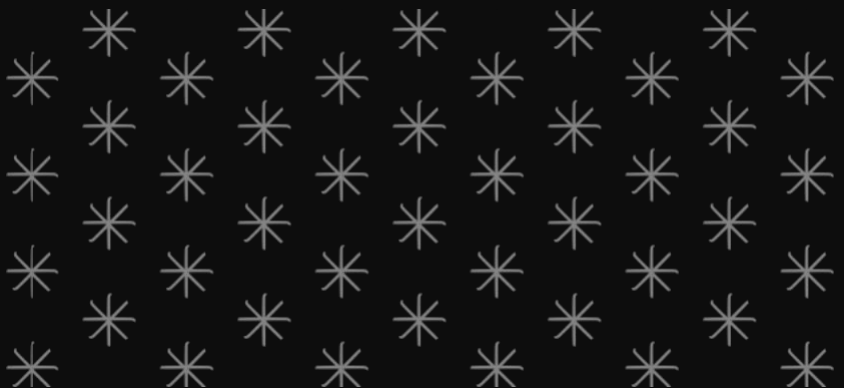
IT1-09-R0

mafs | مَـودة
جـمـعـيـة مـــودة للاســتــقـــرار الأســـري
MAWADDAH ASSOCIATION FOR FAMILY STABILITY

سياسات أمن المعلومات



رقم الإصدار	تاريخ الإصدار	الاعتماد
الإصدار الأول	27 سبتمبر 2021م	بقرار مجلس إدارة رقم 6

جدول المحتويات

تمهيد

تبنت جمعية مودة الخيرية وآثاره متمثلة برئيسة مجلس الإدارة وكافة العاملين بها نظام إدارة امن المعلومات وهو المعيار الدولي الذي يوضح كيفية وضع نظام إدارة أمن المعلومات بشكل معتمد وتطبيقه والحفاظ عليه وتحسينه باستمرار ضمن أطر عملية مما يسمح بالحفاظ على البيانات الحساسة والسرية بشكل آمن والتقليل من احتمال الوصول إليها بشكلٍ غير قانوني أو بدون إذن كما يسمح بإدارة المخاطر الأمنية واسترداد المعلومات وتقليل الخروقات الأمنية.ومن هذا المنطلق يأتي إعداد هذا الدليل ليتلاءم ومواصفة الآيزو ISO27001، وليسلط الضوء على نظام إدارة امن المعلومات في مودة.

قسم تقنية المعلومات في جمعية مودة

المجال

حرصاً من جمعية مودة الخيرية واثاره على تطوير أداءها وتحسين خدماتها المقدمة للمستفيدين ولجميع الجهات ذات العلاقة، سعيا وراء تحقيق رضا هذه الأطراف وتجاوز تطلعاتها، فقد حرصت مودة على تطبيق المواصفة الدولية الأيزو ISO27001 في سبيل تحقيق هذه الغاية.

التعريفات والمصطلحات

يكون للكلمات التالية الدلالات المعرفة بها حيثما وردت في الدليل:

