وزارة الموارد البشرية والتنمية الاجتماعية
المملكة العربية السعودية

الجمعية التعاونية متعددة الأغراض برفحاء
MULTIPURPOSE COOPERATIVE SOCIETY AT RAFHA

السياسة العامة للأمن السيبراني

للجمعية التعاونية متعددة الأغراض برفحاء

الجمعية التعاونية برفحاء
متعددة الأغراض
ترخيص ١٤٧
RAFHA CO. OPERATIVE SOC. TY

المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام الجمعية التعاونية متعددة الاغراض برفحاء 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 الجمعية التعاونية متعددة الاغراض برفحاء ، 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 للجمعية التعاونية متعددة الاغراض برفحاء وتنطبق على جميع العاملين في الجمعية التعاونية متعددة الاغراض برفحاء .

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات الجمعية التعاونية متعددة الاغراض برفحاء الداخلية، مثل: عمليات الموارد البشرية ،عمليات إدارة الموردين ، عمليات إدارة المشاريع ، إدارة 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 الجمعية التعاونية متعددة الاغراض برفحاء بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية الجمعية التعاونية متعددة الاغراض برفحاء والمتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس مجلس الادارة، كما يجب إطلاع العاملين المعنيين في الجمعية التعاونية متعددة الاغراض برفحاء والأطراف ذات العلاقة عليها.

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

2-1 **برنامج استراتيجية الأمن السيبراني** (Cybersecurity Strategy) لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل الجمعية التعاونية متعددة الاغراض برفحاء في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-2 **أدوار ومسؤوليات الأمن السيبراني** (Responsibilities Cybersecurity Roles and) لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجمعية التعاونية متعددة الاغراض برفخاء

2-3 **برنامج إدارة مخاطر الأمن السيبراني** (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفخاء ، وذلك وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفخاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-4 **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية** (Cybersecurity in Information Technology Projects) للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع الجمعية التعاونية متعددة الاغراض برفخاء وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفخاء وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفخاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-5 **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني** (Cybersecurity Regulatory Compliance) للتأكد من أن برنامج الأمن السيبراني لدى الجمعية التعاونية متعددة الاغراض برفخاء متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-6 **سياسة المراجعة والتدقيق الدوري للأمن السيبراني** (Cybersecurity Periodical Assessment and Audit) للتأكد من أن ضوابط الأمن السيبراني لدى الجمعية التعاونية متعددة الاغراض برفخاء مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفخاء ، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على الجمعية التعاونية متعددة الاغراض برفخاء

2-7 **سياسة الأمن السيبراني المتعلق بالموارد البشرية** (Cybersecurity in Human Resources) للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في الجمعية التعاونية متعددة الاغراض برفخاء تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفخاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-8 **برنامج التوعية والتدريب بالأمن السيبراني** (Cybersecurity Awareness and Training Program) للتأكد من أن العاملين الجمعية التعاونية متعددة الاغراض برفحاء لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين الجمعية التعاونية متعددة الاغراض برفحاء بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفحاء والقيام بمسؤولياتهم تجاه الأمن السيبراني.

2-9 **سياسة إدارة الأصول** (Asset Management) للتأكد من أن الجمعية التعاونية متعددة الاغراض برفحاء لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة الجمعية التعاونية متعددة الاغراض برفحاء ، من أجل دعم العمليات التشغيلية الجمعية التعاونية متعددة الاغراض برفحاء ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها الجمعية التعاونية متعددة الاغراض برفحاء ودقتها وتوافرها.

2-10 **سياسة إدارة هويات الدخول والصلاحيات** (Management Identity and Access) لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفحاء من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة الجمعية التعاونية متعددة الاغراض برفحاء

2-11 **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 الجمعية التعاونية متعددة الاغراض برفحاء من المخاطر السيبرانية.

2-12 **سياسة حماية البريد الإلكتروني** (Email Protection) لضمان حماية البريد الإلكتروني الجمعية التعاونية متعددة الاغراض برفحاء من المخاطر السيبرانية.

2-13 **سياسة إدارة أمن الشبكات** (Networks Security Management) لضمان حماية شبكات الجمعية التعاونية متعددة الاغراض برفحاء من المخاطر السيبرانية.

