



السياسات العامة لأمن المعلومات
في الجهات الحكومية



سياسة أمن الشبكة
NETWORK SECURITY
POLICY

م / محمد الجائفي

المحاور



بنود سياسة امن الشبكة

المقدمة

الاهداف

نطاق تطبيق السياسة

مكونات أمن الشبكة

من أهم الحلول والتكنولوجيا الأمنية للشبكة

الخطوات الأساسية لإعداد سياسة أمن الشبكة للجهة حكومية

الأدوار والمسئوليات

بنود سياسة أمن الشبكة

يجب أن تتضمن خطة أمن المعلومات للجهة
الحكومية على ما يلي:



بنود سياسة أمن الشبكة

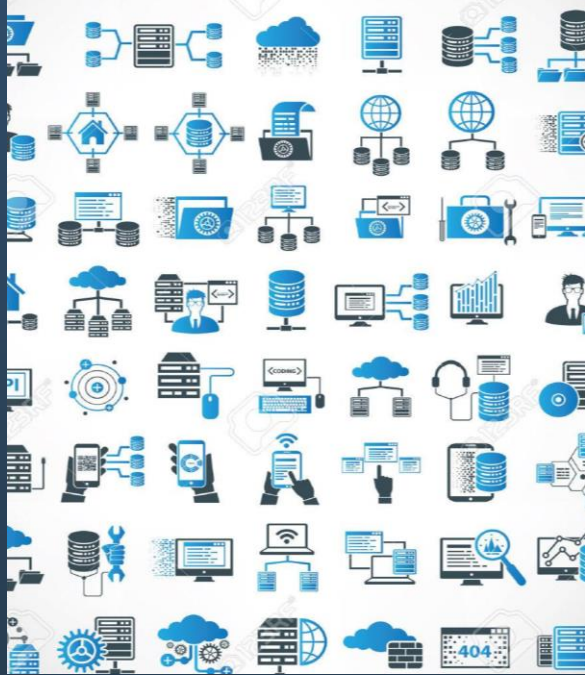


وزارة الإعلام والعلاقات العامة

السياسات العامة لأمن المعلومات
في الجهات الحكومية



وضع التعليمات المناسبة في التعامل مع عناصر الشبكة المعلوماتية المملوكة للجهة الحكومية، وشرائها، أو إصلاحها، أو نقلها، أو إتلافها، بما يتفق مع سياسات أمن وحماية المعلومات عامة وسياسات تصنيف وحساسية المعلومات



وضع التعليمات والضوابط الخاصة بربط عناصر الشبكة بأي معدات أو بالشبكة المعلوماتية للجهة الحكومية بنوعيتها السلكية واللاسلكية



يمنع الإفصاح عن عناوين وإعدادات أي من أنظمة الشبكة الداخلية التابعة للجهة الحكومية دون موافقة الجهة



بنود سياسة أمن الشبكة



وزارة الإعلام والعلاقات العامة

السياسات العامة لأمن المعلومات
في الجهات الحكومية



يجب حماية جميع الشبكات الداخلية المتصلة مع شبكة حكومية أو شبكة عامة أخرى بشكل صحيح

وضع كلمات مرور سرية مناسبة للدخول إلى الشبكة تعطى للأشخاص المخولين بالتوافق مع سياسات النفاذ والدخول

توفير الحد الأدنى لسرعة الشبكة بحيث يتم ضمان قدرة هذه السرعة على تلبية متطلبات العمل الخاصة بالجهة سواء كانت محلية أو واسعة النطاق



بنود سياسة أمن الشبكة



وزارة الاتصال وتقنية المعلومات

السياسات العامة لأمن المعلومات
في الجهات الحكومية



يمنع الموظفون الموصولة أجهزتهم بالشبكة الداخلية من الاتصال بأي شبكة خارجية بأي شكل من الأشكال إلا بموافقة الجهة المختصة

لا يجوز للموظفين ربط أي جهاز نظم معلومات غير مصرح به إلى الشبكة الحكومية دون الحصول على موافقة الجهة المختصة

