الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

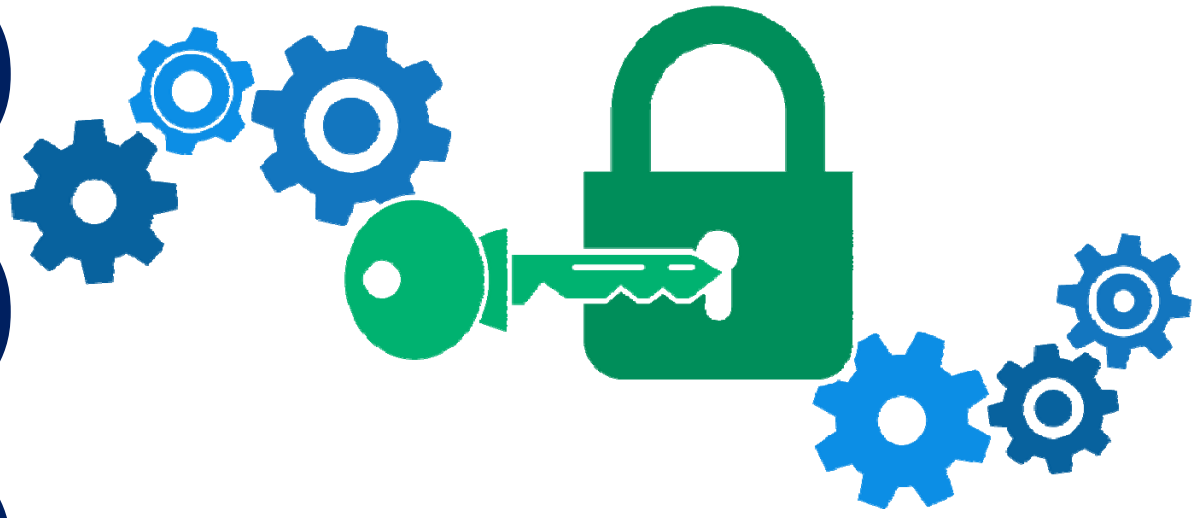
# السياسة الوطنية للتشفير

م. سلمان سليمان
رئيس مركز أمن المعلومات

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# المحتوى

- مقدمة
- نظرة عامة
- هدف السياسة ونطاق التطبيق
- متطلبات السياسة
- تصنيف المعلومات
- معايير التشفير
- الامتثال للسياسة
- أحكام عامة



الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# مقدمة

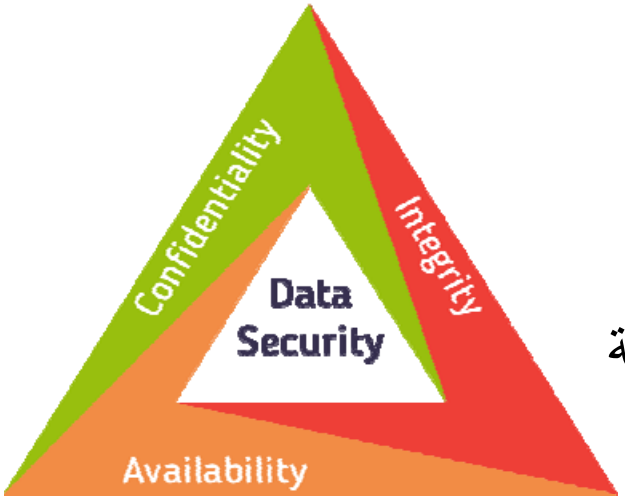
- تهدف هذه الورشة إلى التعريف بالسياسة الوطنية للتشفير لكافة الجهات العامة المعنية بتطبيقها، ممثلة بمسؤولي أمن المعلومات في هذه الجهات، لتمكين كل جهة عامة من تطوير وتطبيق سياسة التشفير الخاصة بها وفقاً لقواعد وضوابط السياسة الوطنية للتشفير
- **تصنيف الوثيقة: مقيدة**
- تم إصدار السياسة الوطنية للتشفير من قبل وزارة الاتصالات والتقانة بمشاركة الجهات المعنية بأمن المعلومات على المستوى الوطني وممثلين عن جهات علمية وبحثية
- اعتمدت السياسة الوطنية للتشفير في جلسة رئاسة مجلس الوزراء بتاريخ 18/12/2019

