جمعية الدعوة والإرشاد
وتوعية الجاليات برفحاء

المملكة العربية السعودية
جمعية الدعوة والإرشاد
وتوعية الجاليات بمحافظة رفحاء
رقم التسجيل / ٣٠٥٢
بإشراف وزارة الموارد البشرية والتنمية الاجتماعية

# السياسة العامة للأمن السيبراني بجمعية الدعوة والإرشاد وتوعية الجاليات في رفحاء

**فقد اقر مجلس الإدارة بجمعية الدعوة والإرشاد وتوعية الجاليات بمحافظة رفحاء في الاجتماع رقم ( ٣)**

**بتاريخ ١٤٤٢/٧/١١هـ الموافق ٢٠٢١/٢/٢٣م السياسة العامة للأمن السيبراني**

معتمد من مجلس الإدارة

ص.ب ١٣١ رفحاء تلفاكس: ٠١٤ ٦٧٦ ١٦ ٨٨ البريد الإلكتروني: info@rd.org.sa
الموقع الإلكتروني: www.rd.org.sa

# المحتويات

## الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية الدعوة والارشاد في رفحاء 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 الدعوة والإرشاد في رفحاء ، 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 الدعوة والارشاد في رفحاء وتنطبق على جميع العاملين في جمعية الدعوة والارشاد في رفحاء.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية الدعوة والارشاد في رفحاء الداخلية، مثل: عمليات الموارد البشرية ،عمليات إدارة الموردين ، عمليات إدارة المشاريع ، إدارة التغيير وغيرها.

## عناصر السياسة

١- 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 الدعوة والارشاد في رفحاء بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لجمعية الدعوة والارشاد في رفحاء والمتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس مجلس الادارة، كما يجب إطلاع العاملين المعنيين في جمعية الدعوة والارشاد في رفحاء والأطراف ذات العلاقة عليها.

٢- يجب على مسؤول تقنية المعلومات تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

٢-١ **برنامج استراتيجية الأمن السيبراني** (Cybersecurity Strategy) لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل جمعية الدعوة والارشاد في رفحاء في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢ **أدوار ومسؤوليات الأمن السيبراني** (Cybersecurity Roles and Responsibilities) لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جمعية الدعوة والإرشاد في رفحاء

٢-٣ **برنامج إدارة مخاطر الأمن السيبراني** (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجمعية الدعوة والإرشاد في رفحاء ، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والارشاد في رفحاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٤ **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية** (Cybersecurity in Information Technology Projects) للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جمعية الدعوة والارشاد في رفحاء وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجمعية الدعوة والارشاد في رفحاء وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والارشاد في رفحاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني** (Cybersecurity Regulatory Compliance) للتأكد من أن برنامج الأمن السيبراني لدى جمعية الدعوة والارشاد في رفحاء متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦ **سياسة المراجعة والتدقيق الدوري للأمن السيبراني** (Cybersecurity Periodical Assessment and Audit) للتأكد من أن ضوابط الأمن السيبراني لدى جمعية الدعوة والارشاد في رفحاء مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جمعية الدعوة والإرشاد في رفحاء

٢-٧ **سياسة الأمن السيبراني المتعلق بالموارد البشرية** (Cybersecurity in Human Resources) للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جمعية الدعوة والارشاد في رفحاء تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٨ **برنامج التوعية والتدريب بالأمن السيبراني** (Training Program Cybersecurity Awareness and) للتأكد من أن العاملين بجمعية الدعوة والارشاد في رفحاء لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بجمعية الدعوة والارشاد في رفحاء بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لجمعية الدعوة والارشاد في رفحاء والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٢-٩ **سياسة إدارة الأصول** (Asset Management) للتأكد من أن جمعية الدعوة والارشاد في رفحاء لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لجمعية الدعوة والإرشاد في رفحاء ، من أجل دعم العمليات التشغيلية لجمعية الدعوة والارشاد في رفحاء ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لجمعية الدعوة والارشاد في رفحاء ودقتها وتوافرها.

٢-١٠ **سياسة إدارة هويات الدخول والصلاحيات** (Management Identity and Access) لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لجمعية الدعوة والارشاد في رفحاء من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجمعية الدعوة والإرشاد في رفحاء

٢-١١ **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 الدعوة والارشاد في رفحاء من المخاطر السيبرانية.

٢-١٢ **سياسة حماية البريد الإلكتروني** (Email Protection) لضمان حماية البريد الإلكتروني لجمعية الدعوة والارشاد في رفحاء من المخاطر السيبرانية.

٢-١٣ **سياسة إدارة أمن الشبكات** (Networks Security Management) لضمان حماية شبكات جمعية الدعوة والارشاد في رفحاء من المخاطر السيبرانية.

