سياسة إدارة التقنية وتكنولوجيا المعلومات

الجمعية الفيصلية الخيرية النسوية

بجدة / تصريح رقم (١٩)

الإصدار الأول	يناير ٢٠٢٣م

الفهرس

المقدمة

أُنشئت إدارة التقنية وتكنولوجيا المعلومات عام ١٤٢٩هـ-٢٠٠٨م، بهدف تعزيز قدارت الجمعية الرقمية وتوفير بيئة عمل محفزة وذات إنتاجية بما يتماشى مع احتياجتها التطويرية لمواكبة كل جديد.

ووفقاً لهذه التطلعات بذلت إدارة التقنية جهوداً كبيرة ساهمت في تحقيق نقلات نوعية على مدار الأعوام الماضية بكفاءة وجودة عالية ضمن استراتيجية متكاملة ومتوافقة مع أطر ولوائح الجمعية وقيمها الجوهرية.

وانطلاقاً من الإيمان الراسخ بأهمية التحول الرقمي وفق إمكانيات الثورة الصناعية الرابعة طبقت الجمعية الفيصلية التقنيات الحديثة لتطوير وتحسين البنية التحتية ورفع مستوى جودة الخدمات المقدمة للمستفيدين وأصحاب المصلحة والمنسوبين في كافة الجوانب الإدارية والتشغيلية لدعم سرعة اتخاذ القرار ،وتقليل الجهد، وتوفير الوقت ،وتسهيل العمليات بالإضافة إلى الحفاظ على البيانات.

يعد هذا التقرير منهجية ودليل لسياسات إدارة التقنية وتكنولوجيا المعلومات في الجمعية الفيصلية وتوثيقاً لما شهدته الجمعية من تطورات تقنية على مستوى البنية الرقمية والبرمجيات والعمليات ومؤشرات التقويم وطرق التحسين والتوصيات

المصطلحات

المصطلح	التعريف
الحوسبة السحابية Cloud Computing	هي نموذج يتيح الوصول الشبكي السهل وحسب الطلب إلى مجموعة مشتركة من الموارد الحاسوبية القابلة للتكوين مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات البرمجية التي يمكن توفيرها وإطلاقها بشكل سريع بأقل جهد إداري أو تفاعل بشري مع مقدم الخدمة.
Server الخادم	جهاز حاسوب بمواصفات خاصة عالية ، قادر على العمل لفترات طويلة جدا دون توقف ومتصل بالإنترنت على مدار الساعة بسرعة كبيرة ويحتوي على نظام تشغيل لربط البرامج مع بيئة العمل وفرض السياسات لحمايتها من الاختراق
Backup النسخ االحتياطي	هو عملية لنسخ ملفات أو قواعد بيانات بحيث يتم الاحتفاظ بهذه النسخ في حالة تعطل المعدات أو حصول أحد الاخطاء.
Antivirus نظام الحماية	مجموعة من البرامج التي صممت خصيصاً للكشف عن الفيروسات وإزالتها من أجهزة الحاسوب، بالإضافة إلى قدرتها على حماية أجهزة الحاسوب من مجموعة متنوعة من التهديدات كبرامج التجسس وبرامج أحصنة طروادة وغيرها من البرامج التي تعرف بالفيروسات
Firewall الجدار الناري	هو الجهاز الذي تقوم المنظمات بوضعه لضمان حماية أمن برامجها وملفّاتها من الاختراق والسرقة من الجهات الخارجيّة، بحيث يتمّ وضع هذا الجهاز تحديداً بين كل من الشبكة الداخلية للمنظّمة وشبكة الإنترنت، بحيث يتمّ تحديد الجهات غير المرغوب بها والتي تتسلّل إلى شبكة الكمبيوتر الداخليّة الخاصة بالمنظمة، ثم إبلاغ المشرف عن النظام بذلك كما يمكن استخدامه لتحديد المواقع التي لا يُسمح للموظّفين بالدخول إليها،
Internet الشبكة العنكبوتية	الإنترنت هو نظام اتصال عالميّ لنقل البيانات عبر أنواع مختلفة من الوسائط، ويُمكن وصفه بأنه شبكة عالميّة تربط شبكات مختلفة سواء كانت شبكات خاصّة، أو عامّة، أو تجاريّة، أو أكاديميّة، أو حكوميّة بواسطة تقنيّات لاسلكية أو ألياف ضوئية
Office 365	سحابة التطبيقات الإنتاجية المصممة للمساعدة على تحقيق أهدافك وإدارة عملك. يجمع Microsoft 365تطبيقات مثل Wordو Excelو PowerPoint بالإضافة لإمكانيو تخزين الملفات والوصول إليها ومشاركتها من أي مكان وتوفير الحماية والأمان للأجهزة في تجربة واحدة متصلة.
Data Base قاعدة بيانات	هي عبارة عن مجموعة من المعلومات المُنظّمة بطريقة تسمح الوصول إليها، وتعديلها، وإدارتها بسهولة. يتم استخدام قواعد البيانات من قِبَل المنظّمات من أجل تخزين المعلومات، واسترجاعها، وإدراتها
Email بريد إلكتروني	عبارة عن خدمة يُمكن من خلالها إرسال واستقبال رسائل إلكترونية الإنترنت وباستخدام أنواع مُختلفة من التطبيقات والبرامج
User ID معرف المستخدم	معرف فريد يعطى للمستخم لتسجيل الدخول
Password كلمة المرور	كلمة تحتوي على حروف وأرقام ورموز ليتمكن المستخدم من الدخول

