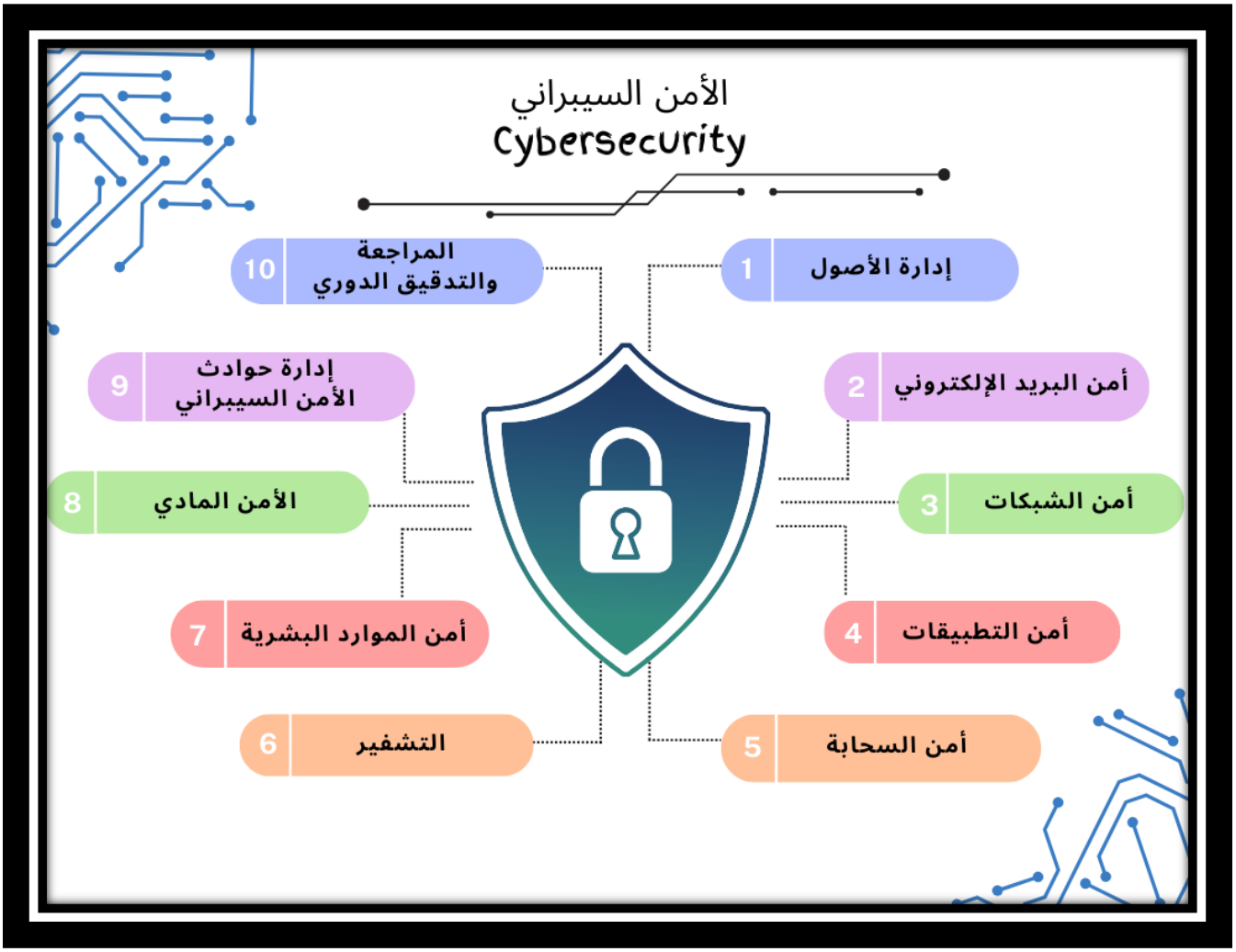
الأمن السيبراني Cybersecurity



إعداد م. سليمه كنينه

دائرة الاستجابة للطوارئ المعلوماتية

10/30/2023

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

الأمن السيبراني
Cybersecurity

يشـير مصـطلح الأمن السّـيبراني إلى الممارسـات التّقنيّة والتنظيمية والإدارية الهادفة لتوفير الحماية لجميع الأنظمة المتّصـلة بالانترنت، مثل الحواسـيب والمخدّمات والأجهزة المحمولة والشّـبكات، والتطبيقات والبيانات والمعلومات، والنظم السـحابية، بالإضـافة إلى حماية البريد الالكتروني ومواقع الويب ووسـائل التواصـل الاجتماعي من الهجمات السيبرانيّة.

