Qatar Cancer Society
الجمعية القطرية للسرطان

سياسة أمن المعلومات

المحتويات

1. المقدمة

تعتبر المعلومات من أهم الموارد الأساسية للمؤسسات، و هي الرصيد الحيوي لضمان استمرار عمل المؤسسة، لذا تعتبر الجمعية الحفاظ على أمن المعلومات هدفاً رئيسيا للعمل لديها، وتعمل على تطبيق أفضل الممارسات من أجل حماية المعلومات من الاستخدام غير المشروع أو المصرح به.

تعريف سياسة أمن المعلومات:

هي عبارة عن تعبير رسمي يقصد به مجموعة القواعد والقوانين التي يتم تطبيقها عند التعامل مع المعلومات والتقنيات المرتبطة بها داخل المنشأة.

أهداف سياسة أمن المعلومات

- تحديد أفضل الممارسات والإجراءات الواجبة للحفاظ على أمن المعلومات
- بيان الإجراءات التي يجب إتباعها لتفادي المخاطر والمهددات والتعامل معها إذا ما وقعت
- تحديد الآليات التي يتم من خلالها تنفيذ وتحقيق المسؤوليات والواجبات لكل مستخدم

نطاق سياسة أمن المعلومات

تشمل سياسة أمن المعلومات لدى الجمعية القطرية للسرطان، جميع أشكال المعلومات الرقمية المتوفرة في خوادم مركز المعلومات، أو على أجهزة الحاسوب المكتبية أو المحمولة أو الهواتف الذكية، أو المعلومات المتناقلة عبر الشبكة أو البريد الإلكتروني.

2. حماية البيانات و تصنيفها

النطاق:

تطبق سياسة حماية البيانات و تصنيفها على الموظفين الذين يتعاملون أو يملكون البيانات.

تصنيف البيانات:

- عام : بيانات عامة عن الجمعية، تُنشر على الموقع الإلكتروني بهدف الشفافية، و هي متوفرة للجميع.
- داخلي – عام: بيانات عامة لجميع موظفي الجمعية، تنشر على الشبكة الداخلية للجمعية، و يحق لجميع موظفي الجمعية الوصول إليها.
- خاص – إدارة: بيانات خاصة بإحدى إدارات الجمعية، يحق لموظفي الإدارة المعنية الوصول إليها فقط.
- خاص – قسم: بيانات خاصة بإحدى الأقسام داخل إدارات الجمعية، يحق لموظفي القسم المعني الوصول إليها فقط.
- خاص – موظف: بيانات مخصصة لإحدى موظفي الجمعية، يحقق للموظف المعني الدخول اليها فقط.

السياسة:

- يُحدد مالك البيانات (Data Owner) لكل مجموعة مترابطة من البيانات.
- يوضح مالك البيانات مدى أهمية البيانات و طريقة تخزينها و صلاحيات الوصول لدى قسم تكنولوجيا المعلومات.
- يوفر قسم نظم المعلومات نسخ احتياطية دورية للبيانات.
- يقوم قسم تكنولوجيا المعلومات بحفظ البيانات و استرجاعها حال تعرضها لأي طارىء.

3. استخدام شبكة الانترنت

النطاق:

تطبق السياسة على جميع الموظفين الذين يستخدمون شبكة الانترنت داخل مقر الجمعية.

السياسة:

- يُسمح بالوصول الى شبكة الانترنت لموظفي الجمعية و تستخدم لأغراض العمل فقط.
- يُسمح لزوار الجمعية باستخدام شبكة الزوار لاستخدام الإنترنت، وهي شبكة منفصلة ذات صلاحيات محدودة.

- عند استخدام الشبكة، لا يُسمح لأي شخص بأن يرسل أو ينشر أية معلومات أو مواد غير قانونية أو غير لائقة.

- على مستخدمي الشبكة عدم تبادل أو التصريح أو إفشاء أية معلومات غير مصرح بها عن الجمعية.

- لا يسمح لأي موظف الإفصاح عن كلمات المرور الخاصة بالوصول إلى شبكة الجمعية للغير.