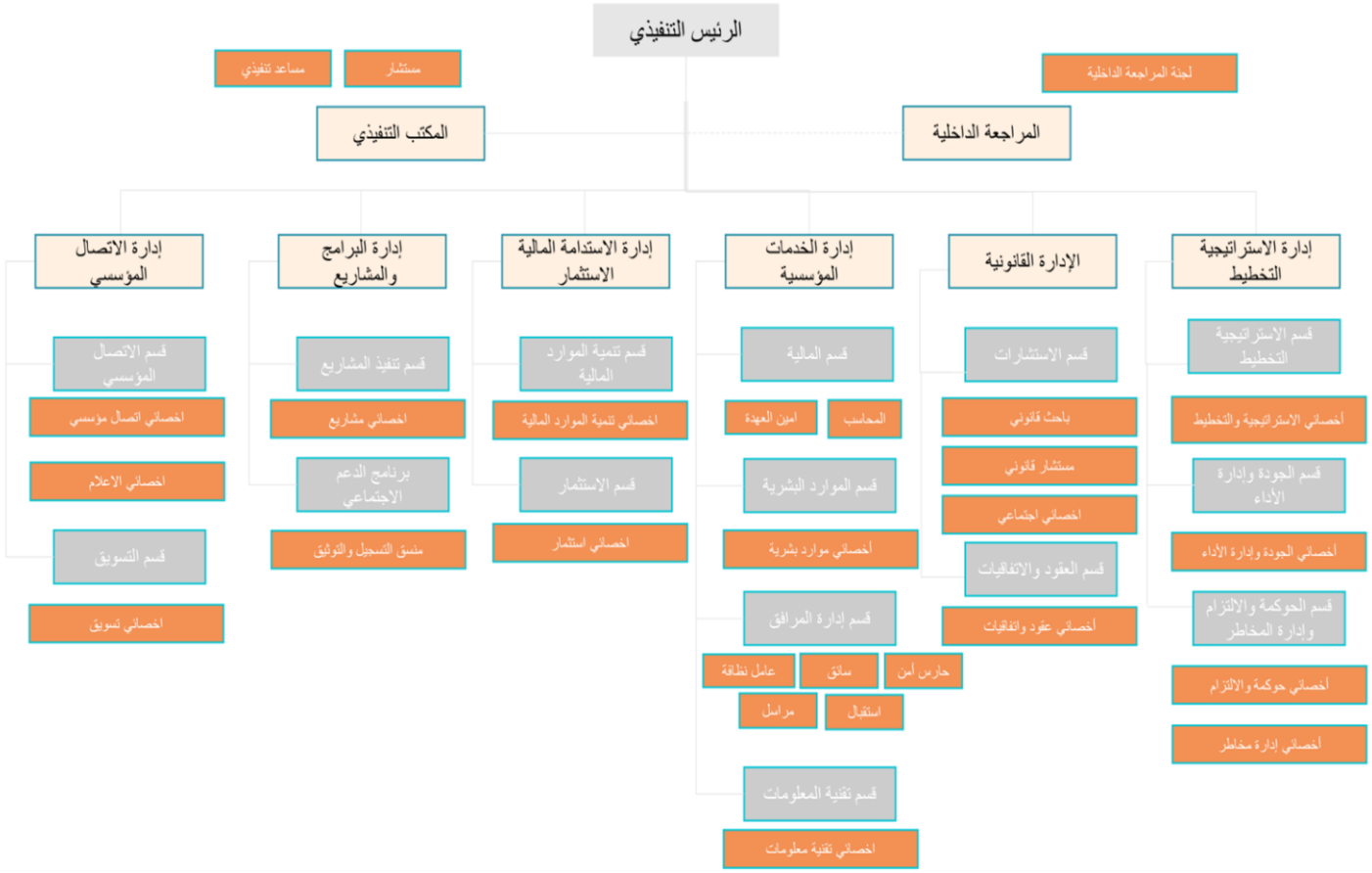
مودة	جمعية مودة مرخصة من وزارة الشؤون الاجتماعية و فرعها الرئيسي في الرياض .
السياسات	التزام الإدارة العليا والعاملين في مودة بمبادئ امن المعلومات تنطبق هذه السياسات على جميع الموظفين، والموردين، وشركاء العمل، وموظفي المقاولين، والوحدات الوظيفية لدى الجمعية دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
الإجراءات	يصف شيئاً يجب إنجازه أو نقطة من النقاط المستهدف الوصول إليها، وينبغي أن يكون الهدف ذكيا smart، أي انه:(قابل للقياس -واقعي -محدد -مرتبط بزمن).

سياق جمعية مودة

مجال عمل مودة: مودة جمعية تنموية متخصصة تعني باستقرار الأسرة السعودية وصحتها، وتهدف الى الحد من نسب الطلاق في المجتمع السعودي ومعالجة آثاره عبر برامج تنموية اجتماعية وحقوقية مستدامة.

الموقع: تقع مودة في مدينة الرياض عاصمة المملكة العربية السعودية.

الهيكل: تتكون مودة من مجموعة من الإدارات حسب ما هو موضح في الهيكل التنظيمي.



سياق جمعية مودة

نبذة عن الجمعية:

منظمة غير ربحية تهدف إلى الاستقرار الأسري في المجتمع السعودي.

الرسالة:

القيادة المجتمعية لدعم وتمكين الأسرة عبر تقديم مبادرات نوعية ذات طابع تنموي.

الرؤية:

تمكين الأسر لمجتمع متماسك ومستدام.

متطلبات نظام إدارة أمن المعلومات(ISMS)

تسمى تقنية المعلومات جنبًا إلى جنب مع أنظمة المعالجة والبنية التحتية الخاصة بها أصول تقنية المعلومات وهذا يضيف قيمة إلى جمعية مودة وبالتالي، يجب حمايتها بشكل مناسب. يقوم أمن المعلومات بحماية المعلومات من مجموعة واسعة من التهديدات من أجل ضمان استمرارية الأعمال، وتقليل أضرار الأعمال الحالية، وفرص الأعمال المستقبلية.

نظام إدارة أمن المعلومات (ISMS) مطلوب لجمعية مودة وهو مدعوم من قبل الإدارات الأخرى مثل إدارة الموارد البشرية وإدارة الشؤون المالية وإدارة الشؤون القانونية والتي توفر الالتزام والامتثال والتي تقود مع وظائف الدعم الأخرى للجمعية إلى تحقيق أهداف أعمالها بطريقة آمنة ووفق جدول مناسب. يوضح إنشاء نظام إدارة أمن المعلومات (ISMS) الخاص بالمعيار الدولي أيزو 27001:2013 التزام الجمعية بحماية أصول تقنية المعلومات. حيث يجب أن يمتد هذا الالتزام الى كل موظف مشارك في العمليات اليومية لتقنية المعلومات وإلى أصحاب المصلحة الآخرين مثل العملاء وشركاء الأعمال والموردين الخارجيين الذين يستخدمون أنظمة تقنية معلومات جمعية مودة.

