# سياسة العامة للأمن السبيراني

**الأهداف :-**

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جمعية جنا لتأهيل الفتيات ذوات الإعاقة 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 جنا، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني.

**نطاق العمل وقابلية التطبيق :**

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لجمعية جنا لتأهيل الفتيات ذوات الإعاقة وتنطبق على جميع العاملين في جمعية جنا وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جمعية جنا 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 بناء على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني والتزام جمعية جنا 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.

يجب على مسؤول تقنية المعلومات تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

٢-١ برنامج استراتيجية الأمن السيبراني لضمان خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع وفعاليتها داخل جمعية جنا لتأهيل الفتيات ذوات الإعاقة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢ أدوار ومسؤوليات الأمن السيبراني لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جمعية جنا لتأهيل الفتيات ذوات الإعاقة.

٢-٣ برنامج إدارة مخاطر الأمن السيبراني لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لجمعية جنا وذلك وفقا للسياسات والإجراءات التنظيمية للجمعية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٤ سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع الجمعية وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لجمعية جنا وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقا للسياسات والإجراءات التنظيمية للجمعية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٥ سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني للتأكد من أن برنامج الأمن السيبراني لدى الجمعية متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٦ سياسة المراجعة والتدقيق الدوري للأمن السيبراني للتأكد من أن ضوابط الأمن السيبراني لدى الجمعية مطبقة، وتعمل وفقا للسياسات والإجراءات التنظيمية للجمعية والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيميا على جمعية جنا لتأهيل الفتيات ذوات الإعاقة.

٢-٧ سياسة الأمن السيبراني المتعلق بالموارد البشرية للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين الموظفين والمتعاقدين في الجمعية تعالج بفعالية قبل إنهاء عملهم و أثناء ذلك وعند انتهائه، وذلك وفق للسياسات والإجراءات التنظيمية لجمعية جنا لتأهيل الفتيات ذوات الإعاقة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٨ برنامج التوعية والتدريب بالأمن السيبراني للتأكد من أن العاملين بجمعية جنا لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بجمعية جنا بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لجمعية جنا والقيام بمسؤولياتهم تجاه الأمن السيبراني.

٢-٩ سياسة إدارة الأصول للتأكد من أن جمعية جنا لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لجمعية جنا، من أجل دعم العمليات التشغيلية للجمعية ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لجمعية جنا ودقتها وتوافرها.

٢-١٠ سياسة إدارة هويات الدخول والصلاحيات لضمان حماية الأمن السيبراني للوصول المنطقي إلى الأصول المعلوماتية والتقنية للجمعية من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بجمعية جنا.

٢-١١ سياسة حماية الأنظمة وأجهزة معالجة المعلومات لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية للجمعية من المخاطر السيبرانية.

٢-١٢ سياسة حماية البريد الإلكتروني لضمان حماية البريد الإلكتروني للجمعية من المخاطر السيبرانية.

٢-١٣ سياسة إدارة أمن الشبكات لضمان حماية شبكات الجمعية من المخاطر السيبرانية.

٢-١٤ سياسة أمن الأجهزة المحمولة لضمان حماية أجهزة جمعية جنا 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 الجمعية وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في الجمعية.

٢-١٥ سياسة حماية البيانات والمعلومات لضمان حماية السرية، وسلامة بيانات ومعلومات الجمعية للسياسات والإجراءات التنظيمية للجمعية ودقتها وتوافرها، وذلك وفقً بالأبواء، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

٢-١٧ سياسة إدارة النسخ الاحتياطية لضمان حماية بيانات الجمعية ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بجمعية من الأضرار الناجمة عن المخاطر للسياسات والإجراءات التنظيمية لجمعية السيبرانية، وذلك وفقًا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-١٨ سياسة إدارة الثغرات ومعياره 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 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 للجمعية وللمتطلبات التشريعية؛ وذلك وفقًا للمتطلبات والتنظيمية ذات العلاقة.

٢-٢٠ سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني 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 جنا وتقليلها.

٢-٢١ سياسة إدارة حوادث وتهديدات الأمن لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقيًا من أجل منع الآثار السلبية المحتملة أو تقليلها.

٢-٢٢ سياسة الأمن المادي لضمان حماية الأصول المعلوماتية والتقنية لجمعية جنا من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

٢-٢٣ سياسة حماية تطبيقات الويب ومعياره لضمان حماية تطبيقات الويب الداخلية والخارجية لجمعية جنا من المخاطر السيبرانية.

٢-٢٤ جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجمعية ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها الخيرية و أنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية

٢-٢٥. سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية لضمان حماية أصول الجمعية من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات وفقً والإجراءات التنظيمية للجمعية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٢-٢٦ سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقً لجمعية جنا والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لجمعية جنت على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

٢-٢٧ سياسة حماية أجهزة و أنظمة التحكم الصناعي لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول الجمعية وسلامتها وسريتها؛ وهي الأصول المتعلقة و أنظمة التحكم الصناعي و أنظمة ضد الهجوم السيبراني مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب (بما يتسق مع استراتيجية الأمن السيبراني للجمعية وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقمرة تنظيميًا على جمعية جنا 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 :

تُمثل القائمة التالية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها و إتباعها:

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 -مسؤوليات مسؤول الشؤون القانونية، على سبيل المثال:

التأكد من أن شروط ومتطلبات الأمن السيبراني والمحافظة على سرية المعلومات في عقود العاملين في جمعية جنا ، والأطراف الخارجية.

٣ -مسؤوليات المدير التنفيذي أو من ينيبه على سبيل المثال:

مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقا للمعايير المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

٤ -مسؤوليات مسؤول الموارد البشرية على سبيل المثال:

تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية جنا.

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.

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 جنا.

٧ -مسؤوليات العاملين، على سبيل المثال:

المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جمعية جنا، والالتزام بها.

## الالتزام بالسياسة:

- يجب على صاحب الصلاحية رئيس مجلس الادارة ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.
- يجب على مسؤول تقنية المعلومات التأكد من التزام جمعية البر الخيرية بالأبواء بسياسات الأمن السيبراني ومعاييره بشكل دوري.
- يجب على جميع العاملين في جمعية البر الخيرية بالأبواء الالتزام بهذه السياسة.
- قد يعرض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية جنا لتأهيل الفتيات ذوات الإعاقة.

## الاستثناءات :

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

جمعية جنا لتأهيل الفتيات ذوات الإعاقة
Jana Charity Association for Qualifying Special Needs Girls

يعتمد رئيس مجلس الإدارة :

هناء عبدالعزيز تاج

جمعية جنا لتأهيل الفتيات ذوات الإعاقة
Jana Charity Association for Qualifying Special Needs Girls
المركز الوطني لتنمية القطاع غير الربحي تصريح ( ١٠٩٣ )

جمعية جنا لتأهيل الفتيات ذوات الإعاقة
Jana Charity Association for Qualifying Special Needs Girls

055 08 50 141
050 21 02 751
info@janaa.org.sa
www.janaa.org.sa