4. استخدام البريد الإلكتروني

النطاق:

تطبق السياسة على جميع الموظفين الذين يستخدمون البريد الإلكتروني المرتبط بنطاق الجمعية (qcs.qa).

السياسة:

- يتم إنشاء بريد إلكتروني مخصص لكل من موظفي الجمعية، مرتبط بنطاق عمل الجمعية (domain)، يشمل البريد اسم المستخدم و نطاق عمل الجمعية على النحو التالي: username@qcs.qa

- لا يجوز استخدام البريد لأية أغراض شخصية.

- لا يجوز استخدام البريد الإلكتروني الشخصي لإرسال أو استقبال أية معلومات متعلقة بالعمل.

- لا يجوز انتهاك قوانين حقوق التأليف والنشر عن طريق إعادة توجيه البريد فيما يحوي من متعلقات العمل بشكل غير لائق.

- عند استخدام البريد، لا يُسمح لأي شخص بأن يرسل أو ينشر أية معلومات أو مواد غير قانونية أو غير لائقة أو تحوي اية مضايقات أو مساس بحقوق الآخرين بأي شكل من الأشكال.

- لا يجوز استخدام البريد الإلكتروني للاشتراك في أية مجموعات نقاشية او اخبارية أو غير متعلقة بذات العمل.

- عند إنشاء بريد الكتروني، على الموظف المسؤول اتباع التعليمات اللازمة لإعادة تعيين كلمة المرور المؤقتة.

- في حال حدوث أية مشكلة في إمكانية الوصول إلى البريد، على الموظف المعني التواصل مع قسم تكنولوجيا المعلومات لأخذ الاجراء المناسب.

5. سياسات وضوابط الدخول الى المعدات و أنظمة المعلومات:

النطاق:

تطبق السياسة على جميع مستخدمي أصول و أنظمة المعلومات التي تعمل تحت بإشراف قسم تكنولوجيا المعلومات.

السياسة:

- يخصص إحدى معدات الحاسوب، اسم مستخدم ، كلمة مرور خاصة لكل موظف، لتسهيل أغراض العمل و الحفاظ على سرية بيانات موظفي الجمعية

- يخصص كلمة مرور خاصة لكل موظف على كل من أنظمة المعلومات الخاصة بالجمعية.

- على كل موظف أو مستخدم الحفاظ على اسم المستخدم و سرية كلمة المرور الخاصة به.

- لا يجوز استخدام أي من معدات الحاسوب لغير أغراض العمل الرسمية.

- ينبغي حفظ سجل خاص بوقت و حالة الدخول الى كل من معدات الحاسوب و أنظمة المعلومات لدى الجمعية من قبل أي مستخدم.

- على قسم تكنولوجيا المعلومات أخذ نسخ احتياطية دورية عن بيانات أنظمة المعلومات، و استرجاعها في حال التعرض لأي طارىء.

- على مستخدم معدات الحاسوب و أنظمة المعلومات إعادة تعيين كلمة المرور المؤقتة التي تُعطى له مؤقتا عند انشاء حسابه.

- يتحمل الموظف مسؤولية إفشاء اسم المستخدم و كلمة المرور الخاصتين به الى أي طرف آخر.

- في حال حدوث أية مشكلة في إمكانية الوصول إلى معدات الحاسوب أو أنظمة المعلومات، على الموظف المعني التواصل مع قسم تكنولوجيا المعلومات لأخذ الاجراء المناسب.

6. الشبكة والوصول

النطاق:

تطبق السياسة على جميع مستخدمي شبكة الجمعية الداخلية من داخل و خارج مقر الجمعية الرئيسي.