التزام الإدارة التنفيذية ومقاصدها

تدعم الإدارة التنفيذية في جمعية مودة أهداف ومبادئ نظام إدارة أمن المعلومات وتلتزم (ISMS) برعاية وتنفيذ السياسات والممارسات في حماية جميع أصول تقنية المعلومات الموجودة لديها أو في عهدتها. يجب أن تضمن اللجنة التوجيهية الإدارية في جمعية مودة ما يلي:

1. التأكد من أن سياسة وأهداف أمن المعلومات تتوافق مع التوجهات الاستراتيجية جمعية مودة.
2. التأكد من أن جميع الالتزامات القانونية والتنظيمية والتعاقدية للجمعية قد تم تحديدها بشكل واضح وأنه قد تم الالتزام بها.
3. تخصيص الموارد اللازمة لنظام إدارة أمن المعلومات.
4. التأكد من أن نظام إدارة أمن المعلومات يحقق النتائج المقصودة والمرجوة منه.

متطلبات نظام إدارة أمن المعلومات(ISMS)

5. يوفر التوجيه الاستراتيجي ويقوم بتقديم الدعم لتطوير وإنشاء نظام إدارة أمن المعلومات.
6. تضمن التطوير والتحسين المستمر لنظام إدارة أمن المعلومات.
7. التأكد من إبلاغ السياسات والإجراءات إلى المهتمين وأصحاب المصلحة والعلاقة.

مراجعة نظام أمن المعلومات

يمكن أن توجد المعلومات إما بشكل مطبوع أو إلكتروني، أو يتم نقلها، أو عرضها على وسائل الإعلام، أو التحدث بها في محادثة هاتفية. ومع ذلك، بغض النظر عن شكل ونموذج المعلومات، أو الوسائل التي يتم من خلالها مشاركتها أو تخزينها، يجب دائمًا القيام بحمايتها بشكل مناسب.

يعد نظام إدارة أمن المعلومات (ISMS)جزءًا من نظام الإدارة الشامل للجمعية، واستنادًا إلى نهج وإطار إدارة المخاطر، لإنشاء وتنفيذ وتحسين أمن المعلومات باستمرار في الهيئة. يوفر معيار (ISO / IEC 27001: 2013) دليلًا إرشاديًا لتطوير هيكل عمل أو نظام لتطوير وتنفيذ وإدارة أمن المعلومات داخل الجمعية.

يتحقق نظام إدارة أمن المعلومات (ISMS) في جمعية مودة من خلال إنشاء بنية تنظيمية، وتنفيذ مجموعة مناسبة من الضوابط والتي تتكون من سياسات وإجراءات ومبادئ توجيهية. تم وضع هذه الضوابط لضمان تحقيق أهداف امن المعلومات المحددة للجمعية. تقود الركائز الأساسية التالية إلى تكوين إطار عمل ضمن نظام أمن المعلومات والسياسات الأمنية في جمعية مودة

1. السرية تتعلق بحماية المعلومات الحساسة والهامة من الإفشاء أو الكشف أو الوصول غير المصرح به.
2. النزاهة تتعلق بمنع التغيير العرضي أو غير المصرح به للمعلومات وصيانتها والمحافظة على دقتها.

متطلبات نظام إدارة أمن المعلومات(ISMS)

3. التوافر تتعلق بحماية موارد تقنية المعلومات الضرورية والهامة وضمان توافر المعلومات عند الحاجة إليها.

يعكس نظام إدارة أمن المعلومات (ISMS) في جمعية مودة التزام الإدارة التنفيذية تجاه قيامها بحماية السرية والنزاهة وتأمين توافر جميع أصول تقنية المعلومات، وفقًا لإطار عمل أمن المعلومات والسياسات الأمنية المعمول بها في الجمعية. يجب أن يكون هيكل وسياسات أمن المعلومات في جمعية مودة الخيرية قابلاً للتطبيق وملزماً لجميع الموظفين وشركاء الأعمال والاستشاريين والموردين.

هيكل (أو إطار) العمل لأمن المعلومات

يعتمد هيكل (أو إطار) أمن المعلومات بشكل أساسي على العوامل الرئيسة الثلاث والتي تتكون من الأفراد والعمليات والتقنية المستخدمة. ستشمل سياسة أمن المعلومات تطوير ونشر السياسات والإجراءات في جمعية مودة، ومراقبة تنفيذها على أساس منتظم ومستمر، وضمان استجابة سليمة ووضع آلية واضحة لإصلاح الممارسات والأوضاع الخاطئة لضمان التطوير والتحسين المستمر.

