١١- سياسة ضمان استمرارية الأعمال

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	تقنية.س.١١
الحالة	معتمدة

-الاعتماد

الحمدالله والصلاة والسلام على رسول الله صلى الله عليه وسلم وبعد:

فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل) في اجتماعهم العادي يوم الاثنين ٢٠٢٢/٩/١٩م على **سياسة ضمان استمرارية الأعمال** وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

المقدمة والأهداف:

الغرض من هذه السياسة هو تحديد الإجراءات الملائمة والتي من شأنها تقليص انقطاع أنشطة العمل وحماية إجراءات العمل الحساسة من الآثار التي قد تنجم عن حدوث عطل واسع في نظم المعلومات أو وقوع الكوارث وضمان مواصلة عمل هذه النظم دون تأخير وذلك من خلال الآتي:

- توفير دليل لفرق استمرارية العمل بالجمعية.
- توفير الإجراءات والموارد اللازمة للمساعدة في التعافي من الكوارث .
- تحديد الجهات الخارجية التي يجب أن يتم إعلامها في حال وقوع كارثة.
- المساعدة في تجنب الارتباك خلال وقوع الكارثة من خلال توثيق واختبار ومراجعة إجراءات الاسترداد.
- تحديد مصادر بديلة للإمدادات والموارد والمواقع
- توثيق إجراءات النسخ الاحتياطي، حماية واسترجاع السجلات الحيوية.

تعريف الكارثة:

يمكن أن يكون سبب الكارثة الإنسان أو الطبيعة، وينتج عن الكارثة عدم القدرة على أداء جميع أو بعض أدوار المؤسسة ومسؤولياتها العادية لفترة من الزمن . وتعرف الكوارث ـ الطوارئ ـ بالجمعية على النحو التالي:

١. تعطل واحد أو أكثر من الأنظمة الحيوية والتي تقوم عليها أهم أنشطة الجمعية.
٢. المبنى غير متاح لفترة طويلة من الزمن.
٣. يتوفر المبنى، ولكن جميع الأنظمة متعطلة.
٤. المبنى وجميع النظم غير متاحة.

يمكن أن تؤدي الأحداث التالية إلى كارثة وتتطلب تفعيل وثيقة التعافي من الكوارث:

١. حريق.

٢. فيضانات.
٣. انقطاع التيار الكهربائي.
٤. الحرب .
٥. السرقة .
٦. هجوم إرهابي وتحدد الخطة نقاط الضعف وتوصي باتخاذ التدابير لمنع انقطاع الخدمة.

السياسات:

١-استمرارية النشاط وتقييم المخاطر

- ينبغي على الجمعية أن تطبق إطاراً مناسباً لإدارة استمرارية النشاط للحد من التأثير الذي قد تتعرض له الهيئة واسترجاع خسارة المعلومات التي فقدت في الكوارث الرئيسية: (الحريق -الفيضان -الهزات الأرضية -العواصف -الأعطال الرئيسية لنظام تقنية المعلومات للأجهزة فقد سجلات أو خدمات المنافع لفترة طويلة فقد الموارد... إلخ.
- يجب أن يستند تخطيط استمرارية النشاط وعلى تحليل المخاطر وتأثيرها لتحديد إمكانية وأثر تلك الانقطاعات من حيث الفترات الزمنية ونطاق الضرر الواقع وفترة الاستعداد.
- تقوم الجمعية بمشاركة كاملة من المسؤولين عن العمليات / الخدمات وموارد العمل الأخرى المرتبطة ببيئة أنظمة المعلومات بإجراء تقييم للمخاطر المترتبة على التوقف والتغيير في بيئة أنظمة المعلومات يتبعه تحليل آثار التغيير.
- يجب أن يشتمل تقييم المخاطر المترتبة على توقيف أنظمة المعلومات والفترات المسموح بها لانقطاع الخدمة وأولويات الاستعادة.

سجل التهديدات:

يعد سجل التهديدات قائمة عالية القيمة تضم مصادر الكوارث التي قد يكون لها تأثير كبير على المرونة التشغيلية للجمعية، وعند تقييم التهديدات يكون احتمالية الحدوث على النحو التالي:

١- احتمالية كبيرة: حدث يقع سنوياً أو بوتيرة أكبر.
٢- محتمل: حدث يقع كل ثلاث سنوات في المتوسط.
٣- نادر: حدث يقع كل عشر سنوات.
٤- غير محتمل: حدث يقع كل ٥٠ سنة أو أكثر.
٥- خارج النطاق: خارج النطاق - لا يتم الالتفات إلى هذه الأحداث في استمرارية الأعمال.