السياسة:

- يستخدم الإتصال عن بعد لشبكة الجمعية لأغراض العمل الرسمية فقط.
- يتم الاتصال بشبكة الجمعية باستخدام أحدث التطبيقات التي تعتمد على بروتوكولات التشفير الموثوقة.
- يخصص كلمة مرور خاصة لكل موظف للاتصال عن بعد و يُحفظ سجل بجميع محاولات الدخول الى الشبكة.
- على كل موظف أو مستخدم الحفاظ على اسم المستخدم و سرية كلمة المرور الخاصة به للإتصال بالشبكة.
- يتحمل الموظف مسؤولية إفشاء اسم المستخدم و كلمة المرور الخاصتين به الى أي طرف آخر.
- يوفر قسم تكنولوجيا المعلومات لجميع الأجهزة المتصلة بالشبكة الإعدادات اللازمة لتوفير الدخول الآمن.
- يوفر قسم تكنولوجيا المعلومات برامج مكافحة الفيروسات و يتم التأكيد على إعدادات الجدار الناري (Firewall) على أجهزة و معدات الحاسوب المتصلة على شبكة الجمعية.
- يقوم قسم تكنولوجيا المعلومات بتوفير و التأكد من إعدادات جهاز الجدار الناري (Firewall، لمنع أي محاولة الدخول غير المصرح به.
- في حال حدوث أية مشكلة في إمكانية الوصول إلى شبكة الجمعية، على الموظف المعني، التواصل مع قسم تكنولوجيا المعلومات لأخذ الاجراء المناسب.

7. أمن مركز المعلومات

النطاق:

تشمل هذه السياسة مركز المعلومات، الإشراف على عمل الخوادم و تأكيد منع الدخول غير المخول إلى المركز.

السياسة:

- توضع الخوادم في مكان آمن، و تحت ظروف بيئية مناسبة.
- يمنع منعاً باتاً الدخول إلى غرفة الخوادم من قبل أي شخص غير مصرح له الا بموافقة و تحت إشراف مسؤول من قسم تقنية المعلومات.
- يتابع قسم تقنية المعلومات انتظام عمل الخوادم من خلال الاتصال عن بعد بالخادم والزيارات الدورية للتأكد من سلامة وأمن المكان.
- ينبغي متابعة سجلات الخوادم بشكل دوري من قبل قسم تقنية المعلومات و أخذ أي إجراء لازم في حالة الطوارئ.
- يقوم قسم تقنية المعلومات بعمل التحديثات الامنية بشكل دوري على أنظمة التشغيل و البرامج المنصبة على الخوادم.

8. التعافي من الكوارث واستمرارية العمل

النطاق:

استمرارية العمل هو نشاط يقوم به فريق استمرارية العمل للتأكد من استمرارية إتاحة وظائف الأعمال الهامة لجميع

الجهات بالجمعية القطرية للسرطان أو حتى فئات المجتمع والتي تستفيد من الخدمات التي تقدمها الجمعية،

حيث تكون جميع هذه الفئات بحاجة للوصول إلى الآليات التي تمكنها من أداء وظائفها ومهامها أو الاستفادة من الخدمة تحت أي ظروف. وتشمل هذه الأنشطة العديد من الأعمال اليومية مثل إدارة المشاريع، ونظام النسخ الاحتياطي، والتحكم بالتغيير، وخدمات الدعم.

البيانات وأنظمة التشغيل التي تتطلب نسخ احتياطية وإعادة تشغيل:

- البريد الإلكتروني الخاص بموظفي الجمعية
- البيانات وقواعد البيانات الخاصة بموقع الجمعية الإلكتروني
- بيانات الملفات المشتركة داخل شبكة الجمعية
- حالة أنظمة التشغيل الافتراضية اللازمة لتشغيل البرمجيات المتوفرة داخل الجمعية (Virtual Machine)
-

مصادر النسخ الاحتياطية:

- الأقراص الصلبة (External HDD)
- التخزين السحابي (Cloud Storage)

السياسة:

يوضح الجدول التالي سياسة النسخ الإحتياطي لكل من البيانات اللازمة لاستمرارية العمل لدى الجمعية:

البيانات/أنظمة التشغيل	مدة النسخ الإحتياطي	مصادر النسخ الإحتياطي
البريد الإلكتروني	يومي	تخزين سحابي
الموقع الإلكتروني	اسبوعي	تخزين سحابي
الملفات المشتركة	يومي ، اسبوعي	أقراص صلبة + تخزين سحابي
أنظمة المعلومات	يومي ، اسبوعي	أقراص صلبة + تخزين سحابي