سياسة أمن المعلومات

سياسة أمن المعلومات في جمعية مودة

ضمان سرية وسلامة (نزاهة) وتوافر المعلومات التي يتم تخزينها ومعالجتها ونقلها، والتأكد من أنها محمية دائمًا خلال عمليات التخزين والمعالجة والنقل.

التحسين المستمر لمستوى أمن المعلومات المكرسة لمكافحة التهديدات وبناء برنامج قوي لنظام إدارة أمن المعلومات، والذي يتم مواءمته لتحقيق أهداف السياسات الموضوعة وغايات الجمعية التنظيمية.

يجب على جمعية مودة تأمين أصول تقنية المعلومات الخاصة بها وبأصحاب العلاقة والمصلحة، أو تحقيقيا لأي ارتباط تعاقدي، باستخدام أنسب التقنيات والطرق.

للامتثال لسياسة أمن المعلومات لجمعية مودة أعلاه يجب عمل التالي:

1. وضع هيكلاً أو إطاراً لتحديد أهداف أمن المعلومات، وتأسيس إحساسًا عامًا بالاتجاه الذي يقوم عليه أمن المعلومات ووضع أسس ومبادئ العمل المتعلقة بأمن هذه المعلومات داخل الجمعية.
2. التعهد بالالتزام بمتطلبات العمل والمتطلبات القانونية والتنظيمية والتشريعية المتعلقة بأنشطتها والامتثال للتعهدات الأمنية المتعاقد عليها.
3. تطور منهاجاً وأسلوباً يمكن استخدامه بشكل متكرر لتقييم المخاطر.
4. تكون على أهبة الاستعداد لتحديد وتخفيف المخاطر التي يمكن أن تؤثر على سرية أو نزاهة أو توافر أصول تقنية المعلومات والمعايير المتعلقة بمراجعة المخاطر المحيطة وتخفيفها وقبولها.
5. وضع سياسات وإجراءات لنظام إدارة أمن المعلومات (ISMS).

سياسة أمن المعلومات

هذه السياسة تنطبق على جميع الموظفين الذين يستخدمون خدمات تقنية المعلومات لجمعية مودة الخيرية. إن عدم الامتثال للسياسات المذكورة أدناه سيؤدي إلى إجراءات تأديبية صارمة. يجب إبلاغ هذه السياسة إلى جميع الموظفين من خلال التدريب والعرض المباشر ومن خلال التواصل.

سياسات أمن المعلومات التي تشكل جزءًا من إطار العمل في (ISMS). وتفي بمتطلبات أمن المعلومات المذكورة أدناه:

سياسة استخدام الأجهزة .

سياسة التحكم في الوصول.

سياسة استخدام الانترنت.

سياسة النسخ الاحتياطية

سياسة استخدام البريد الإلكتروني.

سياسة كلمات المرور.

2.2 استراتيجية نظام إدارة أمن المعلومات

سيتم تنفيذ سياسات أمن المعلومات، وتحقيق أهداف الرقابة والتحكم من خلال ما يلي:

1. إجراء تقييم لمخاطر أمن المعلومات، مرة واحدة على الأقل في السنة، والتأكد من أن المخاطر القائمة في حدود مقبولة.
2. خلق وعي بالسياسات وأهداف أمن المعلومات لدى الموظفين من خلال برنامج التدريب والتوعية بأمن المعلومات وعلى أساس الدور الوظيفي لهم.
3. التأكد من تنفيذ إطار أمن المعلومات بما يتوافق مع السياسات والإجراءات التي تم تطويرها.
4. تشكيل لجنة نظام إدارة أمن المعلومات(ISMSC) التي تمتلك وتراقب فعالية نظام إدارة أمن المعلومات (ISMS) وتتخذ الإجراءات التصحيحية المناسبة.

سياسة أمن المعلومات

5. توفير الموارد والبنية التحتية والأموال اللازمة لتنفيذ نظام إدارة أمن المعلومات (ISMS).
6. يجب تدقيق عمليات وسياسات وإجراءات أمن المعلومات بشكل منتظم ودوري كجزء من عملية تدقيق الجودة الداخلية للجمعية، ومن قبل الوكالات الخارجية المختصة، وحيثما كان ذلك ممكنًا.
7. يتم اعتماد أفضل الممارسات في نظام إدارة أمن المعلومات (ISMS) من خلال اعتماد معايير أمن المعلومات العالمية المتبعة في جميع أنحاء العالم، ومن خلال السياسات والإجراءات الحالية المعمول بها، ومن خلال الأطراف المشاركة والمهتمة والمعنية، ومن خلال المستشارين الخارجيين.