يجب على الشـركات والأفراد تطبيق تلك الممارسـات على حدّ سـواء، بغرض منع الوصـول غير المصـرّح به للبيانات، وحمايتها من أيّ اختراق أو تعديل أو سرقة أو تخريب يمكن أن يطالها.

بعض أنواع التهديدات السيبرانية الشائعة
Some types of common cyber threats

- البرمجيات الخبيثة **Malware** (برمجيات الفدية/التجسس، أحصنة طروادة، الديدان، الفيروسات).
- التصيّد الاحتيالي **Phishing**.
- هجوم الرجل الوسيط **MitM** – **Man in the Middle attack**.
- الهجوم الموزَّع لتعطيل الخدمة **DDoS** – **Distributed Denial of Service**.
- التهديد المستمر المتقدّم **APTs – Advanced Persistent Threats**.
- نقاط الضعف **Vulnerabilities** .
- الاختراق **Hacking**.
- التهديد الداخلي **Insider Threats** (أشخاص حانقين على الشركة، أشخاص مهملين).

Tel: +963 11 3937049 **Fax:** +963 11 3937079 P. Box:60 Sabouraa **E-mail:** infoisc@nans.gov.sy
Website: www.nans.gov.sy

أنواع الأمن السيبراني
Types of cybersecurity

- ✓ الأمن السيبراني للبنية الأساسية.
- ✓ أمن التجهيزات والأنظمة الحاسوبية.
- ✓ أمن البريد الالكتروني.
- ✓ أمن الشبكات.
- ✓ أمن البيانات والمعلومات.
- ✓ أمن التطبيقات.
- ✓ أمن الحوسبة السحابية والاستضافة.
- ✓ الأمن المادي.
- ✓ أمن الموارد البشرية.
- ✓ أمن الأطراف الخارجية.

تعزيز الأمن السيبراني
Cybersecurity Defense

1) إدارة الأصول Asset Management:

يجب أن يكون لدى الجهة قائمة جرد دقيقة وحديثة للأصول المعلوماتية تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة وتوافرها ولذلك يجب اتخاذ الاجرءات التالية:

- تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للجهة.
- تحديد وتوثيق واعتماد وتطبيق سياسة الاستخدام المقبول للأصول المعلوماتية والتقنية للجهة.
- تصنيف الأصول المعلوماتية والتقنية للجهة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2) التعريف وإدارة الوصول Identity and Access Management:

من أجل منع الوصـول غير المصـرح به وتقييد الوصـول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة يجب اتخاذ الإجراءات التالية:

- التحقق من هوية المستخدم (User Authentication) بناء على إدارة تسجيل المستخدم، وإدارة كلمة المرور.
- التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول عن بعد.
- إدارة صـلاحيات المسـتخدمين (Authorization) بناء على مبادئ التحكم بالدخول والصـلاحيات (مبدأ الحاجة إلى المعرفـة والاسـتخـدام، ومبـدأ الحـد الأدنى من الصـلاحيـات والامتيـازات، ومبـدأ فصـل المهـام).

3)حماية الأنظمة System Protection:

لضمان حماية الأنظمة بما في ذلك أجهزة المستخدمين والبنى التحتية من المخاطر السيبرانية يجب اتخاذ الإجراءات التالية:

- الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة وإدارتها بشكل آمن.
- التقييد الحازم لاستخدام أجهزة وسائط التخزين الخارجية.
- إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة (Patch Management).
- مـزامنـة الـتـوقـيـت (Clock Synchronization) مـركـزيـاً ومـن مصـدر دقـيـق ومـوثـوق.