2-14 **سياسة أمن الأجهزة المحمولة** (Mobile Devices Security) لضمان حماية أجهزة الجمعية التعاونية متعددة الاغراض برفحاء 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 التعاونية متعددة الاغراض برفحاء وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في الجمعية التعاونية متعددة الاغراض برفحاء (مبدأ "BYOD").

2-15 **سياسة حماية البيانات والمعلومات** (Data and Information Protection) لضمان حماية السرية، وسلامة بيانات ومعلومات الجمعية التعاونية متعددة الاغراض برفحاء ودقتها وتوافرها، وذلك وفقاً للسياسات

والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برخاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-16 **سياسة التشفير ومعياره** (Cryptography) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية الجمعية التعاونية متعددة الاغراض برخاء ، وذلك وفقاً للسياسات، والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برخاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-17 **سياسة إدارة النسخ الاحتياطية** (Backup and Recovery Management) لضمان حماية بيانات الجمعية التعاونية متعددة الاغراض برخاء ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة الجمعية التعاونية متعددة الاغراض برخاء من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برخاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-18 **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 التعاونية متعددة الاغراض برخاء .

2-19 **سياسة اختبار الاختراق ومعياره** (Penetration Testing) لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجمعية التعاونية متعددة الاغراض برخاء ، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني الجمعية التعاونية متعددة الاغراض برخاء ؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-20 **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 الجمعية التعاونية متعددة الاغراض برخاء أو تقليلها.

2-21 **سياسة إدارة حوادث وتهديدات الأمن السيبراني** (Threat Cybersecurity Incident and 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 الجمعية التعاونية متعددة الاغراض برخاء ، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم 37140 والتاريخ 14\8\1438هـ.

2-22 **سياسة الأمن المادي** (Physical Security) لضمان حماية الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفحاء من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

2-23 **سياسة حماية تطبيقات الويب ومعياره** (Web Application Security) لضمان حماية تطبيقات الويب الداخلية والخارجية الجمعية التعاونية متعددة الاغراض برفحاء من المخاطر السيبرانية.

2-24 **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال** (Resilience Cybersecurity) لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجمعية التعاونية متعددة الاغراض برفحاء ، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها الجمعية التعاونية متعددة الاغراض برفحاء وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

2-25 **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية** (Third-Party and Cloud Computing Cybersecurity) لضمان حماية أصول الجمعية التعاونية متعددة الاغراض برفحاء من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفحاء ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-26 **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة** (Cloud and Computing Hosting Cybersecurity) لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعال، وذلك وفقاً للسياسات والإجراءات التنظيمية الجمعية التعاونية متعددة الاغراض برفحاء ، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية الجمعية التعاونية متعددة الاغراض برفحاء على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

2-27 **سياسة حماية أجهزة وأنظمة التحكم الصناعي** (Cybersecurity Industrial Control Systems) لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول الجمعية التعاونية متعددة الاغراض برفحاء 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 الجمعية التعاونية متعددة الاغراض برفحاء ، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية

والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على الجمعية التعاونية متعددة الاغراض برفخاء المتعلقة بالأمن السيبراني.

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

1-1 مسؤوليات صاحب الصلاحية رئيس مجلس الإدارة أو من ينيبه على سبيل المثال:

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

1-2 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 الجمعية التعاونية متعددة الاغراض برفخاء ، والأطراف الخارجية.

1-3 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.

1-4 مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

- تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية التعاونية متعددة الاغراض برفخاء .

1-5 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.

1-6 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 الجمعية التعاونية متعددة الاغراض برفخاء .

1-7 مسؤوليات العاملين، على سبيل المثال:

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية التعاونية متعددة الاغراض برفحاء ، والالتزام بها.

الالتزام بالسياسة

1. يجب على صاحب الصلاحية رئيس مجلس الادارة ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.
2. يجب على مسؤول تقنية المعلومات التأكد من التزام الجمعية التعاونية متعددة الاغراض برفحاء بسياسات الأمن السيبراني ومعاييره بشكل دوري.
3. يجب على جميع العاملين في الجمعية التعاونية متعددة الاغراض برفحاء الالتزام بهذه السياسة.
4. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في الجمعية التعاونية متعددة الاغراض برفحاء .

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.