المصطلحات

المصطلح	التعريف
برنامج تكسوب Techsoup	برنامج منح البرمجيات للمنظمات غير الربحية خصومات ضخمة على برامج وأنظمة وخدمات تقنية عديدة. تعد شركة التحول التقني الشريك الاستراتيجي لمنظمة تكسوب في الشرق الأوسط وشمال إفريقيا.
Enterprise Mobility + Security (EMS)	عبارة عن نظام أساسي لإدارة التنقل والأمان يساعد على حماية المنظمة وتأمينها وتمكين الموظفين من الوصول.
نظام تخطيط الموارد ERP	هو أحد أنواع أنظمة البرامج التي تساعد المنظمات على أتمتة عمليات الأعمال الأساسية وإدارتها لتحقيق الأداء الأمثل. حيث ينسق تدفق البيانات بين العمليات مما يوفر مصدرًا واحدً اللمعلومات ويقصد به في هذا الدليل: • النظام المالي (فينوس) • نظام إدارة الموارد البشرية (جسر)
نظام إدارة وصرف المساعدات العينية السحابي	نظام سحابي يدير تسليم المساعدات العينية للمستفيدين من الجمعيات الخيرية بكافة انواعها واصنافها عبر آلية موحدة ونظام واحد ، عن طريق صرف بطائق إلكترونية يتم شحنها برصيد يتناسب مع احتياجات المستفيد لبند (غذاء – كساء – دواء)
نظام إدارة الشؤون الإدارية والمستفيدين وأصحاب المصلحة	هو أحد أنواع أنظمة البرامج الخاصة التي تساعد على أتمتة عمليات الأعمال الأساسية وإدارتها لتحقيق الأداء الأمثل. حيث ينسق تدفق البيانات بين العمليات مما يوفر مصدرًا واحدً اللمعلومات ويقصد به في هذا الدليل: • خدمات مركز الأميرة حصة بنت خالد ووحدة الإسكان - (منصة غيث) • الحوكمة - (منصة غيث) • الاتصالات الإدارية (الصادر والوارد) - (منصة غيث) • الهيكل التنظيمي -(منصة غيث)
نظام خدمة العملاء	نظام يقدم حلول سحابية وخدمات عالية الجودة متكاملة لمراكز الاتصال الحديثة: • نظام الكول سنتر السحابي (كلاود كول سنتر بيفاتيل) • نظام المحادثات السحابي (سوشيال بيفاتل) ربط منصات التواصل الاجتماعي والواتساب بيزنس API • ديوان الرسائلSMS
الموقع الإلكتروني	مجموعة من الملفات والموارد ذات الصلة التي يُمكن الوصول إليها عبر شبكة الويب حيث تكون هذه الملفات والموارد مُنظمةً ومُجتمعةً تحت اسم مجال واحد، ويتواجد الموقع الإلكتروني على ما يُعرف بخوادم الويب التي تنتشر فعلياً في مواقع مُختلفة من العالم ويتم الوصول له عبر شبكة الإنترنت باستخدام أحد مُتصفحات الويب.