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# نظرة عامة

- تم إصدارها في سياق الجهود المبذولة لتنظيم أمن المعلومات على المستوى الوطني
- تعميم منهجية أمن المعلومات /خطة أمن المعلومات
- تتضمن القواعد الأساسية للتعامل مع البيانات الحكومية خلال عمليات النقل والحفظ
- تسهم في تحقيق أهداف أمن المعلومات على المستوى الوطني المتمثلة بـ:

1- السرية
2- السلامة
3- التوافرية
4- عدم الإنكار
5- التحقق من الهوية – تحديد السماحيات - المراقبة والمحاسبة



الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# هدف السياسة

- ✓ وضع المنهج العام لسياسة التشفير الوطنية بحيث تكون **المرجع الرئيسي** لجميع الجهات الحكومية في الجمهورية العربية السورية أثناء إعداد سياسة التشفير الخاصة بهم، وذلك بهدف حماية المعلومات وفقاً لدرجة تصنيفها، من خلال تحديد الضوابط المتعلقة باستخدام التشفير في إدارة وتبادل وحفظ المعلومات الإلكترونية الحكومية

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# نطاق التطبيق

- الجهات الحكومية التي يجب أن تلتزم بتطبيق هذه السياسة

- الجهات المستثناة من تطبيق هذه السياسة

- جميع الأصول المعلوماتية للجهات ومستخدميها عند تبادل المعلومات بين :

-حكومة – حكومة

-حكومة - مواطن

-حكومة - قطاع أعمال

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# متطلبات السياسة

- يجب أن تحقق سياسة التشفير في أي جهة عامة ثلاثة متطلبات أساسية:

1. الالتزام بالحد الأدنى على الأقل من خوارزميات التشفير وأطوال المفاتيح وفقاً لهذه السياسة

2. إعادة إنتاج نفس النص الصريح باستخدام البرنامج / الجهاز المستخدم لإنتاج النص المشفر من النص الصريح المحدد عند الطلب

3. تخزين معلومات النص الصريح من قبل الجهة بما تتناسب مع الضوابط والنواظم الخاصة بحفظ الوثائق الإلكترونية كحد أدنى، مع الأخذ بعين الاعتبار إمكانية إتاحتها للجهات الرقابية والقضائية عند الطلب، ووفقاً لأحكام القوانين في الجمهورية العربية السورية

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# تصنيف المعلومات

- تقع على عاتق الجهة مسؤولية تصنيف المعلومات من خلال إعداد سياسة واضحة لتصنيف المعلومات

- صنفت السياسة الوطنية للتشفير المعلومات وفقاً **لحساسيتها وأهميتها** إلى:

- **عادية**
- **مقيدة**
- **سرية**
- **سرية للغاية**

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# حفظ المعلومات وتبادلها وإتلافها

- حفظ المعلومات:

- يجب أن تتوافق إجراءات حفظ المعلومات مع مستوى تصنيفها

- يجب على الجهة وضع إجراءات خاصة لحفظ جميع **وسائط التخزين** التي تحوي معلومات بما يتوافق مع تصنيف المعلومات المخزنة فيها

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# حفظ المعلومات وتبادلها وإتلافها

- تبادل المعلومات ونقلها:

- يجب نقل أي معلومات مصنفة سرية أو سرية للغاية بشكل مشفر حصراً

- يجب إلحاق مستوى التصنيف باسم الملف الرقمي

- إتلاف المعلومات:

- يجب إتلاف المعلومات الإلكترونية بطريقة تتفق مع مستوى تصنيفها

| التصنيف | حفظ المعلومات | تبادل المعلومات | إتلاف المعلومات |
|---|---|---|---|
| العادية | غير مشفر | غير مشفر | حذف عادي |
| المقيدة | إجراءات تحكم | التشفير اختياري | تهيئة |
| السرية | مشفر | مشفر | تدمير/حرق |
| السرية للغاية | مشفر | مشفر وعلى شبكة معزولة | تدمير/حرق |

