السياسات العامة لأمن المعلومات
في الجهات الحكومية

سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة

م / عمار الجحافي

بنود السياسة

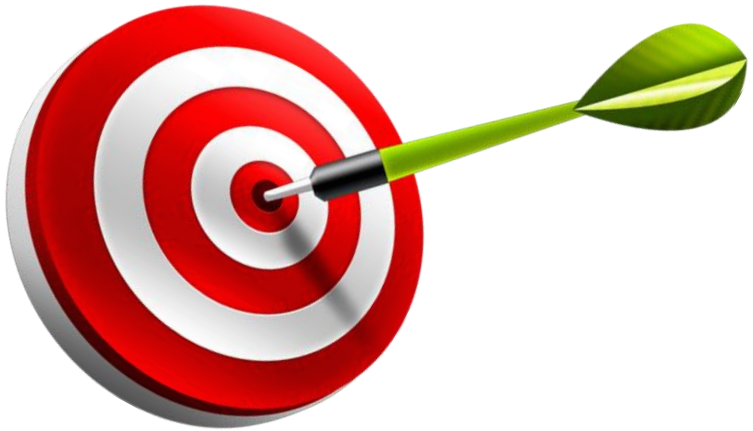
- يجب تنصيب برامج موثوقة ومرخصة لمكافحة الفيروسات والبرامج الخبيثة على جميع أجهزة الحاسوب المملوكة للجهة الحكومية من خوادم، وأجهزة محمولة، وأجهزة مكتبية، مع متابعة تحديثها بشكل مستمر.
- عند ظهور فيروسات لا تستطيع برامج مكافحة الفيروسات الكشف عنها والتخلص منها، فإنه يجب على الدعم الفني للجهة الحكومية الاتصال بالدعم الفني صاحبة المنتج، ومحاولة مكافحة الفيروس بأنفسهم بأسرع وقت ممكن.
- يجب فحص الملفات المنقولة عبر شبكات الحاسوب للجهة باستخدام برامج مكافحة الفيروسات من أجل التأكد من خلوها من البرامج الخبيثة.
- على الجهة الحكومية إجراء تقييم بين فترة وأخرى للتأكد من مدى مطابقة برامج مكافحة الفيروسات وإعداداته بما يتوافق مع سياسات أمن وحماية المعلومات.
- على الجهة الحكومية تطبيق الفقرات الخاصة بالتعامل مع البرامج الخبيثة في سياسات البريد الإلكتروني.
- يمنع استخدام وسائط التخزين والملفات من المصادر مجهولة الأصل إلا بعد فحصها وتنظيفها من الفيروسات والشيفرات الخبيثة.
- يمنع الموظفون من تطوير أو تشغيل أو نسخ أو نشر فيروسات الكمبيوتر أو الشفرات الخبيثة.
- يجب على الجهة الحكومية أن تنفذ تدابير مناسبة لحماية أجهزة الاتصال اللاسلكية أو الأجهزة الحاسوبية المتنقلة من الفيروسات والشيفرات الخبيثة.