المصطلحات

المصطلح	التعريف
برامج المستندات وجداول البيانات والعروض	يقصد به برنامج word, Excel, PowerPoint ضمن حزمة برامج Office365
برنامج التخزين ومشاركة الملفات	يقصد به برنامج التخزين السحابي OneDrive ضمن حزمة برامج Office365
برنامج الرسائل الرسمية والمتابعة	يقصد به برنامج Outlookضمن حزمة برامج Office365
برنامج مجالس المناقشات والتعاون النصية	يقصد به برنامج MS Teamsضمن حزمة برامج Office365
الاجتماعات المرئية والصوتية	يقصد به برنامج Zoom
برنامج إدارة المشاريع والإنتاجية	يقصد به برنامج Trello
برنامج الدعم الفني عن بعد	يقصد به برنامج Anydisk
UPS	مولد الطاقة
الأمن السيبراني	هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق، أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك

السياسات والأحكام |

١. السياسة العامة للأمن السيبراني

٢. سياسة أمن أجهزة المستخدمين

٣. سياسة إدارة هويات الدخول والصلاحيات

٤. سياسة أمن البريد الإلكتروني

٥. سياسة إدارة حزم التحديثات والإصلاحات

٦. سياسة الحماية من البرمجيات الضارة

السياسات والأحكام | السياسة العامة للأمن السيبراني

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الضوابط الأساسية للأمن السيبراني

Essential Cybersecurity Controls

(ECC – 1 : 2018)

إشارة المشاركة: أبيض
تصنيف الوثيقة: غير مصنف

السياسات والأحكام | سياسة أمن أجهزة المستخدمين

الأهداف

تهدف هذه السياسة إلى توفير الحد ألدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات(Threats)الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة Confidentiality
- سلامة المعلومة Integrity
- توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني ا لتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – ١ : ٢٠١٨) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسةمتطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين داخل الجمعية

بنود السياسة

١. حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.
٢. تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات وذلك وفقاً لسياسة إدارة التحديثات المعتمدة في الجمعية
٣. تطبيق ضوابط الإعدادات والتحصين Hardening and Configuration لأجهزة المستخدمين
٤. عدم منح العاملين صلاحيات هامة وحساسة Access Privileged على أجهزة المستخدمين ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات
٥. مزامنة التوقيت Synchronization Clock مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين
٦. منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة تقنية المعلومات لامتلاك صلاحية استخدامها
٧. السماح فقط بقائمة محددة من التطبيقات على أجهزة المستخدمين .
٨. إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط Active Directory الخاص بنطاق الجمعية
٩. تطبيق سياسة مصادقة متعددة العوامل على المستخدمين(MFA) Multi-Factor Authentication لضمان الوصول الآمن إلى الموارد في الجمعية

السياسات والأحكام | سياسة أمن أجهزة المستخدمين

١٠. ضبط إعدادات أجهزة المستخدمين بإدارة الوحدات التنظيمية المناسبة Domain Controller لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة

١١. تنفيذ سياسات النطاق المناسبة Group Policy في الجمعية على جميع الأجهزة لضمان الالتزام بالضوابط التنظيمية والأمنية

متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

- ضبط إعدادات حسابات المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة للمراسلات.
- تأمين أجهزة المستخدمين مادياً داخل مبنى الجمعية

متطلبات أخرى

- التأكد من سلامة تفعيل آلية النسخ الاحتياطي على جهاز المستخدم وتوعيته بأهميته وفقاً لسياسة النسخ الاحتياطي المعتمدة في الجمعية
- حذف بيانات الجمعية المُخزّنة على أجهزة المستخدمين في حال انتهاء المهام الوظيفية بين المستخدم والجمعية.
- نشر الوعي الأمني للعاملين حول قواعد الأمن والسلامة الخاصة باستخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في الجمعية
- استخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لحماية أجهزة المستخدمين.
- مراجعة سياسة أمن أجهزة المستخدمين الشخصية سنوياً وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: إدارة تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: إدارة تقنية المعلومات.

الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصليةالالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية

السياسات والأحكام | سياسة إدارة هويات الدخول والصلاحيات

الأهداف

تهدف هذه السياسة إلى توفير الحد ألادنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات(Threats)الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة Confidentiality
- سلامة المعلومة Integrity
- توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني ا لتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – ١ : ٢٠١٨) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسةمتطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين فيها

بنود السياسة

١. إدارة هويات الدخول والصلاحيات (Identity and Access Management)

١,١ إدارة الصلاحيات

١-١-١ إنشاء هويات المستخدمين Identities User وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بالجمعية الفيصلية

١-١-٢ تطبيق سياسة مصادقة متعددة العوامل على المستحدمين(MFA) Multi-Factor Authentication لضمان الوصول الآمن إلى الموارد في الجمعية

١-١-٣ توثيق واعتماد مصفوفة Matrix لإدارة تصاريح وصلاحيات المستخدمين Authorization بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

الصلاحيات	مدراء الإدارات	أصحاب التخصصات	إدارة التقنية	جميع المستخدمين	الزائرين
File share	Least Privilege	Least Privilege	Full access	Least Privilege	لايوجد
Internet	Full Internet	Full Internet	Full Internet	Limit Internet	Limit Internet
server	لايوجد	لايوجد	Full access	لايوجد	لايوجد
Program	Least Privilege	Least Privilege	Full access	Least Privilege	لايوجد

السياسات والأحكام | سياسة إدارة هويات الدخول والصلاحيات

٤,١,١ منع استخدام الحسابات المشتركة Generic User للوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجمعية الفيصلية

٥,١,١ ضبط إعدادات جميع أنظمة إدارة الهويات والوصول ضمن نظام تسجيل ومراقبة مركزي .

٦,١,١ عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات

٢,١ منح حق الدخول

١,٢,١ متطلبات حق الدخول لحسابات المستخدمين:

- منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجمعية الفيصلية بما يتوافق مع الأدوار والمسؤوليات الخاصة به.
- اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام هوية المستخدم- User ID وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول>< اللقب>

2.2.1 متطلبات حق الوصول للحسابات الهامة والحسّاسة (السيرفرات)

بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبَق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

- تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" Root وحساب "مدير النظام" Admin وحساب "مُعرّف النظام " Sys id
- منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.
- التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر Multi-Factor Authentication (MFA) باستخدام طريقتين على الأقل من الطرق التالية:
  - المعرفة - شيء يعرفه المستخدم "مثل كلمة المرور".
  - الحيازة - شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول ويطلق عليها Password-Time-One
  - الملازمة - صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع".
- يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.
- الدخول عن بُعد إلى شبكة الجمعية الفيصلية.
- منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من مسؤول تقنية المعلومات وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA)
- حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية

السياسات والأحكام | سياسة إدارة هويات الدخول والصلاحيات

٣,٢,١ إلغاء وتغيير حق الوصول

- يجب على مسؤول الموارد البشرية تبليغ مسؤول تقنية المعلومات لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم والجمعية الفيصلية. ويقوم مسؤول تقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.
- في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها

٤,٢,١ مراجعة هويات الدخول والصلاحيات

- مراجعة هويات الدخولUser ID والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.
- تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً

٥,٢,١ إدارة كلمات المرور

تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل الجمعية الفيصلية، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم

ضوابط كلمات المرور	جميع المستخدمين All Users	حسابات المستخدمين ذات الصلاحيات الهامة والحساسة Privileged Users
الحدّ الأدنى لعدد أحرف كلمة المرور	٨ أحرف أو أرقام أو رموز	١٢ أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر ٥ كلمات مرور	تذكّر ٥ كلمات مرور
الحد الأعلى لعمر كلمة المرور	١٨٠ يوم	٤٥ يوم
مدى تعقيد كلمة المرور	مفعل	مفعل
مدة إغلاق الحساب	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق	٣٠ دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	١٠ محاولات غير صحيحة لتسجيل الدخول	١٠ محاولات غير صحيحة لتسجيل الدخول
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	٣٠ دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)
استخدام التحقق متعدد العناصر	مفعل	مفعل

السياسات والأحكام | سياسة إدارة هويات الدخول والصلاحيات

متطلبات أخرى

- يجب استخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.
- مراجعة سياسة أمن أجهزة المستخدمين الشخصية سنوياً وتوثيق التغييرات واعتمادها.
- مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العالقة.

الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات ومسؤول الموارد البشرية.

الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصليةالالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية.

