الموارد البشرية
والتنمية الاجتماعية

جمعية البر الخيرية في طلعة التمياط
Al - Bir Charity Association in Talat Al - Temyat

السياسة العامة للأمن السيبراني

بجمعية البر خيرية في طلعة التمياط

المحتويات

الأهداف

الغـرض من هذه السيـاسة هو توفير متطلبات الأمن السيبراني المبنية على أفضـل الممـارسات والمعـاييـر المتعـلقة بتـوثيـق متطلبات الأمن السيبراني والتـزام جمعية البر الخيرية بطلعة التميـاط بها ، لتقليل المخـاطر السيبرانية وحمايتـها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهـداف الأساسية للحماية وهي : سرية المعلومات ، وسلامتها ، وتوافرها.
وتهدف هذه السيـاسة إلى الالتـزام بمتطلبـات الأعمـال التنظيـمية الخـاصة بـجمعية البر الخيرية بطلـعة التميـاط ، والمتطلبـات التشريـعية والتنظيـمية ذات العـلاقة ، وهـي مطـلب تـشريـعي في الضـابط رقـم 1-3-1 مـن الضـوابط الأسـاسية للأمن السيـبراني (ECC-1:2018) الصـادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغـطي هذه السيـاسة جميـع الأصـول المعلـومـاتية والتقنيـة لـجمعية البـر الخيـرية بطلعة التمياط وتنطبق على جميع العاملين في جمعية البر الخيرية في طلعة التمياط .
وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييـره ذات المواضيـع المختلفة، وكذلك أحد المدخلات لعمليات جمعيـة البر الخيـرية بطلـعة التميـاط 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 جمعية البر الخيرية بطلعة التمياط بها وذلك وفقاً لمتطلبات الأعمال التنظيمية لـجمعية البر الخيرية بطلعة التمياط والمتطلبات التشريعية والتنظيمية ذات العلاقة واعتمادها من قبل رئيس مجلس الادارة, كما يجب إطلاع العاملين المعنيين في جمعية البر الخيرية بطلعة التمياط 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 والأهـداف والمبادرات والمشاريع وفعاليتها داخل جمعية البر الخيرية بطلعة التمياط في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-2 **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 بطلعة التمياط

2-3 برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بطلعة التمياط ، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط 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 جمعية البر الخيرية بطلعة التمياط وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بطلعة التمياط وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-5 سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني
(Cybersecurity Regulatory Compliance) للتأكد من أن برنامج الأمن السيبراني لدى جمعية البر الخيرية بطلعة التمياط 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 جمعية البر الخيرية بطلعة التمياط مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط ، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جمعية البر الخيرية في طلعة التمياط

2-7 سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources) للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جمعية البر الخيرية بطلعة التمياط تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-8 برنامج التوعية والتدريب بالأمن السيبراني
(Cybersecurity Awareness and Training Program) للتأكد من أن العاملين بـجمعية البر الخيرية بطلعة التمياط لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بـجمعية البر الخيرية بطلعة التمياط بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بطلعة التمياط والقيام بمسؤولياتهم تجاه الأمن السيبراني.

2-9 سياسة إدارة الأصول (Asset Management) للتأكد من أن جمعية البر الخيرية بطلعة التمياط لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لـجمعية البر الخيرية بطلعة التمياط ، من أجل دعم العمليات التشغيلية لـجمعية البر الخيرية بطلعة التمياط ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لـجمعية البر الخيرية بطلعة التمياط ودقتها وتوافرها.

2-10 **سياسة إدارة هويات الدخول والصلاحيات** (Identity and Access Management) لضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بطلعة التمياط من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بـجمعية البر الخيرية في طلعة التمياط

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 لـجمعية البر الخيرية بطلعة التمياط من المخاطر السيبرانية.

2-12 **سياسة حماية البريد الإلكتروني** (Email Protection) لضمان حماية البريد الإلكتروني لـجمعية البر الخيرية بطلعة التمياط من المخاطر السيبرانية.

2-13 **سياسة إدارة أمن الشبكات** (Networks Security Management) لضمان حماية شبكات جمعية البر الخيرية بطلعة التمياط من المخاطر السيبرانية.

2-14 **سياسة أمن الأجهزة المحمولة** (Mobile Devices Security) لضمان حماية أجهزة جمعية البر الخيرية بطلعة التمياط 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 بطلعة التمياط وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جمعية البر الخيرية بطلعة التمياط (مبدأ "BYOD").

2-15 **سياسة حماية البيانات والمعلومات** (Data and Information Protection) لضمان حماية السرية، وسلامة بيانات ومعلومات جمعية البر الخيرية بطلعة التمياط ودقتها وتوافرها وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-16 **سياسة التشفير ومعياره** (Cryptography) لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية لـجمعية البر الخيرية بطلعة التمياط ، وذلك وفقا للسياسات ، والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-17 **سياسة إدارة النسخ الاحتياطية** (Backup and Recovery Management) لضمان حماية بيانات جمعية البر الخيرية بطلعة التمياط ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بـجمعية البر الخيرية بطلعة التمياط من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط ، 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 جمعية البر الخيرية في طلعة التمياط .

2-19 سياسة اختبار الاختراق ومعياره (Penetration Testing) لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جمعية البر الخيرية بطلعة التمياط ، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لـجمعية البر الخيرية بطلعة التمياط ؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-20 **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 بطلعة التمياط أو تقليلها.

2-21 **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 بطلعة التمياط ، 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 لـجمعية البر الخيرية بطلعة التمياط 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 لـجمعية البر الخيرية بطلعة التمياط من المخاطر السيبرانية.

2-24 جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال

(Cybersecurity Resilience) لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جمعية البر الخيرية بطلعة التمياط ، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لـجمعية البر الخيرية بطلعة التمياط 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 جمعية البر الخيرية بطلعة التمياط من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لـجمعية البر الخيرية بطلعة التمياط ، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-26 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 لـجمعية البر الخيرية بطلعة التمياط والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لـجمعية البر الخيرية بطلعة التمياط على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

2-27 سياسة حماية أجهزة وأنظمة التحكم الصناعي

(Industrial Control Systems Cybersecurity) لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول جمعية البر الخيرية بطلعة التمياط 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 لـجمعية البر الخيرية بطلعة التمياط ، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على جمعية البر الخيرية بطلعة التمياط المتعلقة بالأمن السيبراني.

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

الأدوار والمسؤوليات

1 - تمُثل القائمة التالية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها وإتباعها :

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 جمعية البر الخيرية بطلعة التمياط ، 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 جمعية البر الخيرية قي طلعة التمياط .

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 لـجمعية البر الخيرية في طلعة التمياط .

1-7 مسؤوليات العاملين، على سبيل المثال :

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية البر الخيرية بطلعة التمياط ، 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 جمعية البر الخيرية بطلعة التمياط بسياسات الأمن السيبراني ومعاييره بشكل دوري.
3. يجب على جميع العاملين في جمعية البر الخيرية بطلعة التمياط الالتزام بهذه السياسة.
4. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الخيرية في طلعة التمياط .

الاستثناءات

يمُنع 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 .