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# مسؤولية أمن وحماية المعلومات

- جميع المعلومات ضمن الجهة، هي ملك لها. وتقع المسؤولية كل من يتعامل بها
- تتحمل الإدارة العليا في الجهة المسؤولية النهائية عن أمن وحماية المعلومات الخاصة بها
- يجب أن تحدد سياسة التشفير القسم أو الأشخاص المعنيين ضمن الجهة عند تطبيق إجراءات حفظ المعلومات ونقلها واسترجاعها وإتلافها
- يجب أن تحدد السياسة الجهة أو القسم المسؤول عن تدقيق إجراءات حفظ المعلومات ونقلها واسترجاعها وإتلافها

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# البروتوكولات الآمنة

- يجب على الجهات اعتماد (أحدث إصدارات) البرتوكولات الآمنة المذكورة في السياسة على الأقل عند إعداد دفاتر الشروط الفنية المتعلقة بالبرمجيات و/أو تبادل المعلومات عبر الشبكات و/أو تصميم المواقع الإلكترونية و/أو تصميم وتنفيذ خدمة إلكترونية ما

على سبيل المثال:

- طبقة التطبيقات: استخدام البروتوكول HTTPS، SFTP
- طبقة النقل: استخدام SSL/TLS

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# التشفير

## التشفير المتناظر

- على الجهات استخدام إحدى هذه الخوارزميات للتشفير المتناظر على الأقل:

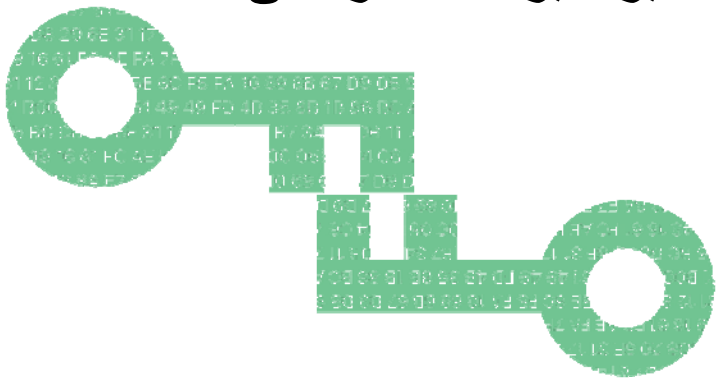
1. خوارزمية 3DES بطول مفتاح 168 بت
2. خوارزمية Gost بطول مفتاح 256 بت
3. خوارزمية AES بطول مفتاح 128 بت
4. أي خوارزمية أخرى، بعد اعتمادها من قبل الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# التشفير

**التشفير غير المتناظر**

• يجب على الجهات استخدام إحدى هذه الخوارزميات للتشفير غير المتناظر على الأقل:



- خوارزمية DH بطول مفتاح 2048 بت

- خوارزمية RSA بطول مفتاح 2048 بت

- نظام التشفير المبني على التوابع القطعية ECDSA بطول مفتاح 256 بت

- أي خوارزمية أخرى، بعد اعتمادها من قبل الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# تشفير المعلومات

- يمكن أن تتواجد المعلومات بعدة حالات:

- **المعلومات المخزنة:** يجب أن تكون المعلومات المخزنة –بغض النظر عن مكان التخزين- والمصنفة سرية أو سرية للغاية مشفرة، ويجب أن تكون إمكانية الوصول إليها مضبوطة وفق سماحيات محددة
- **المعلومات المتبادلة:** يجب أن تكون المعلومات المنقولة أو المتبادلة والمصنفة سرية أو سرية للغاية مشفرة و/أو ترسل عبر قنوات آمنة حسب البرتوكولات ذات الصلة