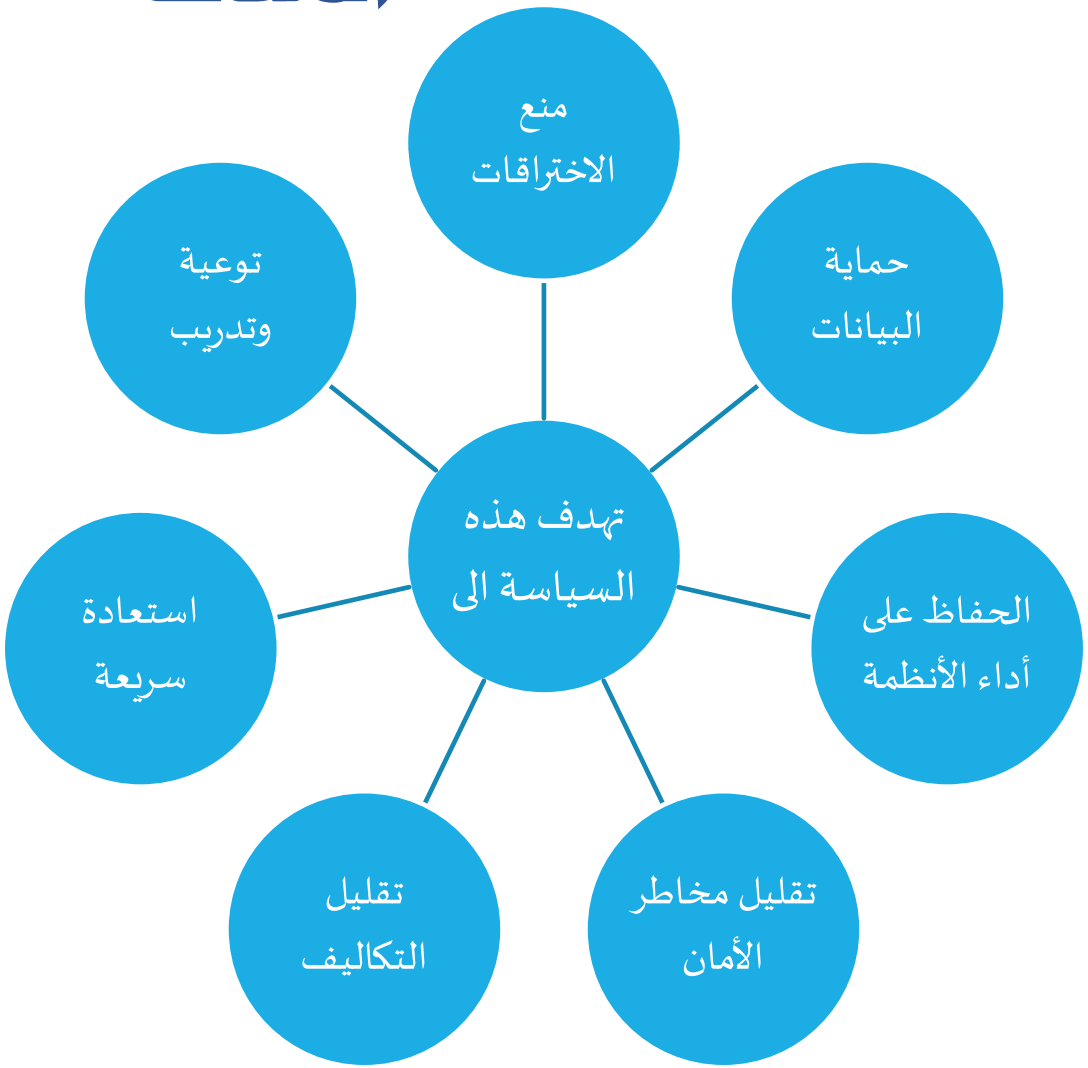
المقدمة

تعد الفيروسات خطرا كبيرا على البيانات وأنظمة المعلومات وأنظمة التشغيل فهي تسبب في وجود مخاطر كبيرة وتهديدات على هذه الأنظمة وقد تسبب الى فقدان المعلومات وافسادها مما يؤدي الى ضرر يصيب جهة العمل.

وبهدف منع واكتشاف التهديدات الأمنية المتعلقة بالبرامج الضارة (الفيروسات والشفرات الخبيثة) التي يمكن أن تؤثر على أمان وأداء الأجهزة والبيئات الرقمية داخل الجهة وجب على الجهة وضع سياسة خاصة بالحماية من الشفرات الخبيثة وفيروسات الأجهزة.

الهدف

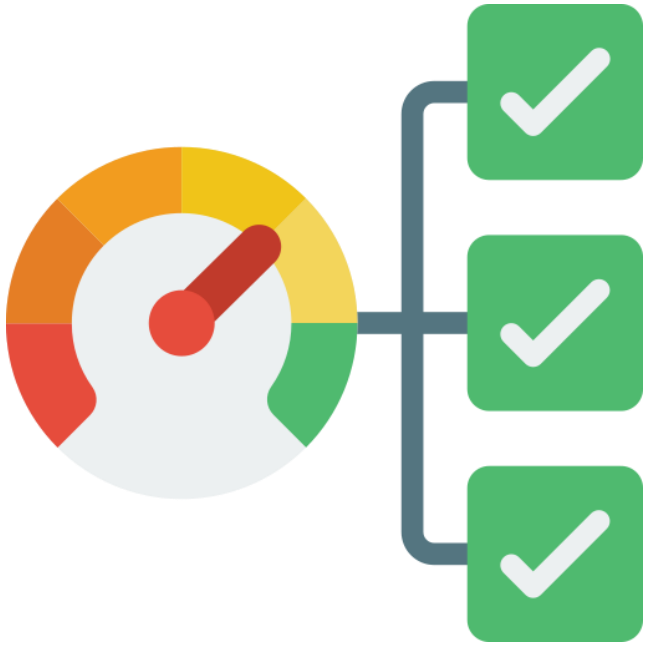



تهدف هذه السياسة الى
منع الاختراقات
حماية البيانات
الحفاظ على أداء الأنظمة
تقليل مخاطر الأمان
تقليل التكاليف
استعادة سريعة
توعية وتدريب