قابلية تطبيق السياسة

تنطبق هذه السياسة على جميع موظفي جمعية مودة الخيرية والمقاولين والاستشاريين والموردين أو البائعين الذين يمكنهم الوصول إلى معلومات تقنية المعلومات. في جميع أنحاء هذا المستند، يتم استخدام كلمة "مستخدم" للإشارة بشكل جماعي إلى كل هؤلاء الأفراد.

نصيحة الأخصائيين في أمن المعلومات

عندما يكون ضروريًا، يجب طلب المشورة والنصيحة في الأمور المتعلقة بأمن المعلومات من إدارة الأمن السيبراني أو مستشار مختص بأمن المعلومات والذي يقوم بالبحث عن الحلول وتوصيلها وتعميمها من خلال إدارة الأمن السيبراني.

التواصل مع السلطات

يجب المحافظة على التواصل مع السلطات المسؤولة عن إنفاذ القانون في المملكة العربية السعودية، ومع إدارة الإطفاء، ومع خدمات الطوارئ، ومع مقدمي خدمات الاتصالات، ويقوم بهذا الدور إدارة الأمن السيبراني والإدارات الأخرى المعنية. يجب الحفاظ على تفاصيل الاتصال بهذه الوكالات في سجلات خاصة ومناسبة وحيث يمكن للمستخدمين الوصول إليها.

سياسة أمن المعلومات

التواصل مع المجموعات والأطراف المعنية

التواصل بالشكل المناسب من قبل إدارة الأمن السيبراني مع المجموعات والأطراف المعنية، ومع منتديات أمن المعلومات المرخصة بقصد معرفة وتلقي التحديثات حول التهديدات الأمنية الحاصلة، وحول نقاط الضعف الجديدة أو المستحدثة، وحول الضوابط أو المخاطر على الخدمات التي تقدمها إدارة الأمن السيبراني.

سياسة استخدام الأجهزة

على مستخدمي الاجهزة الالتزام بسياسة استخدام الاجهزة :

1. يجب على الموظفين استخدام أجهزة الكمبيوتر الخاصة بهم لأغراض العمل فقط ولا يجب استخدامها لأداء أي أنشطة ضارة أو غير مشروعة.
2. يجب على الموظفين الحفاظ على الملفات الخاصة .
3. يجب على الموظفين عدم تثبيت أي برامج غير قانونية على أجهزة الكمبيوتر الخاصة بجمعية مودة
4. يجب على الموظفين استخدام التدابير الامنية المناسبة بما في ذلك وسائل الحماية الموافق عليها مسبقا، ومن هذه الوسائل ليس على سبيل الحصر:
    a) مكافحات الفايروسات.
    b) آخر التحديثات لأنظمة التشغيل والتطبيقات.
    c) الحماية بكلمات المرور.
    d) النسخ الاحتياطي للمعلومات.
5. يجب على الموظفين تسجيل الخروج أو قفل أجهزتهم قبل أن يغادروا اماكن عملهم. كذلك يجب تفعيل كلمة المرور وشاشة التوقف المحمية على أجهزة الكمبيوتر الخاصة بهم.

سياسة التحكم في الوصول

بيان السياسة

تحدد سياسة التحكم في الوصول الاتجاه العام والمبادئ التوجيهية لتنفيذ آليات التحكم في الوصول المادية والمنطقية على حد سواء، لضمان سرية وسلامة وتوافر أنظمة تقنية المعلومات في جمعية مودة.

المتطلبات العامة

متطلبات أمن المعلومات الخاصة بالتحكم في الوصول هي كما يلي:

1. التحكم في الوصول يجب أن يكون متاح ومتوفر ومطبق على كل جهاز كمبيوتر، لمنع المستخدمين غير المخوّلين من الدخول إلى الكمبيوتر، ولمنع الوصول غير المصرّح به إلى البيانات الموجودة على الكمبيوتر أو التي يمكن الوصول إليها من خلاله، لضمان توافر البيانات وموارد الكمبيوتر.
2. يجب توفر أجهزة أو برامج أمن المعلومات والتي تقدم وسيلة وطريقة لمصادقة هوية المستخدم المطلوبة.
3. يجب أن تحمي ضوابط أمن المعلومات بيانات مصادقة المستخدم حتى لا يتمكّن أي مستخدم غير مصرّح له من الوصول إليها.
4. يجب حماية جميع أصول تقنية المعلومات بواسطة أجهزة أو برامج أمن المعلومات التي تمت الموافقة عليها من قبل إدارة تقنية المعلومات.
5. يحظر استخدام أي برنامج أو أداة قادرة على تجاوز أو تعديل نظام أمن المعلومات أو ميزات نظام التشغيل أو أي ضوابط أخرى تخص أمن معلومات التطبيقات أو البيانات ما لم تتم الموافقة عليها من إدارة تقنية المعلومات. ويجب مراقبة مثل هذه البرامج أو الأدوات في حال تمت الموافقة على استخدامها، للتأكد من أنّ العملية تتم فقط ضمن ما هو مصرّح به. كما يجب توثيق استخدام مثل هذه البرامج أو الأدوات وتصنيفها "بالسرّية".

