جمعية البر الخيرية بأم الدوم

تحت إشراف وزارة الموارد البشرية
و التنمية الاجتماعية برقم 413

شجرة لا تموت

السياسة العامة للأمن السيبراني

٢٠٢٠ م

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية البر الخيرية بأم الدوم 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 بـجمعية البر الخيرية بأم الدوم، 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 لـجمعية البر الخيرية بأم الدوم وتنطبق على جميع العاملين في جمعية البر الخيرية بأم الدوم.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لـجمعية البر الخيرية بأم الدوم والمتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس مجلس الادارة، كما يجب إطلاع العاملين المعنيين في جمعية البر الخيرية بأم الدوم 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 والأهـداف والمبادرات والمشاريع وفعاليتها داخل جمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم.

٢-٣ **برنامج إدارة مخاطر الأمن السيبراني** (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بأم الدوم، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بأم الدوم وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جمعية البر الخيرية بأم الدوم.

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

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

٢-٩ **سياسة إدارة الأصول** (Asset Management) للتأكد من أن جمعية البر الخيرية بأم الدوم لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لـجمعية البر الخيرية بأم الدوم، من أجل دعم العمليات التشغيلية لـجمعية البر الخيرية بأم الدوم ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لـجمعية البر الخيرية بأم الدوم 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 لـجمعية البر الخيرية بأم الدوم من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بـجمعية البر الخيرية بأم الدوم.

٢-١١ **سياسة حماية الأنظمة وأجهزة معالجة المعلومات** (Processing Information System and Facilities Protection) لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية لـجمعية البر الخيرية بأم الدوم من المخاطر السيبرانية.

٢-١٢ **سياسة حماية البريد الإلكتروني** (Email Protection) لضمان حماية البريد الإلكتروني لـجمعية البر الخيرية بأم الدوم من المخاطر السيبرانية.

٢-١٣ **سياسة إدارة أمن الشبكات** (Networks Security Management) لضمان حماية شبكات جمعية البر الخيرية بأم الدوم من المخاطر السيبرانية.

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

٢-١٥ **سياسة حماية البيانات والمعلومات** (Data and Information Protection) لضمان حماية السرية، وسلامة بيانات ومعلومات جمعية البر الخيرية بأم الدوم ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٦ **سياسة التشفير ومعياره** (Cryptography) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لـجمعية البر الخيرية بأم الدوم، وذلك وفقاً للسياسات، والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٧ **سياسة إدارة النسخ الاحتياطية** (Backup and Recovery Management) لضمان حماية بيانات جمعية البر الخيرية بأم الدوم ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بـجمعية البر الخيرية بأم الدوم من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بأم الدوم، 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 البر الخيرية بأم الدوم.

٢-١٩ **سياسة اختبار الاختراق ومعياره** (Penetration Testing) لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جمعية البر الخيرية بأم الدوم، وذلك من خلال محاكاة تقنيات الهجوم

السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لـجمعية البر الخيرية بأم الدوم؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٠ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني** (Cybersecurity Event Logs and 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 البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم، 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 لـجمعية البر الخيرية بأم الدوم 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 لـجمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لـجمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing"

والخدمات المدارة ("Managed Services") وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية بأم الدوم، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٦ **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة** (Cloud Computing and Hosting Cybersecurity) لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية بأم الدوم، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لجمعية البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم 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 البر الخيرية بأم الدوم، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على جمعية البر الخيرية بأم الدوم 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 وإتباعها:

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 البر الخيرية بأم الدوم، 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 البر الخيرية بأم الدوم.

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 لـجمعية البر الخيرية بأم الدوم.

١-٧ مسؤوليات العاملين، على سبيل المثال:

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية البر الخيرية بأم الدوم، 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 البر الخيرية بأم الدوم بسياسات الأمن السيبراني ومعاييره بشكل دوري.

٣. يجب على جميع العاملين في جمعية البر الخيرية بأم الدوم الالتزام بهذه السياسة.

٤. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الخيرية بأم الدوم.

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.

المحتويات