PO-IT-01-02-R0

mafs | مَـودة

جـمـعـيـة مـــودة للاســتــقـــرار الأســـري

MAWADDAH ASSOCIATION FOR FAMILY STABILITY

السياسة العامة للأمن السيبراني

رقم الإصدار	تاريخ الإصدار	الاعتماد
الأول	11 ديسمبر 2024	بقرار من مجلس الادارة رقم (7)

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية مودة بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بجمعية مودة، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC- 1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجمعية مودة وتنطبق على جميع العاملين فيها.
وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية مودة الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

عناصر السياسة

1- يجب على مسؤول تقنية المعلومات تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جمعية مودة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة، واعتمادها من قبل الرئيس التنفيذي كما يجب إطلاع العاملين المعنيين في الجمعية والأطراف ذات العلاقة عليها.
2- يجب على مسؤول تقنية المعلومات تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

2-1 أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)

لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جمعية مودة.

2-2 برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)

لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجمعية مودة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-2 سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Regulatory Cybersecurity Compliance)

للتأكد من أن برنامج الأمن السيبراني لدى جمعية مودة متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- على جمعية مودة الالتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني.
- في حال وجود اتفاقيات أو التزامات دولية معتمدة محلياً تتضمن متطلبات خاصة بالأمن السيبراني، فيجب على الجمعية الالتزام بتلك المتطلبات.

4-2 سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Assessment and Audit Cybersecurity Periodical)

للتأكد من أن ضوابط الأمن السيبراني لدى جمعية مودة مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على الجمعية.

الاجراء:

- على الإدارة المعنية بالأمن السيبراني في جمعية مودة مراجعة تطبيق ضوابط الأمن السيبراني سنوياً.
- مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجمعية، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني مثل المراجع الداخلي على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العالقة.
- توثيق نتائج مراجعة وتدقيق الأمن السيبراني، وعرضها على اللجنة الإشرافية لأمن السيبراني. كما يجب أن تشتمل النتائج على نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وخطة معالجة الملاحظات.

5-2 سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)

للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جمعية مودة تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في جمعية مودة.

- تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجمعية بحد أدنى ما يلي:

1. تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Clauses Disclosure-Non) في عقود العاملين في جمعية مودة.
2. إجراء المسح الأمني للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصالحيات الهامة والحساسة.

- يجب أن تغطي متطلبات الأمن السيبراني خلال علاقة العاملين المهنية بالجمعية بحد أدنى ما يلي:

1. التوعية بالأمن السيبراني .
2. تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني للجمعية.

- مراجعة وإلغاء صلاحيات العاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجمعية.
- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية دورياً

6-2 برنامج التوعية والتدريب بالأمن السيبراني (Training Program Cybersecurity Awareness and)

للتأكد من أن العاملين بجمعية مودة لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين في الجمعية بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لجمعية مودة والقيام بمسؤولياتهم تجاه الأمن السيبراني.

الاجراء:

- تطوير واعتماد برنامج للتوعية بالأمن السيبراني في جمعية مودة من خلال قنوات متعددة دورياً وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية لأمن السيبراني.
- يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية جمعية مودة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك:

1. التعامل الآمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني.
2. التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.
3. التعامل الآمن مع خدمات تصفح الإنترنت.
4. التعامل الآمن مع وسائل التواصل الاجتماعي.

- توفير المهارات المتخصصة والتدريب الازم للعاملين في المجالات الوظيفية ذات العالقة المباشرة بالأمن السيبراني في الجمعية، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك:

1. موظفو الإدارة المعنية بالأمن السيبراني.

2. الموظفون المشغلون للأصول المعلوماتية والتقنية للجمعية.
3. الوظائف الإشرافية والتنفيذية.

- مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجمعية دوريا.

7-2 سياسة إدارة الأصول (Asset Management)

للتأكد من أن جمعية مودة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجمعية، من أجل دعم العمليات التشغيلية للجمعية ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لجمعية مودة ودقتها وتوافرها.

الاجراء:

- تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجمعية.
- تصنيف الأصول المعلوماتية والتقنية للجمعية وترميزها والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
- مراجعة متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجمعية سنويا.

8-2 سياسة إدارة هويات الدخول والصلاحيات (Management Identity and Access)

لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لجمعية مودة من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجمعية.

الاجراء:

- توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جمعية مودة، ومراقبة هذه الآلية والتأكد من تطبيقها.
- يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجمعية بحد أدنى ما يلي:

1. التحقق من هوية المستخدم (Authentication User) بناء على إدارة تسجيل المستخدم، وإدارة كلمة المرور.
2. التحقق من الهوية متعدد العناصر (Authentication Factor-Multi) لعمليات الدخول عن بعد.
3. إدارة تصاريح وصلاحيات المستخدمين (Authorization) بناء على مبادئ التحكم بالدخول والصلاحيات (مبدأ الحاجة إلى المعرفة والاستخدام" Need-to-know and Need-to-use"ومبدأ الحد الأدنى من الصلاحيات والامتيازات " Least Privilege"ومبدأ فصل المهام" Segregation of Duties").