٢-١٤ **سياسة أمن الأجهزة المحمولة** (Mobile Devices Security) لضمان حماية أجهزة جمعية الدعوة والارشاد في رفحاء 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 جمعية الدعوة والارشاد في رفحاء وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جمعية الدعوة والارشاد في رفحاء (مبدأ "BYOD").

٢-١٥ **سياسة حماية البيانات والمعلومات** (Data and Information Protection) لضمان حماية السرية، وسلامة بيانات ومعلومات جمعية الدعوة والارشاد في رفحاء ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٦ **سياسة التشفير ومعياره** (Cryptography) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لجمعية الدعوة والإرشاد في رفحاء ، وذلك وفقاً للسياسات، والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٧ **سياسة إدارة النسخ الاحتياطية** (Backup and Recovery Management) لضمان حماية بيانات جمعية الدعوة والارشاد في رفحاء ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجمعية الدعوة والارشاد في رفحاء من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٨ **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 جمعية الدعوة والإرشاد في رفحاء.

٢-١٩ **سياسة اختبار الاختراق ومعياره** (Penetration Testing) لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جمعية الدعوة والإرشاد في رفحاء ، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لجمعية الدعوة والإرشاد في رفحاء ؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٠ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني** (Logs and Cybersecurity Event Monitoring Management) لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال جمعية الدعوة والارشاد في رفحاء أو تقليلها.

٢-٢١ **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 الدعوة والإرشاد في رفحاء ، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤٣٨/٨/١٤هـ.

٢-٢٢ **سياسة الأمن المادي** (Physical Security) لضمان حماية الأصول المعلوماتية والتقنية لجمعية الدعوة والارشاد في رفحاء من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢-٢٣ **سياسة حماية تطبيقات الويب ومعياره** (Web Application Security) لضمان حماية تطبيقات الويب الداخلية والخارجية لجمعية الدعوة والارشاد في رفحاء من المخاطر السيبرانية.

٢-٢٤ **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال** (Resilience Cybersecurity) لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جمعية الدعوة والإرشاد في رفحاء ، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لجمعية الدعوة والارشاد في رفحاء وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

٢-٢٥ **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية** (Cybersecurity Third-Party and Cloud Computing) لضمان حماية أصول جمعية الدعوة والارشاد في رفحاء من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٦ **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة** (Cybersecurity Cloud Computing and Hosting) لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية الدعوة والإرشاد في رفحاء ، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لجمعية الدعوة والارشاد في رفحاء على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

٢-٢٧ **سياسة حماية أجهزة وأنظمة التحكم الصناعي** (Cybersecurity Industrial Control Systems) لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول جمعية الدعوة والارشاد في رفحاء وسلامتها وسريتها؛ وهي الأصول المتعلقة وأنظمة التحكم الصناعي وأنظمة (OT\ICS) ضد الهجوم السيبراني (مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب) بما يتسق مع استراتيجية الأمن السيبراني لجمعية الدعوة والإرشاد في رفحاء ، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على جمعية الدعوة والارشاد في رفحاء المتعلقة بالأمن السيبراني.

٣- يحق لمسؤول تقنية المعلومات الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.

## الأدوار والمسؤوليات

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

١-١ مسؤوليات صاحب الصلاحية رئيس مجلس الإدارة أو من ينيبه على سبيل المثال:

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

١-٢ مسؤوليات مسؤول الشؤون القانونية، على سبيل المثال:

- التأكد من أن شروط ومتطلبات الأمن السيبراني والمحافظة على سرية المعلومات ( Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين في جمعية الدعوة والإرشاد في رفحاء ، والأطراف الخارجية.

١-٣ مسؤوليات المدير التنفيذي أو من ينيبه على سبيل المثال:

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

١-٤ مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

- تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية الدعوة والإرشاد في رفحاء.

١-٥ مسؤوليات مسؤول تقنية المعلومات، على سبيل المثال:

- الحصول على موافقة رئيس مجلس الإدارة على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

١-٦ مسؤوليات رؤساء الإدارات الأخرى، على سبيل المثال:

- دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لجمعية الدعوة والإرشاد في رفحاء.

١-٧ مسؤوليات العاملين، على سبيل المثال:

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية الدعوة والإرشاد في رفحاء ، والالتزام بها.

## الالتزام بالسياسة

١. يجب على صاحب الصلاحية رئيس مجلس الادارة ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

٢. يجب على مسؤول تقنية المعلومات التأكد من التزام جمعية الدعوة والارشاد في رفحاء بسياسات الأمن السيبراني ومعاييره بشكل دوري.

٣. يجب على جميع العاملين في جمعية الدعوة والارشاد في رفحاء الالتزام بهذه السياسة.

٤. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية الدعوة والإرشاد في رفحاء.

## الاستثناءات

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