المملكة العربية السعودية
المركز الوطني لتنمية القطاع الغير ربحي
جمعية التنمية الأهلية ببلعلاء
ترخيص رقم : ٤١٥٣

السياسة العامة للأمن السيبراني

0555664153
@tnmbala40
t.balala37@gmail.com
المملكة العربية السعودية - الباحة - بلعلاء
مصرف الراجحي alrajhi bank | SA0280004666080100320008
466608010032008

المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية التنمية الأهلية ببلعلاء 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 التنمية الأهلية ببلعلاء والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-١:٢٠١٨) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجمعية التنمية الأهلية ببلعلاء وتنطبق على جميع العاملين في جمعية التنمية الأهلية ببلعلاء.

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

٢-٣ **برنامج إدارة مخاطر الأمن السيبراني** (Cybersecurity Risk Management) لضمان إدارة المخاطر السيبرانية على نحو مُمنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجمعية التنمية الأهلية ببلعلاء، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٤ **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية** (in Information Technology Projects Cybersecurity) للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جمعية التنمية الأهلية ببلعلاء وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجمعية التنمية الأهلية ببلعلاء وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني** (Regulatory Compliance Cybersecurity) للتأكد من أن برنامج الأمن السيبراني لدى جمعية التنمية الأهلية ببلعلاء متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦ **سياسة المراجعة والتدقيق الدوري للأمن السيبراني** (Assessment and Audit Cybersecurity Periodical) للتأكد من أن ضوابط الأمن السيبراني لدى جمعية التنمية الأهلية ببلعلاء مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جمعية التنمية الأهلية ببلعلاء.

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 التنمية الأهلية ببلعلاء تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

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

٢-١٠ **سياسة إدارة هويات الدخول والصلاحيات** (Management Identity and Access) لضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية لجمعية التنمية الأهلية ببلعلاء من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجمعية التنمية الأهلية ببلعلاء.

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

٢-١٢ **سياسة حماية البريد الإلكتروني** (Email Protection) لضمان حماية البريد الإلكتروني لجمعية التنمية الأهلية ببلعلاء من المخاطر السيبرانية.

٢-١٣ **سياسة إدارة أمن الشبكات** (Networks Security Management) لضمان حماية شبكات جمعية التنمية الأهلية ببلعلاء من المخاطر السيبرانية.

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

٢-١٥ **سياسة حماية البيانات والمعلومات** (Data and Information Protection) لضمان حماية السرية، وسلامة بيانات ومعلومات جمعية التنمية الأهلية ببلعلاء ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٦ **سياسة التشفير ومعياره** (Cryptography) لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لجمعية التنمية الأهلية ببلعلاء، وذلك وفقاً للسياسات، والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٧ **سياسة إدارة النسخ الاحتياطية** (Backup and Recovery Management) لضمان حماية بيانات جمعية التنمية الأهلية ببلعلاء ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجمعية التنمية الأهلية ببلعلاء من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، 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 التنمية الأهلية ببلعلاء.

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

٢-٢٠ **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني** (Logs and Monitoring Management 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 التنمية الأهلية ببلعلاء أو تقليلها.

٢-٢١ **سياسة إدارة حوادث وتهديدات الأمن السيبراني** (Threat Management Cybersecurity Incident and) 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 التنمية الأهلية ببلعلاء، 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 لجمعية التنمية الأهلية ببلعلاء 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 لجمعية التنمية الأهلية ببلعلاء 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 التنمية الأهلية ببلعلاء، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لجمعية التنمية الأهلية ببلعلاء وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

٢-٢٥ **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية** (Computing Cybersecurity Third-Party and Cloud) لضمان حماية أصول جمعية التنمية الأهلية ببلعلاء من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لجمعية التنمية الأهلية ببلعلاء، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

٢-٢٧ **سياسة حماية أجهزة و أنظمة التحكم الصناعي** (Cybersecurity Industrial Control Systems) لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول جمعية التنمية الأهلية ببلعلاء 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 التنمية الأهلية ببلعلاء، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على جمعية التنمية الأهلية ببلعلاء 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 التنمية الأهلية ببلعلاء، 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 التنمية الأهلية ببلعلاء.

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 لجمعية التنمية الأهلية ببلعلاء.

١-٧ مسؤوليات العاملين، على سبيل المثال:

- المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية التنمية الأهلية ببلعلاء، 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 التنمية الأهلية ببلعلاء بسياسات الأمن السيبراني ومعاييره بشكل دوري.

٣. يجب على جميع العاملين في جمعية التنمية الأهلية ببلعلاء الالتزام بهذه السياسة.

٤. قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية التنمية الأهلية ببلعلاء.

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.

تم اعتماد هذه السياسة باجتماع مجلس الإدارة رقم ٢ بتاريخ يوم الاحد ١٤٤٣/١١/٢٧ هـ

رئيس مجلس الإدارة بجمعية التنمية الاهلية ببلعلاء

عبدالوهاب عبدالله الصهبي