السياسات والأحكام | سياسة أمن البريد الإلكتروني

الأهداف

تهدف هذه السياسة إلى توفير الحد ألدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات(Threats)الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة Confidentiality
- سلامة المعلومة Integrity
- توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني ا لتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (٢٠١٨ : ١ – ECC) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسةمتطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين فيها

بنود السياسة

١. يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية Filtering رسائل البريد الإلكتروني وحظر الرسائل المشبوهة مثل: الرسائل الإقتحامية Emails Spamورسائل التصيّد الإلكتروني Phishing Emails
٢. تطبيق خاصية التحقق من الهوية متعدد العناصر Authentication Factor-Multi للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكترونيWebmail
٣. أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.
٤. توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقاً على خوادم البريد الإلكتروني والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم
٥. توثيق مجال البريد للجمعية الفيصلية عن طريق استخدام الوسائل الالزمة؛ مثل طريقة إطار سياسة المرسل (Framework Policy Sender)لمنع تزوير البريد الإلكتروني كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة DMARC message Incoming verification
٦. يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى الجمعية الفيصلية
٧. يجب اتخاذ الإجراءات اللازمة لمنع استخدام البريد الإلكتروني للجمعية الفيصلية في غير أغراض العمل.
٨. منع وصول مسؤول النظام Administrator System إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق

السياسات والأحكام | سياسة أمن البريد الإلكتروني

٩. يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين
١٠. تذييل رسائل البريد الإلكتروني المرسلة إلى خارج الجمعية الفيصلية بشعار إخلاء المسؤولية
١١. يجب استخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لنظام البريد الإلكتروني.

الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات .

الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصليةالالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية.

السياسات والأحكام | سياسة إدارة حزم التحديثات والإصلاحات

الأهداف

تهدف هذه السياسة إلى توفير الحد ألدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات(Threats)الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة Confidentiality
- سلامة المعلومة Integrity
- توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني ا لتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – ١ : ٢٠١٨) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسةمتطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين في الجمعية.

بنود السياسة

١. إدارة حزم التحديثات والإصلاحات بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة.
٢. تنزيل حُزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل الجمعية الفيصلية مره واحدة شهرياً على الأقل.
٣. استخدام أنظمة تقنية موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.
٤. وضع خطة للاسترجاع وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات.
٥. جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.
٦. في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة.
٧. . تنصيب التحديثات والإصلاحات للأصول التقنية على النحو التالي:

الأصل	المدة
أنظمة التشغيل	أسبوعياً
التطبيقات	أسبوعياً
قواعد البيانات	٣ أشهر
أجهزة الشبكة	شهرياً

السياسات والأحكام | سياسة إدارة حزم التحديثات والإصلاحات

٨. يجب استخدام مؤشر قياس الأداء KPI لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.
٩. مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها

الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: مسؤول تقنية المعلومات ومسؤول الموارد البشرية.

الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصليةالالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية.

السياسات والأحكام | سياسة الحماية من البرمجيات الضارة

الأهداف

تهدف هذه السياسة إلى توفير الحد ألادنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات(Threats)الداخلية والخارجية. وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة Confidentiality
- سلامة المعلومة Integrity
- توافر المعلومة Availability

تتبع هذه السياسة متطلبات الهيئة الوطنية للأمن السيبراني ا لتي قامت بتطوير الضوابط الأساسية للأمن السيبراني (ECC – ١ : ٢٠١٨) بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسةمتطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

نطاق العمل

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بالجمعية الفيصلية، وتنطبق على جميع العاملين فيها.

بنود السياسة

- تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها وضبط إعداداتها وفقاً للمعايير التقنية الأمنية المعتمدة في الجمعية الفيصلية
- تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة Malware وإدارتها بشكل آمن.
- التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل (الفيروسات) Virus،(وأحصنة طروادة) Horse Trojan،(والديدان) Worms،(وبرمجيات التجسس) Spyware ،(وبرمجيات الإعلانات المتسللة) Adware،(ومجموعة الجذر) Root Kits .
- التأكد من ملائمة تقنيات وآليات الحماية لأنظمة التشغيل الخاصة بالجمعية الفيصلية Windows.
- تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.
- ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد االلكتروني الواردة والصادرة.
- يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت والمعروفة باستضافتها لبرمجيات ضارة.