4)حماية البريد الإلكتروني Email Protection:

لضمان حماية البريد الالكتروني للجهة من المخاطر السيبرانية يجب إجراء مايلي:

- تحليل وتصـفية (Filtering) رسـائل البريد الإلكتروني وخصـوصـا رسـائل التصـيّد الاحتيالي (Phishing Emails) والرسـائل الاقتحامية (Spam Emails) باسـتخدام تقنيات وآليات الحماية الحديثة والمتقدّمة للبريد الالكتروني.
- التحقق من الهويـة متعـدد العنـاصـر (Multi-Factor Authentication) عن طريق إعـداد تكوين بروتوكولات الانترنت **DKIM** و **DMARC** و**SPF** .
- النسخ الاحتياطي والأرشفة للبريد الإلكتروني.

- الحماية من التهديدات المتقدمة المستمرة(**APT Protection**)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.
- توثيق مجال البريد الإلكتروني بالطرق التقنية، مثل طريقة إطار سياسة المرسل **Sender Policy Framework (SPF).**

5) إدارة أمن الشبكات Networks Security Management:

لضمان حماية شبكات الجهة من المخاطر السيبرانية يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة واتخاذ الإجراءات التالية:

- العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد الطبقات (Defense-in-Depth).
- عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار.
- أمن التصفح والاتصال بالانترنت، ويشمل ذلك التقييد الحازم للمواقع الالكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد.
- أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة.
- ضبط المنافذ المفتوحة وحركة البيانات من خلال استخدام الجدران النارية.
- ضبط وإدارة منافذ وبروتوكولات وخدمات الشبكة.
- أنظمة الحماية المتقدمة لاكتشاف ومنع التطفل (Intrusion Prevention Systems).
- أمن نظام أسماء النطاقات(DNS).
- حماية الشبكة من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.

6)أمن الأجهزة المحمولة Mobile Devices Security:

حماية الأجهزة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها

أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة مبدأ (**BYOD**) Bring Your Own Device (احضر الجهاز الخاص بك)عند ارتباطها بشبكة الجهة وبالتالي يجب:

- فصل وتشفير البيانات والمعلومات (الخاصة بالجهة) المخزّنة على الأجهزة المحمولة وأجهزة (BYOD).
- الاستخدام المحدد والمقيّد بناءً على ما تتطلبه مصلحة أعمال الجهة.
- حذف البيانات والمعلومات (الخاصـــة بالجهة) المخزّنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة.
- التوعية الأمنية للمستخدمين.

7) حماية البيانات والمعلومات Data and Information Protection:

لضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشـريعية والتنظيمية ذات العلاقة يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السـيبراني وأن تغطي بالحد الأدنى مايلي :

- ملكية البيانات والمعلومات.
- تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms).
- خصوصية البيانات والمعلومات.

8) التشفير Cryptography:

لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الالكترونية للجهة، وذلك وفقا للسـياسـات والإجراءات التنظيمية للجهة، والمتطلبات التشـريعية والتنظيمية ذات العلاقة يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني للتشفير في الجهة وأن تغطي بالحد الأدنى مايلي:

- معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً).
- الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.
- تشفير البيانات أثناء النقل والتخزين بناء على درجة تصنيفها.

9) إدارة النسخ الاحتياطية Backup and Recovery Management:

لضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من

الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للجهة وأن تغطي بالحد الأدنى مايلي:

- نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
- القدرة على الاستعادة السريعة للبيانات والخدمات والنظم بعد التعرض لحوادث الأمن السيبراني.
- إجراء احتبار دوري لمدى فعالية استعادة النسخ الاحتياطية.

10) حماية تطبيقات الويب Web Application Security:

لضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية يجب اتخاذ الإجراءات التالية بالحد الأدنى:

- استخدام جدار الحماية لتطبيقات الويب (Web Application Firewall).
- استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture).
- استخدام بروتوكلات آمنة (مثل بروتوكول HTTPS).
- توضيح سياسة الاستخدام الآمن للمستخدمين.
- التحقق من الهوية متعدد العوامل (Multi-Factor Authentication) لعمليات دخول المستخدمين.

11) اختبار الاختراق Penetration Testing:

لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة يجب إجراء محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية واكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني من خلال:

- نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدّمة خارجياً (عن طريق الانترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الالكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الالكتروني والدخول عن بعد.
- إجراء اختبار الاختراق دورياً.

