١- سياسة الأمن السيبراني

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	تقنية.س.01
الحالة	معتمدة

-الاعتماد

الحمدالله والصلاة والسلام على رسول الله صلى الله عليه وسلم وبعد:
فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل) في اجتماعهم العادي يوم الاثنين ٢٠٢٢/٩/١٩م على سياسة الأمن السيبراني وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية مكافحه السرطان الخيرية (تفاؤل) يهدف 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 بـجمعية مكافحة السرطان الخيرية (تفاؤل)، 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 وتنطبق على جميع العاملين فيها.

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

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

٢-١ برنامج إستراتيجية الأمن السيبراني (CYBERSECURITY STRATEGY) **لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل الجمعية في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.**

٢-٢ أدوار ومسؤوليات الأمن السيبراني CYBERSECURITY (RESPONSIBILITIES AND ROLES) **لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني الجمعية.**

٢-٣ برنامج إدارة مخاطر الأمن السيبراني (CYBERSECURITY RISK MANAGEMENT) **لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجمعية وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية 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 الجمعية وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية للجمعية وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية للجمعية والمتطلبات التشريعية والتنظيمية ذات العلاقة.**

٢-٥ سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (CYBERSECURITY REGULATORY COMPLIANCE) **للتأكد من أن برنامج الأمن السيبراني لدى الجمعية 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 الجمعية مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية الجمعية ، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة.

٢-٧ سياسة الأمن السيبراني المتعلق بالموارد البشرية (CYBERSECURITY IN HUMAN RESOURCES) للتأكد من أن أخطار الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) الجمعية تعالج بفعالية قبل إنهاء عملهم وأثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٨ برنامج التوعية والتدريب بالأمن السيبراني (AWARENESS AND TRAINING PROGRAM CYBERSECURITY) للتأكد من أن العاملين بالجمعية لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بالجمعية بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية للجمعية والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٢-٩ سياسة إدارة الأصول (ASSET MANAGEMENT) للتأكد من أن الجمعية لديها قائمة جرد دقيقة وحديثة الأصول تشمل التفاصيل ذات العالقة لجميع الأصول المعلوماتية والتقنية المتاحة للجمعية ، من أجل دعم العمليات التشغيلية ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية، وسلامتها للجمعية، دقتها وتوافرها.

٢-١٠ سياسة إدارة هويات الدخول والصلاحيات (MANAGEMENT IDENTITY AND ACCESS) لضمان حماية الأمن السيبراني للوصول المنطقي(LOGICAL ACCESS) إلى الأصول المعلوماتية والتقنية للجمعية من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجمعية .

٢-١١ سياسة حماية الأنظمة وأجهزة معالجة المعلومات (PROCESSING AND INFORMATION SYSTEM

FACILITIES PROTECTION) لضمان حماية الأنظمة، وأجهزة معالجة المعلومات، بما في ذلك أجهزة المستخدمين، والبنى التحتية للجمعية من المخاطر السيبرانية.

٢-١٢ سياسة حماية البريد الإلكتروني(EMAIL PROTECTION) لضمان حماية البريد الإلكتروني للجمعية من المخاطر السيبرانية.

٢-١٣ سياسة إدارة أمن الشبكات (NETWORKS SECURITY MANAGEMENT) لضمان حماية شبكات الجمعية من المخاطر السيبرانية.

٢-١٤ سياسة أمن الأجهزة المحمولة (DEVICES MOBILE SECURITY) لضمان حماية أجهزة الجمعية بما في ذلك (أجهزة الحاسب المحمول، الهواتف 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 الجمعية (مبدأ "BYOD").

٢-١٥ سياسة حماية البيانات والمعلومات (DATA AND PROTECTION INFORMATION) لضمان حماية السرية، وسلامة بيانات ومعلومات الجمعية ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٦سياسة التشفير ومعياره (CRYPTOGRAPHY) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجمعية وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٧ سياسة إدارة النسخ الاحتياطية (BACKUP AND MANAGEMENT RECOVERY) لضمان حماية بيانات

الخاصة بالجمعية من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية، 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 الجمعية.

٢-١٩ سياسة اختبار الاختراق ومعياره (PENETRATION TESTING) لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجمعية ، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني؛ 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 المخاطر بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال الجمعية أو تقليلها.

٢-٢١ سياسة إدارة حوادث وتهديدات الأمن السيبراني (THREAT AND CYBERSECURITY INCIDEN 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 ، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤\٨\١٤٣٨هـ.

٢-٢٢ سياسة الأمن المادي (SECURITY PHYSICAL) لضمان حماية الأصول المعلوماتية والتقنية للجمعية 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 للجمعية من المخاطر السيبرانية.

٢-٢٤ جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (CYBERSECURITY RESILIENCE) لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجمعية ، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها على الجمعية وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

٢-٢٥ سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (THIRD- AND CLOUD CYBERSECURITY COMPUTING PARTY) لضمان حماية أصول الجمعية من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الاسناد لتقنيه المعلومات)."OUTSOURCING "

والخدمات المدارة " MANAGED SERVICES " وفقاً للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٦ سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (CLOUD HOSTING CYBERSECURITY COMPUTING AND) لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجمعية ، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة وضمان حماية الأصول المعلوماتية والتقنية للجمعية على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

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 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.

١-٣ مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

- تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية.

١-٤ 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.

١-٥ 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 للجمعية.

١-٦ مسؤوليات العاملين، على سبيل المثال:

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في الجمعية والالتزام بها.

الالتزام بالسياسة

1. يجب على صاحب الصلاحية رئيس مجلس الإدارة ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

٢. يجب على مسؤول تقنية المعلومات التأكد من التزام الجمعية بسياسات الأمن السيبراني ومعاييره بشكل دوري.

3. يجب على جميع العاملين في الجمعية الالتزام بهذه السياسة.

٤. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في الجمعية.

الاستثناءات

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