السياسات العامة لأمن المعلومات
في الجهات الحكومية

سياسة التشفير

م / عمار الجحافي

بنود السياسة

- في حال تبادل المعلومات الحساسة عبر الشبكات أو البريد الإلكتروني، يجب أن تعتمد الجهة الحكومية على تقنيات التشفير وذلك لضمان سرية وسلامة ومصداقية هذه المعلومات وبالتوافق مع سياسات تصنيف وحساسية المعلومات.
- استخدام خوارزمية تشفير مثبتة ومعتمدة عالمياً، أو أي خوارزميات يتم الموافقة عليها من قبل الجهة المختصة بذلك.
- وضع التعليمات المناسبة التي تضمن إجراء عملية التشفير وفك التشفير بطريقة آمنة وصحيحة.
- تحديد وتوثيق أسماء الموظفين المخولين الذين يجب أن تصرف لهم مفاتيح تشفير وبرامج تشفير حسب متطلبات أعمالهم.
- وضع التعليمات التي تحدد كيفية التعامل مع الوثائق والملفات التي تم فقدانها أو الإفصاح عن مفاتيح تشفيرها أو فك تشفيرها بشكل غير مرخص.

بنود السياسة

- وضع التعليمات الخاصة بإدارة مفاتيح التشفير، على أن تراعى فيها الأمور التالية:
  - ✓ حفظ نسخ احتياطية عن مفاتيح التشفير الخاصة بالإدارة في مكان آمن لاستعمالها عند الحاجة.
  - ✓ مواصفات الأنظمة والبرمجيات المستخدمة في إدارة مفاتيح التشفير طوال دورة حياتها.
  - ✓ اعتماد أو إلغاء اعتماد مفاتيح التشفير (عند الإفصاح عنها بشكل غير مرخص أو استقالة الموظف مثلاً).
  - ✓ يجب تحديد مدة صلاحية المفاتيح وتغييرها بصورة دورية.
  - ✓ يجب تحديد الحد الأدنى لأطوال مفاتيح التشفير المستخدمة.
  - ✓ إدارة مفاتيح التشفير داخل الجهة الحكومية بشكل آمن.

المقدمة

يقصد بسياسة التشفير بانها مجموعة من السياسات والإجراءات التي تحدد كيفية استخدام وتنفيذ آلية التشفير في الجهة.

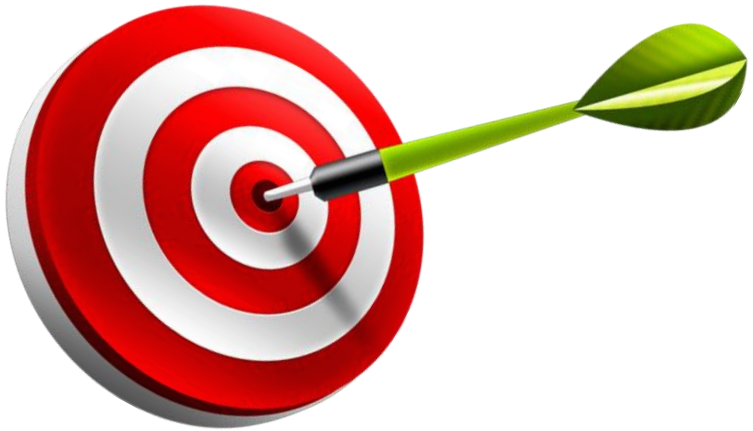
والتشفير هو عملية تحويل البيانات من نصوص ومعلومات قابلة للقراءة إلى شكل مشفر غير قابل للقراءة إلا بواسطة أولئك الذين يمتلكون المفتاح الصحيح لفك التشفير وذلك لضمان سرية وسلامة هذه المعلومات وهناك عدة طرق للتشفير وعلى الجهة تطبيق ما يناسبها في الأنظمة الخاصة بها.

فسياسة التشفير تعتبر أمراً هاماً في أمان المعلومات وتهدف إلى حماية البيانات الحساسة والمعلومات السرية من الوصول غير المصرح به.

الهدف

تهدف هذه السياسة الى

- حماية سرية وسلامة البيانات
- تمكين التبادل الآمن
- الامتثال للقوانين
- صد الهجمات السيبرانية

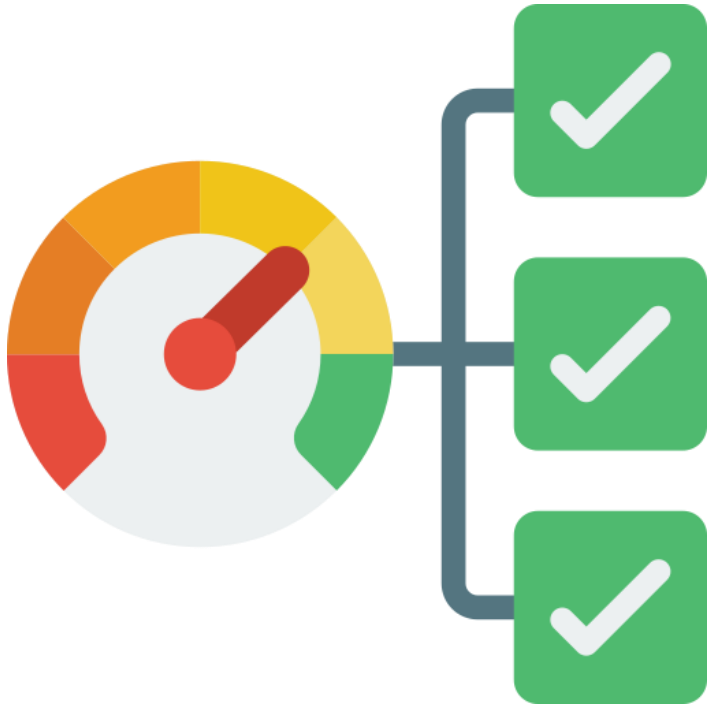


النطاق

جميع الاصول المعلوماتية الإلكترونية الخاصة بالجهة المحمية أو الحساسة على النحو المحدد في سياسة تصنيف البيانات.

تطبق على جميع العاملين في الجهة، بما في ذلك الجهات التي تتعامل معها والاطراف الخارجية.

الأدوار والمسئوليات



❖ مسئوليات الجهة

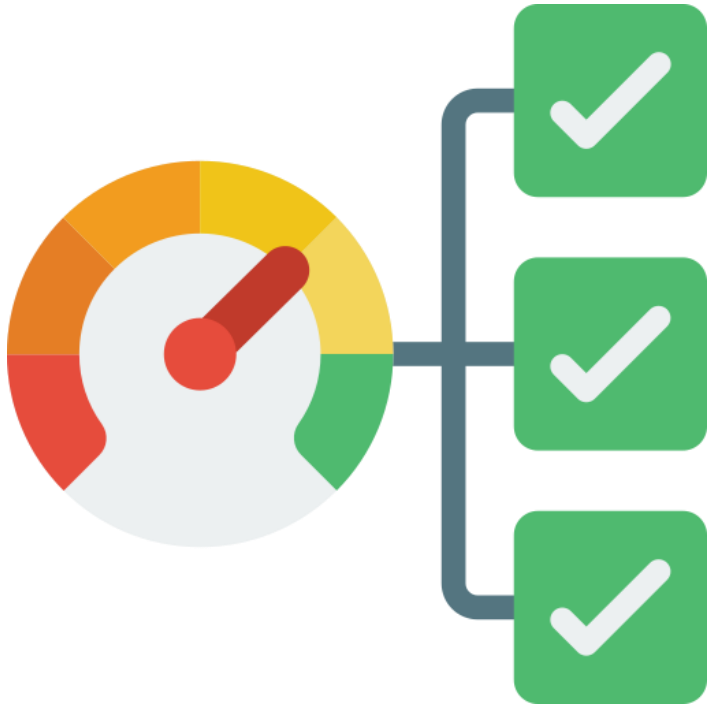
- اعتماد سياسة التشفير لضمان حماية بيانات الجهة من الكشف الغير مصرح به.

❖ مسئوليات إدارة نظم المعلومات أو تطوير البرمجيات

- الاشراف على تكوين أنظمة التشفير وضمان أداءها الأمني.
- ضمان تشفير البيانات الحساسة في قواعد بيانات نظم المعلومات وفق أفضل الممارسات.

الأدوار والمسئوليات

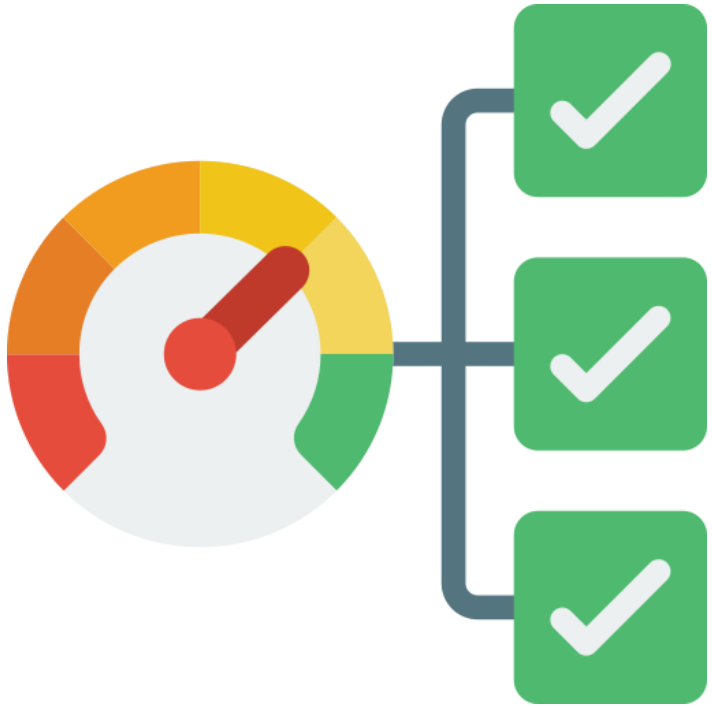
❖ مسئوليات إدارة أمن المعلومات



- تنفيذ وإدارة وتحديث سياسة التشفير والإشراف عليها.
- تحديد وتوجيه استراتيجيات التشفير والتقنيات المستخدمة اما تصميم خوارزمية جديدة او استخدام خوارزمية تشفير مثبتة ومعتمدة عالميا.
- تحديد وتوثيق أسماء الاشخاص المخولين لإدارة مفاتيح وبرامج تشفير.
- وضع التعليمات المناسبة التي تضمن إجراء عملية التشفير وفك التشفير بطريقة آمنة وصحيحة.
- القيام باستراتيجيات النسخ الاحتياطي والاستعادة لمفاتيح التشفير.
- القيام بالتدريب والتوعية حول التشفير للموظفين.
- الاطلاع على أحدث تقنيات التشفير، واقتراح تقنيات تشفير أفضل، أو مفاتيح تشفير أطول لمواكبة التقدم في أمن لمعلومات، ومن ثم اعتماد تلك المقترحات.

الأدوار والمسئوليات

❖ مسئوليات إدارة الشبكات والسيرفرات



- تحديد الطرق أو التقنيات المناسبة لتشفير المجلدات/الملفات/سواقات الاقراص المحلية/وسائط التخزين المتنقلة التي تحتوي على بيانات حساسة قبل خزنها أو نقلها، واعتمادها من قبل الإدارة العامة لنظم المعلومات، ومن ثم تدريب المستخدمين عليها.
- مراقبة التزام المستخدمين ببنود سياسة التشفير أثناء استخدام الشكبة.

انتهى،،،