يجب أن يتم مراجعة إعدادات وإدارة أنظمة الاتصال والمعلومات بشكل دوري

يجب ان يتم مراعاة امن المعلومات عند تصميم ومعمارية الشبكات بحيث توفر قدر مناسب من العزل والاستقلالية لضمان الحماية والسرية وبما يستلزمه احتياج العمل

يجب ان لا تؤثر عملية الاتصال مع أي شبكة أخرى على المعايير الأمنية لطرفي الاتصال

يمنع توصيل الموارد الحاسوبية المملوكة للموظفين بالشبكة الداخلية دون إذن مسبق من إدارة أمن الشبكات أو الجهة المختصة، وتمنح الجهة الحكومية موافقة استخدام هذه الموارد الشخصية بمعايير مطابقة لسياسات أمن المعلومات

بنود سياسة أمن الشبكة



وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات
في الجهات الحكومية



يجب تشفير المعلومات المصنفة تصنيفاً خاصاً عند نقلها من خلال اتصال خارجي غير آمن

يجب تشفير المعلومات المصنفة تصنيفاً عالي السرية عند نقلها داخل الشبكة المحلية على أن تكون آلية التشفير متوافقة مع سياسات أمن المعلومات

في حال وجود شبكات لاسلكية، يجب على الجهة الحكومية التوثيق والمراقبة والتحكم في الشبكات اللاسلكية المتصلة بشبكة الحكومة الداخلية ووضع الضوابط والإجراءات المناسبة لتشغيلها وإدارتها

يجب إتباع الضوابط الأمنية السليمة من توثيق الدخول واستخدام التشفير لحماية البيانات المنقولة عبر الشبكات اللاسلكية المتصلة مع شبكة الحكومة الداخلية

يمنع الوصول الى تجهيزات أو شبكة أو أنظمة الجهة الحكومية الداخلية من خارج الجهة عبر شبكة الإنترنت مباشرة أو باستخدام تقنيات الشبكة الظاهرية الخاصة بالضرورة القصوى وعبر إجراءات وآليات عمل وتصاريح موثقة وبشكل محدود وآمن وبعد موافقة من إدارة / قسم أمن المعلومات أو الجهة المختصة

المقدمة



يمكن تعريف أمن الشبكة على انها مجموعة من القواعد والإجراءات التي تهدف إلى حماية البيانات والمعلومات وضمان سلامة الشبكات الحاسوبية من كافة المخاطر والتهديدات التي من الممكن ان تواجهها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية،

لتأمين وحماية الشبكة يجب وضع سياسة تتضمن الضوابط والتعليمات المناسبة التي تساعد في كيفية التعامل مع عناصر الشبكة المعلوماتية وتأمينها، كما يجب أن تتكيف سياسة أمن الشبكة مع احتياجات الجهة الحكومية. على ان يتم بمتابعة التطورات التكنولوجية والتهديدات الأمنية الجديدة وتحديث سياسة أمن الشبكة بشكل منتظم للتأكد من توافقها مع التطورات والتحديات الجديدة.

النطاق

تطبق هذه السياسة على كافة العناصر والمكونات والأصول المعلوماتية المتعلقة عملها بالشبكة واسعة النطاق وبنوعها السلكية واللاسلكية، والتي تشكل البنية التحتية لشبكة المعلومات والاتصالات، وعلى البيانات والمعلومات المخزنة التي تمتلكها الجهة سواء التي يتم معالجتها واستخدامها داخل الجهات الحكومية أو خارجها، وعلى كافة العاملين في الجهة والمستخدمين المتصلة أجهزتهم بالشبكة.

الأهداف

تهدف هذه السياسة الى:

- تحديد ووضع المتطلبات والضوابط الأساسية واللازمة لأمن الشبكة المعلوماتية والإجراءات اللازمة لحماية المعلومات تحت سيطرة وتحكم الجهة الحكومية.
- توفير إطار عمل يحدد المبادئ والإرشادات والمتطلبات الأمنية التي يجب اتباعها لحماية الشبكة من التهديدات الداخلية والخارجية.
- توضيح كيفية التعامل مع عناصر الشبكة المعلوماتية بشكل آمن، وتحديد الاحتياجات المطلوب توافرها في هذه المكونات لضمان أمن وحماية الأنظمة المتصلة بهذه الشبكة، من أجل الوصول إلى شبكة مستقرة وأمنة تلي متطلبات عمل الجهة.

مكونات واهداف سياسة أمن الشبكة المعلوماتية

ضمان سرية جميع موارد ومكونات الشبكة المعلوماتية

ضمان وحماية سلامة البيانات

الحفاظ على توافريه تجهيزات البنية التحتية لتكنولوجيا المعلومات

فرض وتطبيق التحكم في الوصول

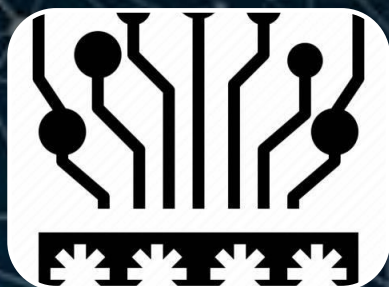
مراقبة بيئة تكنولوجيا المعلومات للتأكد من عدم انتهاك السياسة



من أهم الحلول والتكنولوجيا الأمنية للشبكة



Physical Security



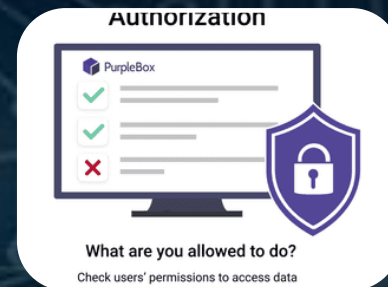
Encryption



Access Control



Node authentication



Access Rights (Authorization)



