سياسة الأمن السيبراني ومضاد الفيروسات في الجمعية

الهدف من السياسة:

تهدف سياسة الأمن السيبراني ومضاد الفيروسات في الجمعية إلى توفير بيئة آمنة للبيانات والمعلومات الرقمية الخاصة بالجمعية من خلال اتخاذ الإجراءات الوقائية ضد الهجمات الإلكترونية، الفيروسات، البرمجيات الضارة، والمخاطر التقنية الأخرى. كما تهدف إلى ضمان حماية المعلومات الحساسة التي تحتويها الأنظمة الإلكترونية للحد من المخاطر التي قد تؤثر على العمليات اليومية والأهداف الاستراتيجية للجمعية.

المبادئ الأساسية للسياسة:

1 .حماية البيانات:

- جميع البيانات الشخصية والمالية الخاصة بالجمعية يجب أن تكون محمية باستخدام تقنيات الأمان الحديثة مثل التشفير وبرامج الحماية ضد الفيروسات.
- يجب التأكد من أن جميع المعلومات الحساسة محفوظة في بيئة محمية وآمنة.

2 .إجراءات الأمان على الأجهزة:

- يجب تثبيت برامج مضاد الفيروسات على جميع أجهزة الحاسوب المحمولة والمكتبية داخل الجمعية.
- يجب أن يكون هناك تحديثات دورية لجميع برامج الأمان (مثل مضاد الفيروسات والجدران النارية).
- يجب على جميع الموظفين والمستخدمين التأكد من أن الأجهزة التي يستخدمونها محمية بكلمات مرور قوية وأجهزة تشفير (مثل تشفير محركات الأقراص الثابتة).

3 .إدارة وصول المستخدمين:

- يجب تحديد وتقييد وصول الموظفين إلى المعلومات الحساسة حسب الحاجة، مع الالتزام بمبدأ "الوصول المحدود"

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

-يجب أن تكون كلمات المرور قوية ويتم تغييرها بشكل دوري. كما يجب تطبيق تقنيات التحقق بخطوتين (2FA) على الأنظمة الحساسة.

4.الحماية من الفيروسات والهجمات الإلكترونية:

- جميع الأجهزة يجب أن تحتوي على برامج مضاد الفيروسات المعتمدة والتي يتم تحديثها تلقائيًا.
- يجب فحص البريد الإلكتروني المرسل والوارد بشكل منتظم للكشف عن الفيروسات والمرفقات الضارة.
- يجب على موظفي الجمعية تجنب فتح روابط أو مرفقات مشبوهة أو غير موثوق بها.

5.التدريب والتوعية:

- يجب أن يتلقى جميع الموظفين تدريبًا دوريًا حول مخاطر الأمن السيبراني وأفضل الممارسات لحماية الأجهزة والبيانات.
- يجب توعية الموظفين بخصوص المخاطر المتعلقة بالبريد الإلكتروني الاحتيالي وطرق التصرف السليم في حال حدوث هجوم.

6.إجراءات الطوارئ والاستجابة للهجمات:

- يجب أن يكون لدى الجمعية خطة استجابة للهجمات السيبرانية، بما في ذلك الإجراءات التي يجب اتخاذها في حال حدوث اختراق للبيانات أو الهجوم.
- يجب على قسم تكنولوجيا المعلومات الإبلاغ عن أي خرق أمني فور حدوثه والعمل على حل المشكلة بأسرع وقت ممكن.

7.النسخ الاحتياطي للبيانات:

- يجب إجراء نسخ احتياطية دورية لجميع البيانات الهامة، سواء على الخوادم المحلية أو السحابية، لضمان استعادتها في حال حدوث أي خلل أو هجوم إلكتروني.
- يجب الاحتفاظ بنسخ احتياطية للبيانات في مكان آمن وفصلها عن النظام الأساسي.

ص.ب 51384 الرياض 11543 – المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

8.المراجعة والتدقيق المستمر:

- يجب إجراء مراجعات أمنية منتظمة لأنظمة الجمعية للتأكد من أن جميع السياسات والإجراءات قد تم تطبيقها بشكل صحيح.
- يجب تحديث برامج الأمان وأنظمة مكافحة الفيروسات بانتظام استجابة للتطورات المستمرة في تهديدات الأمن السيبراني.

مسؤوليات الموظفين:

- الموظف: يجب على جميع الموظفين اتباع سياسات وإجراءات الأمان السيبراني ومضاد الفيروسات المعتمدة من قبل الجمعية.
- قسم تكنولوجيا المعلومات: مسؤول عن إدارة وتنفيذ الحلول التقنية اللازمة لحماية البيانات والأجهزة. كما يجب عليهم مراقبة الأنظمة بشكل دوري لاكتشاف أية تهديدات أو خروقات أمنية.

الامتثال للقوانين:

تلتزم الجمعية بجميع القوانين واللوائح المحلية المتعلقة بالأمن السيبراني وحماية البيانات

التطبيق والمراجعة:

-تعتبر هذه السياسة ملزمة لجميع الموظفين في الجمعية. في حالة عدم الامتثال لأي جزء من هذه السياسة، يتم اتخاذ الإجراءات التصحيحية حسب ما تراه إدارة الجمعية مناسبًا.

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa