات أمن المعلومات الأخرى وفهمها والامتثال لها.

2.8. سياسة التدريب على أمن تكنولوجيا المعلومات:

- يتم تقديم استراتيجية التوعية بأمن المعلومات من خلال طرق متعددة تهدف إلى زيادة وعي المستخدم.
- توفير دورات تدريبية إلزامية ومجدولة للتوعية الأمنية.
- عند تعيين موظفين جدد يتم اطلاعهم على سياسة حماية البيانات وسياسة الاستخدام المقبول لتكنولوجيا المعلومات.