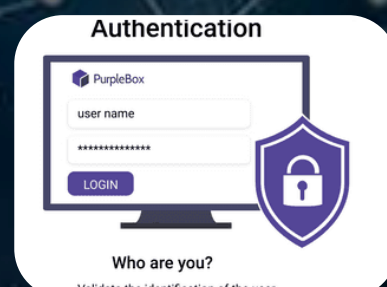
Antivirus software



Routing Control



Firewalls, IDS, IPS



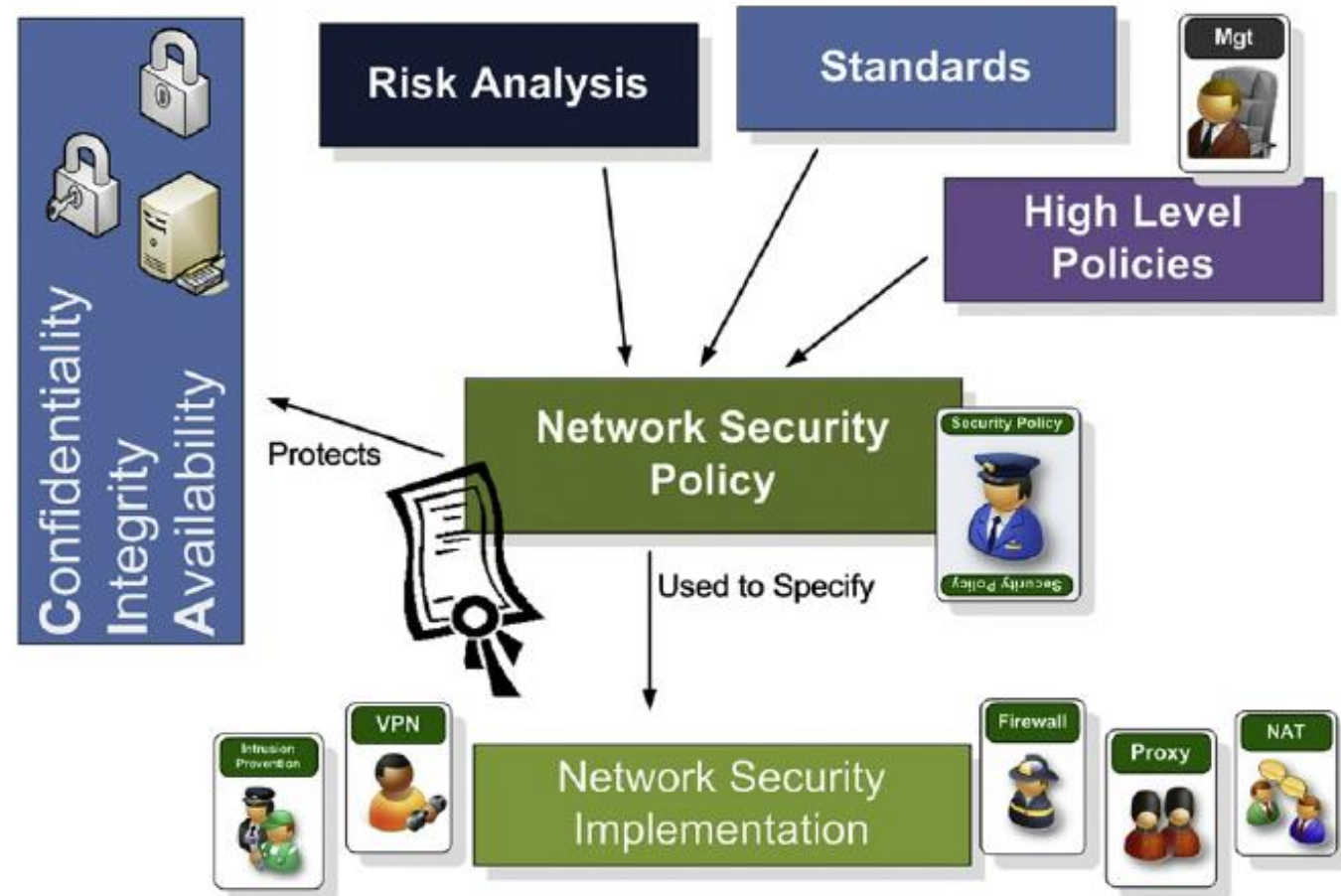
User authentication

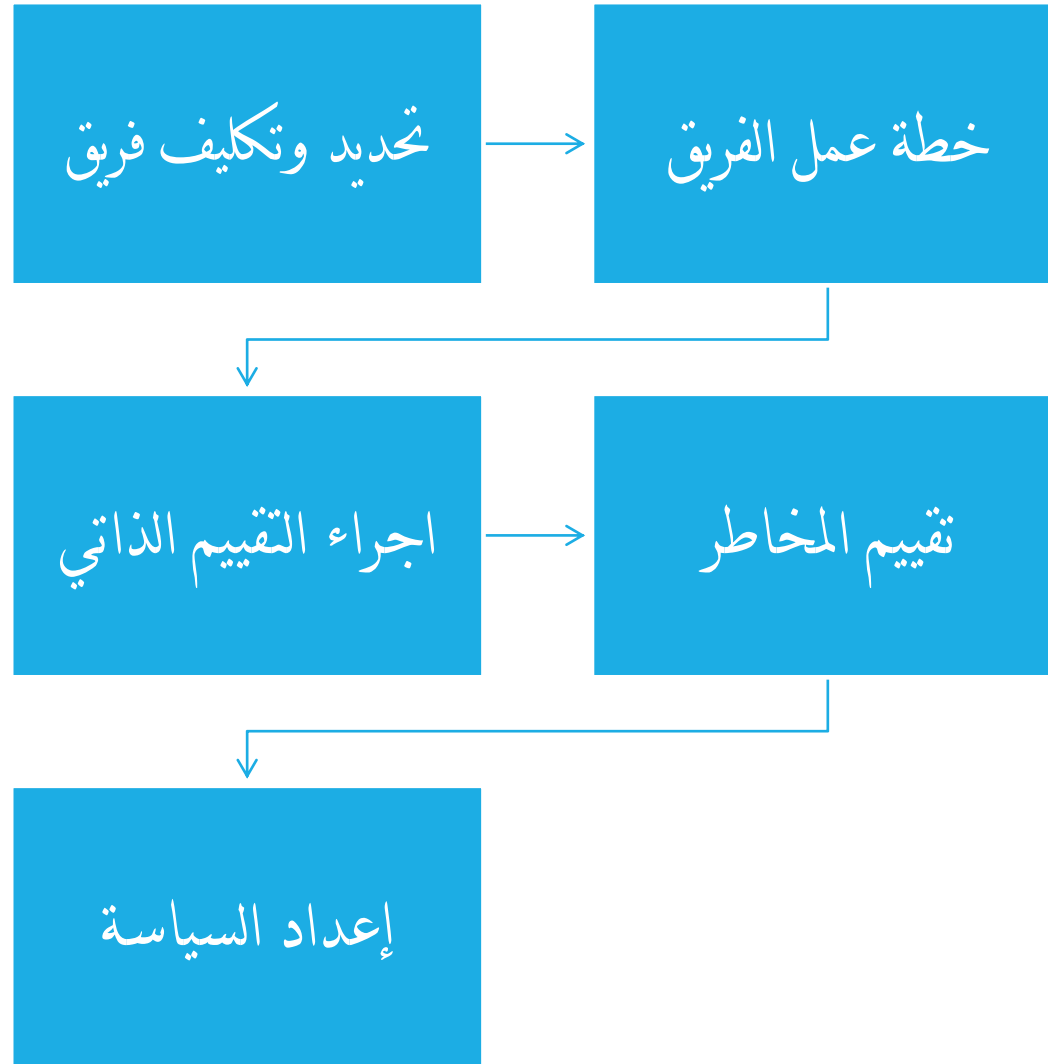


Passwords and Passphrases



Token & Digital signature





الخطوات الأساسية لإعداد سياسة أمن الشبكة لجهة حكومية

الخطوات الأساسية لإعداد سياسة أمن الشبكة للجهة حكومية

- تقوم قيادة الجهة الحكومية بتكليف فريق مسؤول عن إعداد السياسة خلال فترة زمنية محددة وتحديد أدوار ومسئوليات الفريق.

1. تحديد وتكليف فريق

- يعد الفريق خطة عمل تفصيلية تحدد الإجراءات اللازمة لإعداد السياسة، والخطوات التي يجب اتخاذها من قبل الفريق تحتوي على الأهداف، والنطاق، والمراحل، والمهام.

2. خطة عمل الفريق

- تحديد نقاط الضعف والثغرات الامنية في الشبكة عن طريق تحليل المعلومات التي سيتم تجميعها من معرفة وفهم المتطلبات وعمل استبيان بواسطة الفريق المكلف.

3. اجراء التقييم الذاتي