فئة التهديد	التهديد	الاحتمالية	طريقة العلاج
الكوارث الطبيعية	الحريق	احتمالية كبيرة	١- التأكد من توفير أدوات السلامة في جميع مرافق الجمعية. ٢- انصراف الموظفين إلى نقطة تجمع خارج مكان الحريق، والاطمئنان على سلامة الجميع. ٣-السيطرة على الحريق بإخماده بواسطة أدوات السلامة.

	الفيضان	غير محتمل	بحكم أن مدينة الأحساء لا توجد بقرب مسطحات مائية فإن نسبة حدوث هذا التهديد غير محتملة.
	الإعصار/العاصفة	نادر	١- التأكد من سلامة جميع الموظفين. ٢-الحرص على عمل نسخ احتياطية للبيانات بشكل دوري للعمل على استعادتها لاحقًا في حال حدوث مثل هذا النوع من التهديدات.
	الزلزال	نادر	١- التأكد من سلامة جميع الموظفين. ٢-الحرص على عمل نسخ احتياطية للبيانات بشكل دوري للعمل على استعادتها لاحقا في حال حدوث مثل هذا النوع من التهديدات.
	ضربات البرق الهبوط	محتمل	١- التأكد من سلامة جميع الموظفين. ٢-الحرص على عمل نسخ احتياطية للبيانات بشكل دوري للعمل على استعادتها لاحقًا في حال حدوث مثل هذا النوع من التهديدات.
	النشاط البركاني	خارج النطاق	بحكم أن مدينة الأحساء لا توجد بقرب مسطحات مائية فإن نسبة حدوث هذا التهديد غير محتملة.
	تسونامي	خارج النطاق	بحكم أن مدينة الأحساء لا توجد بقرب مسطحات مائية فإن نسبة حدوث هذا التهديد غير محتملة.

	القوارض	نادر	يتم عمل تعقيم بشكل دوري للتأكد من خلو القوارض وهذا تهديد نادر حدوثه
	انتشار الحشرات	نادر	يتم عمل تعقيم بشكل دوري للتأكد من خلو الحشرات وهذا تهديد نادر حدوثه

فئة التهديد	التهديد	الاحتمالية	طريقة العلاج
الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS	محتمل	تم وضع برنامج حماية على السيرفر الخاص بقاعدة البيانات الموجودة على نظام رافد الخاص بالجمعية (server firewall) كما يتم اختبار الثغرات بشكل دوري من قبل الفريق التقني للنظام.
	القراصنة	محتمل	يتم عمل اختبار للثغرات على النظام بشكل دوري من قبل الفريق التقني للنظام.
	فقد البيانات	محتمل	يتم أخذ نسخ احتياطية من قواعد البيانات للجمعية بشكل يومي من خلال سكربت برمجي منشأ من قبل فريق تطوير نظام رافد. ويمكن من خلالها استعادة البيانات الموجودة.
	فيروسات الفدية	محتمل	فيما يخص الهجوم على النظام المستخدم بالجمعية (نظام رافد) فإنه يتم تشفير البيانات ذات الحساسية بنظام تشفير من قبل فريق الأمن السيبراني بنظام رافد كما يتم عمل اختبار للثغرات على

			النظام بشكل دوري من قبل الجهة المفعلة للنظام
	الأنشطة ذات الصلة بالحرب الإلكترونية	محتمل	فيما يخص الهجوم على النظام المستخدم بالجمعية (نظام رافد) فإنه يتم عمل اختبار للثغرات على النظام بشكل دوري من قبل الجهة المفعلة للنظام

سياسة النسخ الاحتياطي والاسترجاع في حال الكوارث:

المقدمة والأهداف:

الغرض من هذه السياسة هو: التأكد من عمل نسخة احتياطية مساندة للمعلومات الإلكترونية واسترجاعها من قبل الجمعية بشكل مخطط. سريع وفعال وآمن بناء على متطلبات العمل.