سياسة استخدام الانترنت

مستخدمي الانترنت يجب عليهم الاتي:

1. استخدام خدمات الإنترنت لأغراض العمل.
2. يجب على مستخدمي الانترنت عدم استخدام خدمة الإنترنت لأنشطة غير مشروعة، بما في ذلك إرسال أو تلقي مواد حقوق الطبع والنشر في انتهاك لقوانين حقوق النشر المعمول أو اتفاقات الترخيص.
3. يجب ان يكون استخدام الانترنت خاضع للمساءلة ويستخدم فقط في نشر المعلومات المناسبة من خلال خدمات الإنترنت.
4. يجب على مستخدمي الإنترنت عدم استخدام نظم المعلومات لتوزيع أي رموز أو معلومات ضارة، و / أو الاحتيال، أو تمكين فيروسات الكمبيوتر من القيام بأي نشاط للقرصنة داخل بيئة العمل أو خارجها.
5. لا يسمح لمستخدمي الإنترنت زيارة المواقع التي ترتبط بالقرصنة، والتصيد، وتجنب أي من المواقع الخبيثة المعروفة وعادة يتم حظر هذه المواقع.
6. يجب على مستخدمي الإنترنت عدم نشر أي معلومات سرية لجمعية مودة على شبكة الإنترنت دون موافقة مسبقة وإذن من مدير الإدارة ذات الصلة.
7. يجب اتباع جميع القوانين المعمول بها في المملكة العربية السعودية بشأن الإنترنت ومعلومات الاستخدام بدقة.

سياسة النسخ الاحتياطي

المقدمة

لحماية معلومات جمعية مودة الخيرية ومواردها التقنية من جميع التهديدات الداخلية والخارجية، يجب الاحتفاظ بنسخ احتياطية من البيانات لجميع أنظمة تقنية المعلومات العاملة والحيوية والعمل على صيانتها والمحافظة عليها، وينبغي أن يتم ذلك بشكل مجدول ووفق منهجية موحدة على مستوى الجمعية. ستتناول هذه الوثيقة مبادئ تنفيذ النسخ الاحتياطي للبيانات وطرق وأساليب استعادة البيانات الهامة.

الهدف

من هذه السياسة هو التأكد من إجراء عملية النسخ الاحتياطي للمعلومات المهمة المتعلقة بالعمل في جمعية مودة الخيرية، وأن عملية النسخ الاحتياطي تتم على أساس مجدول ومنتظم لمنع فقدان البيانات، أو منع حدوث أي تأثير سلبي على سير العمل.

نطاق العمل

هذه السياسة قابلة للتطبيق على جميع أصول تقنية المعلومات الخاصة بجمعية مودة الخيرية، والتي يتم استخدامها من قبل الموظفين، والمقاولين، والاستشاريين، والموردين.

تفاصيل السياسة

يجب إجراء نسخ احتياطية لجميع المعلومات والبيانات والإعدادات اللازمة بشكل منتظم، لضمان إمكانية استرداد جميع التطبيقات والمعلومات وبيانات الخدمات في حالة فشل الأنظمة أو فقدان الخدمات والبيانات أو تلفها.

سياسة النسخ الاحتياطي

البيان التوضيحي للسياسة

"تقوم جمعية مودة بتنفيذ العمليات والإجراءات المناسبة لضمان توافر أصول تقنية المعلومات الخاصة بها وإتاحتها للاستخدام".

يجب حماية جميع المعلومات الخاصة بالعمل المهمة والحساسة من خلال عملية نسخ احتياطية مناسبة، كما يجب توفير وسائل النسخ الاحتياطية الكافية لضمان إمكانية استعادة جميع المعلومات والبرامج الأساسية في حال وقوع عجز أو فشل في الأنظمة أو الوسائط.

1. يجب الحفاظ على الحد الأدنى من المستوى المطلوب والمحدد من المعلومات المنسوخة احتياطيًّا، بما في ذلك السجلات وجميع المعلومات اللازمة لسير العمل.
2. يتم تحديث وجدولة النسخ الاحتياطي من قبل مسؤولي النسخ الاحتياطي جنبًا إلى جنب مع مالكي البيانات، ويجب الالتزام بالجدول المعتمد لجميع أنشطة النسخ الاحتياطي.
3. يجب إعطاء بيانات النسخ الاحتياطي مستوى من الحماية المادية والبيئية، وذلك بما يتوافق مع المعايير المطبقة في الموقع الرئيسي للجمعية.
4. يجب الاحتفاظ بالنسخ الاحتياطية للفترات اللازمة لتلبية متطلبات العمل والمتطلبات القانونية أو التشريعية، كما يجب على مالكي البيانات تحديد الفترة اللازمة للاحتفاظ بالبيانات الأساسية الخاصة بالعمل، مع تحديد أي متطلبات للقيام بأرشفة هذه البيانات أو الاحتفاظ بنسخ في الأرشيف منها.