- تحديد الاصول المعلوماتية للشبكة، وتحديد الثغرات والتهديدات الأمنية ومدى تأثيرها في حال حدوثها (أثر ونوع التهديد على الجهة واحتمالية حدوثه)، وتصنيف المخاطر مثل (عالي، متوسط ومنخفض)

4. تقييم المخاطر

- يتم اعداد السياسة والتي تتكون من مقدمة عن السياسة، الهدف ، النطاق، والمسئوليات والأدوار لتطبيق السياسة، وكذلك الامتثال للسياسة.

5. إعداد السياسة

الأدوار والمسؤوليات

من أهم مسؤوليات الإدارة العليا في الجهة

وضع التعليمات المناسبة في التعامل مع عناصر الشبكة المعلوماتية المملوكة للجهة الحكومية، وشرائها، إصلاحها، نقلها، أو إتلافها، بما يتفق مع سياسات أمن وحماية المعلومات عامة وسياسات تصنيف وحساسية المعلومات.

وضع التعليمات والضوابط الخاصة بربط عناصر الشبكة بأي معدات أو بالشبكة المعلوماتية للجهة الحكومية بنوعها السلكية واللاسلكية.

وضع الصلاحيات المناسبة للأشخاص المتخصصين بتشغيل وصيانة وإدارة عمل الشبكات اعتماداً على الوصف الوظيفي لكل منهم

توفير الحد الأدنى لسرعة الشبكة بحيث يتم ضمان قدرة هذه السرعة على تلبية متطلبات العمل الخاصة بالجهة سواءً كانت محلية أو واسعة النطاق.