السياسات:

أ-متطلبات النسخ الاحتياطية:

- يتم أخذ النسخ الإلكترونية المخزنة في المخزنة في أنظمة المعلومات لدى الجمعية بناءً على احتياجات العمل ووفقاً لإجراءات معرفه في خطة النسخ الاحتياطي والمعتمدة لدى إدارة تقنية المعلومات.
- تكون إدارة تقنية المعلومات مسؤولة عن أخذ النسخ الاحتياطي لجميع أنظمة تقنية المعلومات التي تديرها وذلك وفقاً لخطط النسخ الاحتياطية التي تم تطويرها لتلك الأنظمة.
- يكون جميع موظفي الجمعية مسؤولين عن أخذ النسخ الاحتياطية الخاصة بمهام على خوادم ملفات الشبكة أو الوسط المختار للنسخ الاحتياطية.
- يجب استخدام وسائط مناسبة لتخزين النسخ الاحتياطية بحيث التأكد من أنها خالية من الأخطاء وصالحة للاستخدام

- يجب استبدال وسائط تخزين النسخ الاحتياطية بعد مواجهة أي خطأ أو على فترات زمنية محددة مسبقاً أيهما يقع أولاً.
- يتوجب على رئيس قسم البنية التحتية متابعة استخدام وسائط النسخ الاحتياطية على أن يتم استبدال تلك الوسائط بعد استخدامها حسب نظام النسخ الاحتياطية.

ج-الاحتفاظ بالبيانات:

تقوم إدارة تقنية المعلومات بالتأكد من الاحتفاظ بنسخ البيانات الخاصة بأنظمة المعلومات للمدة المطلوبة من قبل الهيئة أو حسب متطلبات النظام.

د -استرجاع النسخ الاحتياطية:

يتم استرجاع النسخ الاحتياطية على أساس الحاجة وبناء على تفويض مناسب من مدير إدارة تقنية المعلومات.

يتم استرجاع النسخ الاحتياطية وفقاً لإجراءات استرجاع النسخ الاحتياطية

هـ-فحص استرجاع النسخ الاحتياطية:

- تقوم إدارة تقنية المعلومات بإجراء اختبارات على استرجاع النسخ الاحتياطية على عينة من البيانات المخزنة في النسخ الاحتياطية بشكل دوري للتأكد من قابليتها للاسترجاع.
- يتم إجراء اختبارات استرجاع النسخ الاحتياطية وفقاً لإجراءات فحص استرجاع النسخ الاحتياطية.

١٢-سياسة معدل الاستخدام الأمثل للأنظمة:

المسؤول عنها	الاتصال المؤسسي
رمز السياسة	إعلام.س.١٢
الحالة	معتمدة

-الاعتماد

الحمدالله والصلاة والسلام على رسول الله وبعد:

فقد اطلع أعضاء الجمعية العمومية بجمعية مكافحة السرطان الخيرية بالأحساء (تفاؤل) في اجتماعهم العادي يوم الإثنين الموافق ٢٠٢٢/٩/١٩م على **سياسة معدل الاستخدام الأمثل للأنظمة** وقرروا اعتمادها والعمل بموجبها ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

رئيس مجلس الإدارة

محمد بن عبد العزيز العفالق

سياسة معدل الاستخدام الأمثل للأنظمة:

المقدمة والأهداف:

الغرض من هذه السياسة هو وضع قواعد الاستخدام المقبول لأنظمة المعلومات لدى جمعية تفاؤل.

السياسات:

ا-الاستخدامات العامة ومسؤولية الائتمان:

يصرح للمستخدمين باستخدام مصادر المعلومات لدى جمعية تفاؤل فقط لأغراض العمل المصرح لهم القيام بذلك وسيتعرض المستخدم الذي يخالف ذلك للإجراءات التأديبية والقانونية المناسبة.

تؤول ملكية كافة بيانات الحاسب الذي تم إنشاؤها أو استلامها أو إرسالها باستخدام أنظمة المعلومات لدى جمعية تفاؤل لملكية الجمعية ولا تعتبر مملوكة من قبل المستخدم وتحتفظ الهيئة بحقها بفحص كافة البيانات لأي سبب وبدون إخطار ومثال ذلك عندما تكون هناك شبهات بمخالفة هذه القواعد أو اية سياسات وإجراءات لدى الهيئة.