سياسة النسخ الاحتياطي

5. سيتم توسيع نطاق الضوابط المطبقة على وسائط حفظ المعلومات في موقع الجمعية الرئيسي وبحسب تصنيف المعلومات الموجودة فيه لتشمل موقع النسخ الاحتياطي.
6. يجب مراجعة سجلات النسخ الاحتياطي من قبل مسؤول النسخ الاحتياطي بشكل مجدول ومنتظم، وعلى النحو المحدد من مسؤول تقنية المعلومات أو مديري الإدارات المعنيين أو مالك البيانات. إذا كان هناك أي تعارض في سجلات النسخ الاحتياطي، يجب مراجعة الأخطاء لمعرفة السبب الأساسي، مع وضع الضوابط اللازمة لمنع وقوع ذلك والحد منه.

سياسة استخدام البريد الالكتروني

مستخدمي البريد الالكتروني يجب عليهم الالتزام بالآتي:

1. استخدام خدمات البريد الإلكتروني فقط لأغراض العمل.
2. مستخدمي البريد الالكتروني يجب ان يكونوا مسؤولين عن الاستخدام المناسب ونشر المعلومات من خلال خدمات البريد الإلكتروني.
3. عدم استخدام البريد الالكتروني للأخرين.
4. لا يجوز استخدام خدمات البريد الإلكتروني الخارجي (هوتميل، ياهو، وGmail) لإرسال المعلومات التي تصنف كمعلومات عمل ذات صلة دون موافقة مسبقة وإذن من الإدارة الخاصة بهم.
5. لا يجوز استخدام خدمات البريد الإلكتروني لأنشطة غير مشروعة، بما في ذلك، وليس على سبيل الحصر، إرسال أو استقبال مواد حقوق الطبع والنشر في انتهاك لقوانين حقوق الطبع والنشر أو اتفاقيات الترخيص.
6. يحظر ارسال رسائل البريد الإلكتروني غير المرغوب فيها، أو غير المصرح بها، أو توزيع أي رسائل المكروهة، بما في ذلك أي بريد مزعج، والبرمجيات الخبيثة، أو المحتوى غير المرغوب فيها. يجب على المستخدمين الذين يتلقون أي بريد إلكتروني من هذا المحتوى من أي مستخدم، إبلاغ الأمر إلى مدير الإدارة ومسؤول تكنولوجيا المعلومات على الفور.
7. لا تعمم أو ترسل التنبيهات والرسائل الخداعة عن طريق البريد الإلكتروني الواردة إلى أي شخص آخر عدا إدارة تقنية المعلومات.
8. لا يجوز الاشتراك بعناوين البريد الإلكتروني إلى أي مجموعة بريدية لأي سبب آخر غير اغراض العمل.
9. عدم ارسال أي رسائل، بغض النظر عن صحتها، والتي قد تسبب الضرر أو تنتحل أي شخصية، أو التي يمكن أن تفسر على أنها إهانة.

سياسة كلمات المرور

بيان السياسة:

" يجب على جمعية مودة أن تفرض سياسة كلمة مرور موحدة عبر البنية التحتية لتقنية المعلومات الخاصة بها لضمان اعتماد المستخدمين ممارسات أمن معلومات جيدة في اختيار كلمة المرور الخاصة بهم واستخدامها."

المتطلبات العامة:

فيما يلي المتطلبات العامة لأمن كلمة المرور. سيتم تغطية هذه البنود لاحقا من الوثيقة بالتفصيل:

1. جميع كلمات مرور الحساب يجب أن تطبق متطلبات كلمة المرور المعقدة (password complexity).
2. يمنع تخزين أو نقل جميع كلمات المرور عبر ملفات بدون تشفير. ويجب الاحتفاظ بها أو إرسالها بطريقة آمنة في جميع الأوقات.
3. يجب حماية جميع الحسابات من خلال تنفيذ عمليات قفل الحساب بعد عدد محدد من محاولات تسجيل الدخول غير الناجحة.
4. يجب حماية حسابات المستخدمين من الوصول غير المصرح به من خلال تنفيذ مهلة لخمول الحساب (idle account) ومهلة الجلسة (session timeout).
5. يجب حجب وإخفاء كلمة المرور على الشاشة أثناء قيام المستخدمين بكتابتها.
6. يمنع استخدام ميزة "تذكر كلمة المرور" في التطبيقات أو الأنظمة.
7. يجب على المستخدمين الحفاظ على سرية كلمات المرور الخاصة بهم.
8. يتعين تنفيذ المتطلبات المتعلقة بالنقطة 1 إلى 8 أعلاه من الناحية التقنية واليا، قدر الإمكان.
9. يجب تحديد إجراءات لإدارة كلمة المرور الآمنة وتوثيقها، بما في ذلك:
    أ. تخصيص كلمة المرور الأولية.
    ب. إعادة تعيين كلمة المرور.
    ت. فتح الحسابات المغلقة.
10. يجب إدارة الأنظمة متعددة المستخدمين أو الأنظمة المشتركة بطريقة آمنة وفعالة.