في حال وجود شبكات لاسلكية، يجب على الجهة الحكومية التوثيق والمراقبة والتحكم في الشبكات اللاسلكية المتصلة بشبكة الحكومة الداخلية ووضع الضوابط والإجراءات المناسبة لتشغيلها وإدارتها.

يجب إتباع الضوابط الآمنة السليمة من توثيق الدخول واستخدام التشفير لحماية البيانات المنقولة عبر الشبكات اللاسلكية المتصلة مع شبكة الحكومة الداخلية.

وضع كلمات مرور سرية مناسبة لدخول إلى الشبكة تعطي للأشخاص المخولين بالتوافق مع سياسات النفاذ والدخول .

مراجعة إعدادات وإدارة أنظمة الاتصال والمعلومات بشكل دوري.

توفير الأجهزة التي تدعم حماية الشبكة مثل أجهزة الجدار الناري وأجهزة وكشف، ومنع التطفل، والاختراق، وغيرها.

الأدوار والمسؤوليات

من أهم مسؤوليات ضابط أمن المعلومات

التدقيق والمراجعة بموافقة الجهة لتقييم مدى توافق النواحي الخاصة بأمن المعلومات على الشبكات ومتابعة الجوانب الأمنية الخاصة بالشبكة المعلوماتية في الجهة

متابعة التقارير الخاصة بالمشاكل الأمنية التي تواجهها الشبكة المعلوماتية في الجهة والمساعدة في حلها.

من أهم مسؤوليات المسئول عن الشبكة

التأكد من توافق مواصفات الأجهزة والأنظمة والتطبيقات الخاصة بالشبكة المعلوماتية في الجهة مع السياسات العامة لأمن المعلومات وبشكل يضمن إمكانية التوسع والتحديث

المحافظة على مستوى أداء ثابت للشبكة، وضبط الإعدادات الخاصة بالأجهزة المتواجدة على الشبكات لتعمل بطريقة آمنة

ضبط وإدارة ومتابعة تشغيل الأجهزة والأنظمة الخاصة بحماية الشبكة المعلوماتية للجهة

تشفير المعلومات المصنفة تصنيفاً عالي السرية عند نقلها داخل الشبكة المحلية على أن تكون آلية التشفير متوافقة مع سياسات أمن المعلومات

مراقبة أداء الشبكات والأنظمة وإدارتها أولاً بأول، ورفع تقارير للجهة بشكل دوري

عدم الإفصاح عن عناوين وإعدادات أي من أنظمة الشبكة الداخلية التابعة للجهة دون موافقة الجهة

مراعاة أمن المعلومات عند تصميم ومعمارية الشبكات بحيث توفر قدر مناسب من العزل والاستقلالية لضمان الحماية والسرية وبما يستلزمه احتياج العمل

حماية جميع الشبكات الداخلية المتصلة مع شبكة حكومية أو شبكة عامة أخرى بشكل صحيح.

الأدوار والمسؤوليات

من أهم مسؤوليات المستخدمين

يمنع الموظفون الموصلة
أجهزتهم بالشبكة
الداخلية من الاتصال
بأي شبكة خارجية بأي
شكل من الأشكال إلا
بموافقة الجهة
المختصة

عدم ربط أي جهاز نظم
معلومات غير مصرح به
إلى الشبكة الحكومية
دون الحصول على
موافقة الجهة المختصة

يمنع توصيل الموارد
الحاسوبية المملوكة
للموظفين بالشبكة الداخلية
من دون إذن مسبق من إدارة
/ قسم أمن الشبكات أو
الجهة المختصة، وتمنح الجهة
الحكومية موافقة استخدام
هذه الموارد الشخصية
بمعايير مطابقة لسياسات أم
المعلومات

تنفيذ وتطبيق جميع
التعليمات والإجراءات
التي تنص عليها سياسة
امن الشبكة، حفظ
المعلومات والملفات على
الأجهزة التي يتم
تحديدها من إدارة /
قسم أمن الشبكات أو
الجهة المختصة

انتہی،،،