4.إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).

5.المراجعة الدورية لهويات الدخول والصلاحيات.

- مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات في الجمعية دورياً.

9-2 سياسة حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)

لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية لجمعية مودة من المخاطر السيبرانية.

الاجراء:

- توثيق وتطبيق متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي:

1. الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة(Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.
2. التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها.
3. إدارة حزم التحديثات، والإصلاحات للأنظمة والتطبيقات والأجهزة(Management Patch) .
4. مزامنة التوقيت(Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.

- مراجعة متطلبات أمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجمعية سنوياً.

10-2 سياسة حماية البريد الإلكتروني (Email Protection)

لضمان حماية البريد الإلكتروني لجمعية مودة من المخاطر السيبرانية.

الاجراء:

- اعتماد وتطبيق متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني لحماية البريد الإلكتروني للجمعية بحد أدنى ما يلي:

1. تحليل وتصفية رسائل البريد الإلكتروني (وخصوصاً رسائل التصيد الإلكتروني " Phishing Emails "والرسائل الإقتحامية "Spam Emails ")باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني.

2. التحقق من الهوية متعدد العناصر (Authentication Factor-Multi) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني(Webmail) .
3. النسخ الاحتياطي والأرشفة للبريد الإلكتروني.
4. الحماية من التهديدات المتقدمة المستمرة(APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً(Zero-Day Malware) وإدارتها بشكل آمن.
5. توثيق مجال البريد الإلكتروني للجمعية بالطرق التقنية، مثل طريقة إطار سياسة المرسل.(Sender Policy Framework)

- مراجعة تطبيق متطلبات الأمن السيبراني الخاصة بحماية البريد الإلكتروني للجمعية سنوياً.

11-2 سياسة إدارة أمن الشبكات (Networks Security Management)

لضمان حماية شبكات جمعية مودة من المخاطر السيبرانية.

الاجراء:

- يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجمعية بحد أدنى ما يلي:
- العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، والازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية(Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth).

1. عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار.
2. أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.
3. أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناء على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجمعية.
4. قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.
5. أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات(Systems Prevention Intrusion) .
6. أمن نظام أسماء النطاقات(DNS) .
7. حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة(APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً(Zero- Day Malware) ، وإدارتها بشكل آمن.

- مراجعة تطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجمعية سنوياً.

12-2 سياسة أمن الأجهزة المحمولة (Mobile Devices Security)

لضمان حماية أجهزة جمعية مودة المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بأعمال الجمعية وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جمعية مودة .

الاجراء:

يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة والأجهزة الشخصية للعاملين عند ارتباطها بشبكة الجمعية.

- تطبيق متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمول للجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة للجمعية بحد أدنى ما يلي:
  1. فصل وتشفير البيانات والمعلومات الخاصة بالجمعية المخزنة على الأجهزة المحمولة.
  2. الاستخدام المحدد والمقيد بناء على ما تتطلبه مصلحة أعمال الجمعية.
  3. حذف البيانات والمعلومات الخاصة بالجمعية المخزنة على الأجهزة المحمولة عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجمعية.
  4. التوعية الأمنية للمستخدمين.
- مراجعة تطبيق متطلبات الأمن السيبراني الخاصة لأمن الأجهزة المحمولة للجمعية سنوياً.

13-2 سياسة حماية البيانات والمعلومات (Data and Information Protection)

لضمان حماية السرية، وسلامة بيانات ومعلومات جمعية مودة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجمعية، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
- يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي:
  1. ملكية البيانات والمعلومات.
  2. تصنيف البيانات والمعلومات وآلية ترميزها.
  3. خصوصية البيانات والمعلومات.
- مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجمعية سنوياً.

14-2 سياسة التشفير ومعياره (Cryptography)

لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لجمعية مودة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني للتشفير في الجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى ما يلي:
  1. معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً).
  2. الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.
  3. تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
- مراجعة تطبيق متطلبات الأمن السيبراني للتشفير في الجمعية دورياً.

15-2 سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)

لضمان حماية بيانات ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجمعية مودة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- اعتماد وتطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي:
  1. نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
  2. القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.
  3. إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.
- مراجعة تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجمعية.

16-2 سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)

لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال الجمعية.

الاجراء:

- تحديد وتوثيق وتطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى ما يلي:
  1. فحص واكتشاف الثغرات دورياً.
  2. تصنيف الثغرات حسب خطورتها.
  3. معالجة الثغرات بناء على تصنيفها والمخاطر السيبرانية المترتبة عليها.
  4. إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.
  5. التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.
- مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية للجمعية سنوياً.

17-2 سياسة اختبار الاختراق ومعياره (Penetration Testing)

لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جمعية مودة، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني للجمعية؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجمعية.
- تنفيذ عمليات اختبار الاختراق في الجمعية.
- يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق بحد أدنى ما يلي:

1. نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد.
2. عمل اختبار الاختراق دورياً.
3. مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في الجمعية سنوياً.