سياسة كلمات المرور

11. يجب تحديد كلمات المرور الهامة والحرجة وتخزينها بشكل آمن.
12. يمنع الموظف من كتابة كلمة المرور أثناء مشاهدة شخص ما.
13. يمنع الموظف من كتابة كلمة المرور وتخزينها في أي مكان.
14. يمنع الموظف من مشاركة كلمة المرور مع أي شخص بما في ذلك العائلة وزملاء العمل، وموظفي إدارة تقنية المعلومات.

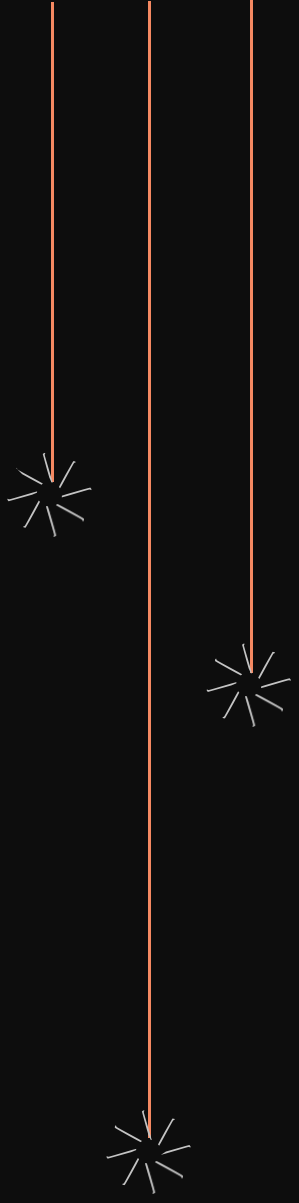
إنشاء كلمات مرور قوية

من الآليات الشائعة للتحكم في الوصول إلى نظم الحاسوب هي عبر استخدام نظام كلمة المرور. ترتبط كل كلمة مرور بهوية أو اسم مستخدم معينة. لتوفير مستوى معقول من الحماية، يوصى بما يلي:

1. يجب أن تحتوي كلمة المرور على ما لا يقل عن ثمانية (8) خانات (خليط بين الأحرف والأرقام والخانات الخاصة) للمستخدمين العاديين وأربعة عشر (14) خانة على الأقل لمسؤولي إدارة الأنظمة.
2. يجب أن تكون كلمة المرور حساسة لحالة الأحرف ويجب أن تحتوي على حرف واحد على الأقل من جميع الفئات الأربعة التالية:
    أ. الأحرف الصغيرة a – z
    ب. الأحرف الكبيرة A – Z
    ت. الأرقام من 0 - 9
    ث. الأحرف الخاصة على سبيل المثال@ #$ %^&*()_+~=\\{}[]:" <> /، الخ.

سياسة كلمات المرور

3. يمنع أن تكون كلمات المرور كلمة موجودة في القاموس أو اسم البلد. ويمنع أن تكون أسماء معروفة بشكل شائع، أو تسلسل من الحروف أو الأرقام يمكن تخمينه بسهولة، أو أي بيانات التي يمكن ربطها بسهولة بالمستخدم، مثل أعياد الميلاد، وأسماء مثل اسم الزوج أو الزوجة، والأطفال، وما إلى ذلك.
4. لا يجب أن تتضمن كلمات المرور ما يلي:
   أ. "اسم المستخدم" إما كما هو، أو معكوس أو بأحرف كبيرة.
   ب. الاسم الأول، أو الاسم المتوسط أو أسماء العائلة.
   ت. اسم المؤسسة أو الشركة أو الهيئة.
   ث. 3 أحرف مكررة أو أكثر، على سبيل المثال (aaa, 111, +++)
   ج. 3 أحرف متتالية من الأبجدية أو أرقام، في ترتيب تصاعدي أو تنازلي، على سبيل المثال (ABC, cba, 123,321)



mafs | مَودة

جمعية مودة للاستقرار الأسري

MAWADDAH ASSOCIATION FOR FAMILY STABILITY