ينبغي على الموظفين والمقاولين والمستخدمين من طرف ثالث الذين يستخدمون أو لديهم إمكانية الوصول إلى معلومات جمعية تفاؤل أن يكونوا على دراية بالحدود الحالية لاستخدامهم لأنظمة المعلومات.

حقوق الملكية الفكرية والتراخيص:

- جمعية تفاؤل الخيرية تقدر وتحترم حقوق الملكية الفكرية (التي تشمل حقوق النسخ وحقوق التصميم وحقوق براءة الاختراع وتراخيص الشفرات المصدرية للبرنامج والوثائق المرتبطة بأنظمة المعلومات لديها.
- يمنع انتهاك أي حقوق محمية بحقوق النسخ أو براءة الاختراع أو حقوق الملكية الفكرية الأخرى أو اللوائح والأنظمة المشابهة بما في ذلك ودون حصر تركيب البرامج غير المصرح بها أو غير القانونية على أنظمة الهيئة والأنظمة الأخرى التابعة لجمعية تفاؤل.
- يجب أن تحفظ إدارة تقنية المعلومات بمعلومات مناسبة عن التراخيص والأحكام والشروط المتعلقة بأنظمة المعلومات العامة التي لديها.
- يمنع منعاً بات استخدام برمجيات أو حقوق فكرية غير مرخصة.

الاستخدام غير المقبول للأنظمة والشبكات:

- يمنع إدخال برامج خبيثة (الفيروسات -الشفرات الخبيثة -طروادة. إلخ) إلى أنظمة المعلومات لدى تفاؤل.
- يمنع إدخال البرامج أو المشاركة في برنامج الهيئة سواء تم تحميلها من الإنترنت أو تم الحصول عليها من وسائط أخرى دون تفويض من إدارة تقنية المعلومات.
- يمنع تقديم عروض، أو منتجات، أو بنود، أو خدمات تنطوي على الغش والخداع باستخدام موارد الأنظمة لدى جمعية تفاؤل.
- يمنع الكشف عن كلمات المرور التي يستخدمها الآخرون للدخول إلى حساباتهم أو السماح باستخدام تلك الحسابات من قبل أطراف أخرى.
- يمنع إجراء مسح للمنافذ أو مسح أمني لشبكة معلومات تفاؤل أو نظام معلوماتها إلا إذا كان ذلك مصرحاً به من قبل مدير تقنية المعلومات ويتم إرسال إشعارات مسبقة وذلك للأشخاص المعنيين.
- يمنع تنفيذ أي شكل من أشكال مراقبة الشبكة والتي يتم خلالها اعتراضها البيانات التي لا تعني الجهاز المضيف لحساب الموظف إلا إذا كان هذا النشاط جزءاً من الوظيفة المهمة المصرح بها للموظف أو بطلب من الإدارة المعنية وبموافقة إدارة أمن المعلومات.

- يمنع التحايل والالتفاف حول تعريف هوية المستخدم، أو أمن أي مضيف، أو شبكة، أو حاسوب.
- يمنع استخدام أي برنامج - لغة - أمر أو إرسال الرسائل من أي نوع بغرض التداخل مع أو تعطيل طرفية أي مستخدم من خلال أية وسائل محلياً أو عبر الإنترنت.
- يمنع تزويد معلومات تتعلق بموظفي الهيئة أو قوائم أسمائهم إلى أي أطراف خارج تفاؤل.

استخدام البريد الإلكتروني والشبكات

١. يمنع إرسال أي رسائل بريد غير مرغوب فيه بما في ذلك إرسال البريد غير النافع المواد الإعلانية إلى الأشخاص الذين لم يطلبوا تلك المواد بصفة محددة (رسائل البريد الإلكتروني الاقتحامية).
٢. تمنع المضايقة عبر البريد الإلكتروني سواء من حيث اللغة أو بتكرار أو بحجم الرسائل.
٣. يمنع منعاً باتاً الاستخدام غير المصرح به أو تزوير معلومات ترويسة البريد الإلكتروني أو محتوياتها.
٤. يمنع إنشاء أو تحرير الرسائل التسلسلية أو برامج هرمية من أي نوع.