18-2 سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)

لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جمعية مودة، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم 37140 والتاريخ 14\8\1438هـ.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجمعية.
- يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى ما يلي:
  1. وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد.
  2. تصنيف حوادث الأمن السيبراني.
  3. تبليغ الهيئة عند حدوث حادثة أمن سيبراني.
  4. مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة.
  5. الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.
- مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجمعية دوريا.

19-2 سياسة الأمن المادي (Physical Security)

لضمان حماية الأصول المعلوماتية والتقنية لجمعية مودة من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجمعية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.
- يجب أن تغطي متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجمعية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب بحد أدنى ما يلي:
  1. الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجمعية، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها).

2. سجلات الدخول والمراقبة(CCTV).
3. حماية معلومات سجلات الدخول والمراقبة .
4. أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين) .
5. أمن الأجهزة والمعدات داخل مباني الجمعية وخارجها.

- مراجعة متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجمعية من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب سنوياً.

20-2 جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Resilience Cybersecurity)

لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جمعية مودة، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجمعية.
- يجب أن تغطي إدارة استمرارية الأعمال في الجمعية بحد أدنى ما يلي :
  1. التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني .
  2. وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجمعية.
  3. وضع خطط التعافي من الكوارث(Disaster Recovery Plan) .
- مراجعة متطلبات الأمن السيبراني ضمن إدارة استمرارية أعمال الجمعية سنوياً.

21-2 سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing Cybersecurity)

لضمان حماية أصول جمعية مودة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة) وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الاجراء:

- تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجمعية.

- يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجمعية أو الخدمات المقدمة لها بحد أدنى ما يلي:
  1. بنود المحافظة على سرية المعلومات(Non-Disclosure Clauses) والحذف الآمن من قبل الطرف الخارجي لبيانات الجمعية عند انتهاء الخدمة.
  2. إجراءات التواصل في حال حدوث حادثة أمن سيبراني.
  3. إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجمعية والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية سنوياً.
- يحق لمسؤول تقنية المعلومات الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.

الأدوار والمسؤوليات

1- تُمثل القائمة الآتية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها:

1-1 مسؤوليات صاحب الصلاحية الرئيس التنفيذي أو من ينيبه على سبيل المثال:

1-1-1 إنشاء لجنة إشرافية للأمن السيبراني ويكون مسؤول تقنية المعلومات أحد أعضائها.

2-1 مسؤوليات الشؤون القانونية على سبيل المثال:

1-2-1 التأكد من أن شروط ومتطلبات الامن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين في جمعية مودة والأطراف الخارجية.

3-1 مسؤوليات المراجع الداخلي على سبيل المثال:

1-3-1 مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

1-1-4تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية مودة.

5-1 مسؤوليات مسؤول تقنية المعلومات على سبيل المثال:

1-5-1 الحصول على موافقة رئيس التنفيذي على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل سنوي.

6-1 مسؤوليات رؤساء الإدارات الأخرى على سبيل المثال:

1-6-1 دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لجمعية مودة.

1-7مسؤوليات العاملين على سبيل المثال:

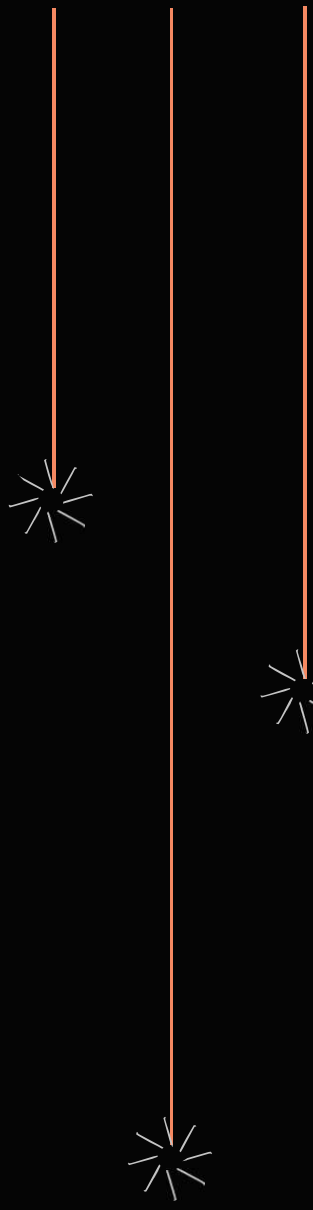
1-7-1 المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية مودة والالتزام بها.

الالتزام بالسياسة

1- يجب على صاحب الصلاحية الرئيس التنفيذي ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.
2- يجب على مسؤول تقنية المعلومات التأكد من التزام جمعية مودة بسياسات الأمن السيبراني ومعاييره بشكل دوري.
3- يجب على جميع العاملين في جمعية مودة الالتزام بهذه السياسة.
4- قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراءٍ تأديبي حسب الإجراءات المتبعة في جمعية مودة.

الاستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من مسؤول تقنية المعلومات أو اللجنة الإشرافية للأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.



mafs | مَودة

جمعية مودة للاستقرار الأسري

MAWADDAH ASSOCIATION FOR FAMILY STABILITY