12) إدارة نقاط الضعف Vulnerabilities Management:

لضمان اكتشاف الثغرات الأمنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة يجب اتخاذ الإجراءات التالية:

- فحص واكتشاف الثغرات دورياً.
- تصنيف الثغرات حسب خطورتها.
- معالجة الثغرات بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها.
- إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.
- متابعة مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.

13) الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية
Cybersecurity in Information Technology Projects

يجب تضمين متطلبات الأمـــــن السيبراني في منهجية وإجـــــراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.

يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة ولمشاريع تطوير التطبيقات والبرمجيات الخاصة بها بحد أدنى ما يلي:

- تقييم الثغرات ومعالجتها.
- استخدام معايير التطوير الآمن للتطبيقات (Secure Coding Standards).
- استخدام مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات والمكتبات الخاصة بها (Libraries).
- إجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة.
- أمن التكامل (Integration) بين التطبيقات.
- إجراء مراجعة للإعدادات والتحصين (Secure Configuration and Hardening) وحزم التحديثات قبل إطلاق التطبيقات.

14) الأمن المادي Physical Security:

لضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب يجب اتخاذ الإجراءات التالية:

- الدخول المصرح به للأماكن الحساسة في الجهة (مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها).
- توفر سجلات الدخول والمراقبة.
- حماية معلومات سجلات الدخول والمراقبة.
- أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة (وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين).
- أمن الأجهزة والمعدّات داخل مباني الجهة وخارجها.

15) الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة
Cloud Computing and Hosting Cybersecurity

يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة للجهة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة بالحد الأدنى مايلي:

- تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والإستضافة، وإعادتها للجهة (بصيغة قابلة الاستخدام) عند إنتهاء الخدمة.
- فصل البيئة الخاصة بالجهة (وخصوصاً الخوادم الإفتراضية) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
- موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل الدولة.

16) الأمن السيبراني المتعلّق بالموارد البشرية Cybersecurity in Human Resources

لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة، يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة أن تكون بالحد الأدنى مايلي:

- تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات Non-Disclosure Clauses) في عقود العاملين في الجهة (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة).

- إجراء المسح الأمني (Screening or Vetting) (على سبيل المثال لا الحصر: فحص السجل الجنائي، والتحقق من المؤهلات) للعاملين في وظائف الأمن السيبراني والوظائف التقنية ذات الصلاحيات الهامة والحساسة.
- التوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها).
- يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.

17) برنامج التوعية والتدريب بالأمن السيبراني
Cybersecurity Awareness and Training Program

يجب تزويد العاملين ببرنامج للتدريب والتوعية بالأمن السيبراني (عند بداية المهنة الوظيفية وخلالها) ويجب أن يغطي كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية بما في ذلك:

- التعامل الآمن مع خدمات البريد الالكتروني خصوصاً مع رسائل التصيد الاحتيالي.
- التعامل الآمن مع خدمات تصفح الانترنت.
- التعامل الآمن مع وسائل التواصل الاجتماعي.
- التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين.
- الوقاية من هجمات الهندسة الاجتماعية.

18) الأمن السيبراني المتعلّق بالأطراف الخارجية Third-Party Cybersecurity

يجب تحديد وتوثيق واعتماد وتطبيق متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية من مخاطر الأمن المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بالجهة:

بنود عامة:

- يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة الجهة مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.
- يجب تحديد واختيار الأطراف الخارجية المقدّمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

- يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل الجهة ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.
- يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية (مثل اتفاقية مستوى الخدمة **Service-Level Agreement SLA**) بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

فيما يتعلق بموظفي الأطراف الخارجية:

- يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود موظفي الأطراف الخارجية (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع الجهة) و الحذف الآمن من قِبَل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.

فيما يتعلق بخدمات الإسناد لتقنية المعلومات "Outsourcing" أو الخدمات المدارة "Managed Services" المقدمة من قبل الأطرف الخارجية:

- إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود مايضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.
- يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل الدولة.
- يجب أن تكون خدمات الإسناد على الأنظمة الحساسة عن طريق شركات وجهات معتمدة وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

فيما يتعلق بالتوثيق وضوابط الوصول:

- يجب أن تُطوّر الأطراف الخارجية وتتبع عملية رسمية وموثّقة بعناية لمنح وإلغاء حق الوصول إلى جميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات الجهة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بالجهة.
- يجب توفير إمكانية الوصول إلى معلومات الجهة ومعالجتها بطريقة آمنة ومراقبة.

- يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات الجهة بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بالجهة.
- يجب تطبيق نظام التحقّق من الهوية متعدّد العوامل على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بالجهة أو تنقلها أو تُخزّنها.
- يجب إلغاء حقوق الوصول فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة بالجهة أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.
- يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في الجهة.
- يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب الجهة.

فيما يتعلق بإدارة التغيير:

- يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات الجهة وبما يتوافق مع متطلّبات الأمن السيبراني.
- يجب مراجعة واختبار التغييرات التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالجهة قبل تطبيقها على بيئة الإنتاج (Production Environment).
- يجب إبلاغ الأطراف المعنية في الجهة بالتغييرات الرئيسية المخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بالجهة.

فيما يتعلق بإدارة حوادث الأمن السيبراني واستمرارية الأعمال:

- يجب أن تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ الجهة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.
- يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و الجهة في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

- يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة للجهة وفقاً لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة بالجهة.

فيما يتعلق بمتطلبات حماية البيانات والمعلومات:

- يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات الجهة وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في الجهة.
- يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات الجهة وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في الجهة.
- يجب عمل نُسخ احتياطية من بيانات ومعلومات الجهة بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بالجهة.
- يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات الجهة الموجودة في الأنظمة الحسّاسة والبيانات الشخصية (Data privacy)، والتي تُعالجها الأطراف الخارجية – في بيئة الاختبار إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling) أو تقنيات إخفاء البيانات (Data Anonymization).
- يجب عدم نقل بيانات ومعلومات الجهة الموجودة في الأنظمة الحسّاسة – والتي تُعالجها الأطراف الخارجية – خارج بيئة الإنتاج.
- يجب تصنيف بيانات ومعلومات الجهة الموجودة في الأنظمة الحسّاسة – والتي تُعالجها الأطراف الخارجية – وفقاً لسياسة تصنيف البيانات والمعلومات المعتمدة في الجهة.

19) إدارة سجلات الأحداث ومراقبة الأمن السيبراني
Cybersecurity Event Logs and Monitoring Management

لضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة وبالتالي يجب :

- تفعيل سجلات الأحداث (**Event logs**) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة.

- تفعيل سجلات الأحـــــداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة.
- تحديد التقنيات والحلول اللازمة Security Information and Event Management (**SIEM**) لجمع سجلات الأحداث الخاصة بالأمن السيبراني.
- المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني.
- ألّا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني عن 12 شهر.

20) إدارة حوادث وتهديدات الأمن السيبراني
Cybersecurity Incident and Threat Management

لضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة وبالتالي يجب اتخاذ الإجراءات التالية:

- تصنيف حوادث الأمن السيبراني.
- وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة.
- وضع خطط التعافي من الكوارث (Disaster Recovery Plan)
- تبليغ الهيئة الوطنية لخدمات تقانة المعلومات/مركز أمن المعلومات عند حدوث حادثة أمن سيبراني.
- مشاركة التنبيهات والمعلومات ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة الوطنية لخدمات تقانة المعلومات.

21) المراجعة والتدقيق الدوري للأمن السيبراني
Cybersecurity Periodical Assessment and Audit

- مراجعة وتدقيق ضوابط الأمن السيبراني لدى الجهة والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجهة.
- يجب التأكد من تطبيق ضوابط الأمن السيبراني دورياً، ومرّة واحدة سنوياً على الأقل للأنظمة الحسّاسة للتأكد من مواءمتها مع الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة الحساسة.
- يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها.
- يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية.

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

دمتم بأمان

مع تحيات مركز أمن المعلومات

2023

Tel: +963 11 3937049 **Fax:** +963 11 3937079 P. Box:60 Sabouraa **E-mail:** infoisc@nans.gov.sy
Website: www.nans.gov.sy