



السياسة العامة للأمن السيبراني بجمعية البر الخيرية في شعبة نصاب

معتمد من مجلس الإدارة
جمعية البر الخيرية بشعبة نصاب

المحتويات

الصفحة	الموضوع
٢	الأهداف
٢	نطاق العمل وقابلية التطبيق
٢	عناصر السياسة
٧	الأدوار والمسؤوليات
٩	الالتزام بالسياسة
٩	الاستثناءات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية البر الخيرية في شعبة نصاب 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 البر الخيرية في شعبة نصاب ، 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 البر الخيرية في شعبة نصاب وتنطبق على جميع العاملين في جمعية الدعوة والارشاد في رحاء.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعايره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية البر الخيرية في شعبة نصاب 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 في شعبة نصاب بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لجمعية البر الخيرية في شعبة نصاب والمتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس مجلس الادارة، كما يجب إطلاع العاملين المعنيين في جمعية البر الخيرية في شعبة نصاب والأطراف ذات العلاقة عليها.

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

١-٢ برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy) لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل جمعية البر الخيرية في شعبة نصاب في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

- ٢-٢ أدوار ومسؤوليات الأمن السيبراني (Responsibilities Cybersecurity Roles and) لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جمعية البر الخيرية في شعبة نصاب
- ٣-٢ برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجمعية البر الخيرية في شعبة نصاب ، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية في شعبة نصاب والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- ٤-٢ سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (in Information Cybersecurity Technology Projects) للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جمعية البر الخيرية في شعبة نصاب وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجمعية البر الخيرية في شعبة نصاب وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية في شعبة نصاب والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- ٥-٢ سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Regulatory Cybersecurity Compliance) للتأكد من أن برنامج الأمن السيبراني لدى جمعية البر الخيرية في شعبة نصاب متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.
- ٦-٢ سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Assessment and Cybersecurity Periodical Audit) للتأكد من أن ضوابط الأمن السيبراني لدى جمعية البر الخيرية في شعبة نصاب مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية في شعبة نصاب ، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقررة تنظيمياً على جمعية الدعوة والإرشاد في رحاء
- ٧-٢ 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 في شعبة نصاب تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية البر الخيرية في شعبة نصاب ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

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

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

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

١٢-٢ سياسة حماية البريد الإلكتروني (Email Protection) لضمان حماية البريد الإلكتروني لجمعية البر الخيرية في شعبة نصاب من المخاطر السيبرانية.

١٣-٢ سياسة إدارة أمن الشبكات (Networks Security Management) لضمان حماية شبكات جمعية البر الخيرية في شعبة نصاب من المخاطر السيبرانية.

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

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

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

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

١٨-٢ 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.

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

٢٠-٢ سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Monitoring Management Logs and Cybersecurity Event) 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 في شعبة نصاب أو تقليلها.

٢١-٢ سياسة إدارة حوادث وتهديدات الأمن السيبراني (Threat Cybersecurity Incident and Management) لضمان اكتشاف حوادث الأمن السيبراني وتحديدتها في الوقت المناسب، وإدارتها بشكل فعال، والتعامل مع تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جمعية البر الخيرية في شعبة نصاب ، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم ٣٧١٤٠ والتاريخ ١٤٣٨/١١/١٤هـ.

٢٢-٢ سياسة الأمن المادي (Physical Security) لضمان حياة الأصول المعلوماتية والتقنية لجمعية البر الخيرية في شعبة نصاب من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢٣-٢ سياسة حماية تطبيقات الويب ومعياره (Web Application Security) لضمان حماية تطبيقات الويب الداخلية والخارجية لجمعية البر الخيرية في شعبة نصاب من المخاطر السيبرانية.

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

٢٥-٢ سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Computing Third-Party and Cloud Cybersecurity) لضمان حماية أصول جمعية البر الخيرية في شعبة نصاب 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 في شعبة نصاب ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

٢٧-٢ سياسة حماية أجهزة وأنظمة التحكم الصناعي (Cybersecurity Industrial Control Systems)

لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول جمعية البر الخيرية في شعبة نصاب 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 في شعبة نصاب، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقررة تنظيمياً على جمعية البر الخيرية في شعبة نصاب 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- تمثل القائمة التالية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعايره 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.

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

■ التأكد من أن شروط ومتطلبات الأمن السيبراني والمحافظة على سرية المعلومات (Non-disclosure) (Clauses) ملزمة قانونياً في عقود العاملين في جمعية البر الخيرية في شعبة نصاب، والأطراف الخارجية.

٣-١ 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.

٤-١ مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

■ تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية الدعوة والإرشاد في رحاء.

٥-١ 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.

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

■ دعم سياسات الأمن السيبراني وإجراءاته ومعايير وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لجمعية الدعوة والإرشاد في رحاء.

٧-١ مسؤوليات العاملين، على سبيل المثال:

■ المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية البر الخيرية في شعبة نصاب ، والالتزام بها.

الالتزام بالسياسة

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

٢. يجب على مسؤول تقنية المعلومات التأكد من التزام جمعية البر الخيرية في شعبة نصاب بسياسات الأمن السيبراني ومعايير بشكل دوري.

٣. يجب على جميع العاملين في جمعية البر الخيرية في شعبة نصاب الالتزام بهذه السياسة.

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

الاستثناءات

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