السياسات والأحكام | سياسة الحماية من البرمجيات الضارة

- القيام بعمليات مسح اسبوعياً لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.
- تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والاصلاحات.
- إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها)مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ
- إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.
- على مسؤول تقنية المعلومات التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من خطورتها.
- استخدام مؤشر قياس الأداء KPI ضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

الأدوار والمسؤوليات

- راعي ومالك وثيقة السياسة: مسؤول تقنية المعلومات.
- مراجعة السياسة وتحديثها: مسؤول تقنية المعلومات.
- تنفيذ السياسة وتطبيقها: المدير التنفيذي ومسؤول تقنية المعلومات .

الالتزام بالسياسة

- على مسؤول تقنية المعلومات ضمان التزام الجمعية الفيصلية بهذه السياسة دورياً.
- على إدارة تقنية المعلومات وجميع الإدارات في الجمعية الفيصليةالالتزام بهذه السياسة.
- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب إجراءات المتبعة في الجمعية الفيصلية.

الأهداف

- تعزيز قدارت الجمعية الرقمية وتوفير بيئة عمل محفزة وذات إنتاجية بما يتماشى مع احتياجاتها التطويرية لمواكبة كل جديد.
- تطوير وتحسين البنية التحتية مع ضمان قابلية التوسع ضمن معايير قياسية.
- رفع مستوى جودة الخدمات المقدمة للمستفيدين وأصحاب المصلحة ومتابعة تطويرها.
- ضمان الالتزام والامتثال التنظيمي وتمكين المنسوبين من سرعة اتخاذ القرار في كافة الجوانب الإدارية والتشغيلية لتحقيق مبدأ الشفافية المطلوبة في ممارسة الأعمال.
- ابتكار الحلول المستدامة لتسريع نمو الأعمال بدقة وجودة عالية .
- تقليل الجهد والتكلفة، وتوفير الوقت.
- تعزيز تبني إطار عمل مبني على التعاون والابتكار.

دائرة تقنية المعلومات

ختاماً:

تطبق هذه السياسات ضمن أنشطة الجمعية الفيصلية وعلى أعضاء مجلس الإدارة وجميع العاملين الذين يعملون تحت إدارة واشراف الجمعية الاطلاع على الأنظمة المتعلقة بهذه السياسات والإلمام بها والالتزام بما ورد فيها من أحكام عند أداء واجباتهم ومسؤولياتهم الوظيفية ونشرها على الموقع الإلكتروني للجمعية وفق الصيغة المرفقة بالاعتماد.

المرجع:

مراجعة واعتماد أصحاب الصلاحية :

عُرض في مجلس الإدارة الجلسة رقم (1) بتاريخ 1444/6/17 هـ الموافق 2023/1/10م ضمن جدول الأعمال (بند رقم 3) وهو الاطلاع على قرارات اللجنة التنفيذية واعتمادها لتحديث لوائح وسياسات وأنظمة الجمعية الفيصلية الذي تم مراجعتها في اللجنة التنفيذية جلسة رقم (9) بتاريخ 1444/5/21 هـ الموافق 15 ديسمبر 2022 م.

"تم الاطلاع واعتماد هذه السياسة والعمل بموجبها من تاريخ الاعتماد"

توقيع واعتماد مجلس الإدارة

ت	أعضاء مجلس الإدارة	التوقيع
١	السيدة خيرية محمد نور ناصر رحيمي	
٢	السيدة أميمة محمد علي عبد الواحد مغربي	
٣	السيدة فاطمة محمد عباس فارسي	
٤	الدكتورة سعاد عبود ابو بكر بن عفيف	
٥	الدكتورة سها محمود سعد علاوي	
٦	الدكتورة عبلة عبد الحميد محمد بخاري	
٧	الدكتورة ندى عمر على العولقي	
٨	السيدة أماني أحمد محمد مظهر	
٩	السيدة عبير غازي هاشم جليدان	
١٠	السيدة لنا احمد عبد القادر شيناوي	
١١	السيدة لينا عمر صديق بن صديق	
١٢	السيدة هلا عبد الله هاشم السقاف	
١٣	الدكتورة مريم عبد الله سرور الصبان	

شكرا