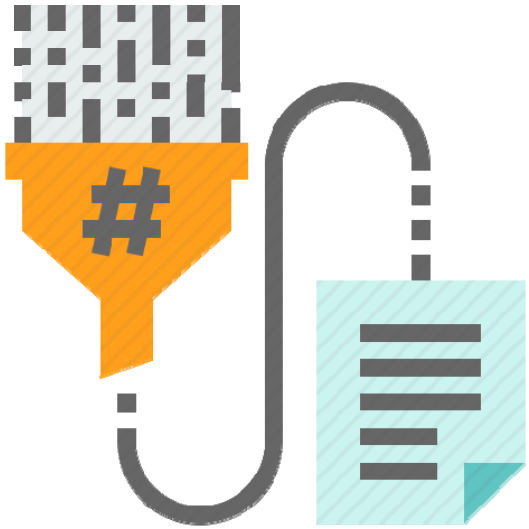
- **المعلومات المستخدمة:** لا يمكن تشفيرها يتمثل الحل الوحيد باستخدام الأماكن الآمنة فيزيائيا للتعامل معها

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# خوارزميات الاختزال

- يجب أن تتوقف الجهات عن استخدام تابع SHA-1 بشكل تدريجي
- على الجهات استخدام إحدى هذه الخوارزميات على الأقل:

1. SHA-2 -
2. SHA-3 -



الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# الامتثال للسياسة

يجب أن يمتثل لهذه السياسة والسياسات المرتبطة بها كل من يشملهم نطاق التطبيق:

- **الجهات العامة**، وذلك من خلال:

1. وضع سياسة تشفير متوافقة مع هذه السياسة
2. أن يتوفر قسم/موظف متخصص بالإشراف على تطبيق هذه السياسة
3. يمكن الاستعانة بمدقق خارجي معتمد من الهيئة

- **مستخدمي نظم المعلومات**

عدم الامتثال /انتهاك السياسة يتوجب العقوبات والمساءلة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# أحكام عامة

- لا يحقق التشفير بمفرده حماية أمنية كاملة مرتبطة بتخزين ومعالجة ونقل المعلومات الحساسة؛ استخدامها لا يغني عن الحاجة لتقييم المخاطر، وتوعية وتدريب الموظفين، وتحقيق تحكم بالنفاذ فيزيائي ومنطقي مناسبين لحماية الأصول المعلوماتية الحكومية
- تقوم الهيئة بمراجعة هذه السياسة سنوياً، وتعدلها إذا دعت الحاجة
- على الجهة تأهيل وتوعية وتدريب مستخدمي هذه السياسة بخصوص سياسة أمن المعلومات عموماً
- في حال كان تصنيف المعلومات سري أو سري للغاية، فعلى الجهة القيام بأعمال الصيانة المتعلقة بالمنظومات المعلوماتية في موقع العمل
- في حال كان تصنيف المعلومات سري أو سري للغاية، فعلى الجهة إجراء عملية النسخ الاحتياطي للمعلومات بصورة مشفرة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# الخلاصة

ماذا على الجهات العامة أن تفعل للامتثال للسياسة الوطنية للتشفير ؟

- تشكيل وتكليف فرق عمل /لجان خاصة تضم أعضاء فنيين مؤهلين وحقوقيين وماليين لتطوير السياسة الوطنية للتشفير
- تصنيف المعلومات الخاصة بالجهة وفق سياسة موثقة/السياسة الوطنية لأمن المعلومات-السياسة الوطنية للتشفير
- إعداد وثيقة سياسة التشفير في إطار خطة إدارة وتنظيم أمن المعلومات لدى الجهة وبما يتوافق مع السياسة الوطنية للتشفير
- التوعية والتدريب والتأهيل وتعريف جميع العاملين بمسؤولياتهم والعواقب الناجمة عن خرق السياسة
- متابعة تطبيق قواعد وأحكام السياسة ومراجعتها وتطويرها بشكل دوري وعند الضرورة
- التعاون والتنسيق مع الهيئة الوطنية لخدمات الشبكة وعدم التردد في طلب المساعدة والمشورة

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

# شكرا لإصغائكم