النطاق

تنطبق هذه السياسة على الأجهزة والأنظمة والتطبيقات والشبكات في الجهة. كما تنطبق على مسئولي أمن المعلومات والبنى التحتية والمستخدمين داخل الجهة والأطراف ذات العلاقة.

الأدوار والمسئوليات



❖ مسئوليات الجهة

- تلتزم الإدارة العليا في الجهة باعتماد سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة.

❖ مسئوليات مدير أمن المعلومات

- المسؤول الرئيسي عن تنفيذ وإدارة سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة داخل الجهة.
- يعمل على تقييم المخاطر وتحليل التهديدات الأمنية ويطبق الإجراءات الوقائية المناسبة فيما يخص هذه السياسة.
- يضمن تنفيذ وصيانة الحلول التقنية للحماية والكشف عن الشفرات الخبيثة والفيروسات.
- إذا استلزم أي تغيير على موارد المعلومات نتيجة مكافحة الفيروسات والبرامج الخبيثة فيجب الخضوع لسياسة التغيير.
- يقيم أداء السياسة والتدابير الأمنية بشكل دوري ويقدم تقارير حول الامتثال والتحسينات المطلوبة

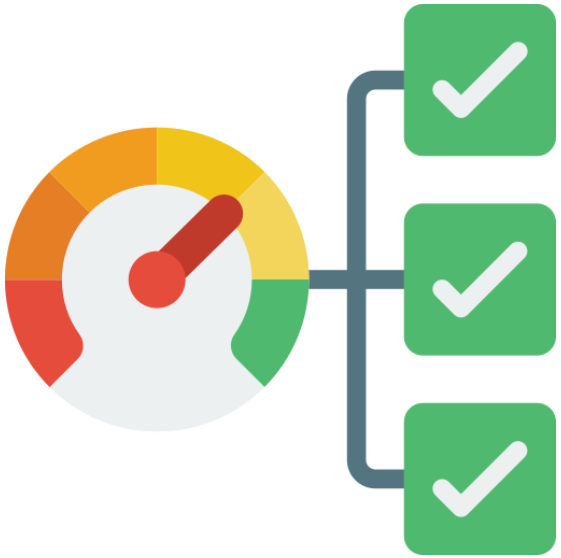
الأدوار والمسئوليات

❖ مسئوليات مهندسي الشبكات أو أمن المعلومات

- تحديث برامج المكافحة للفيروسات والبرامج الخبيثة بشكل دوري وفقا لأخر تحديث وعند عدم القدرة على التحديث من الانترنت فيجب إيجاد حلول بديله لذلك.
- مراقبة عمليات التحديث لبرامج مكافحة الفيروسات.
- التأكد من اقفال المنافذ التي لا تستخدمها الأنظمة والتي تستغلها الفيروسات والبرامج الخبيثة كثغرات
- التأكد من النسخ الاحتياطي بشكل دوري للبيانات والأنظمة حتى يتم الاستعادة لها في حالة ان سببت الفيروسات والبرامج الخبيثة لاي تغيير او تخريب.
- مراقبة وكشف عن التهديدات الأمنية واتخاذ الإجراءات الضرورية.
- تقديم الدعم الفني للمستخدمين فيما يتعلق بقضايا الأمان والشفرات الخبيثة.
- العمل على تطوير وتحسين البنية التحتية لأمن المعلومات.

❖ مسئوليات المستخدمين

- الالتزام بتطبيق بنود السياسة.
- في حالة ظهور أي رسائل تحذيرية على وجود فيروسات او برامج خبيثة فانه يجب رفع تقرير للمدير المسئول
- عدم استخدام البرامج غير المرخصة او التجريبية وإذا استلزم ذلك فانه يجب الخضوع لسياسة التغيير
- عدم استخدام أي وسائط تخزين الا بعد التأكد من خلوها من الفيروسات والبرامج الخبيثة



سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة

انتهى،،،