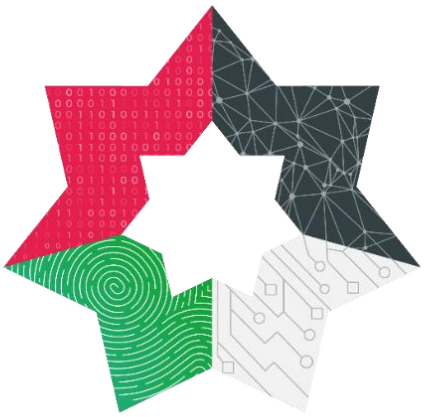

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

سياسة اعتماد منتجات الأمن السيبراني للوزارات والدوائر الحكومية

Government's Cybersecurity Products Acquisition Policy (2023)

الصادرة عن المجلس الوطني للأمن السيبراني بموجب قراره المتخذ في جلسته رقم (2)

المنعقدة بتاريخ 2023/11/27

جدول المحتويات

Contents-1

رقم الإصدار	تاريخ الإصدار	ملخص عن التعديلات	أرقام الصفحات المشمولة بالتعديل
1	2023/11/27	لا يوجد تعديلات	-
			-
			-
			-
			-

1. المقدمة

في إطار سعي المركز الوطني للأمن السيبراني إلى بناء منظومة فعالة للأمن السيبراني في المملكة وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات، و إدراكاً من المركز بأن من أهم التهديدات التي تواجهها الشبكات المعلوماتية في جميع أنحاء العالم هي تلك المتأتية من سلاسل التوريد وما تعتريه من مخاطر ناتجة عن عدم وجود آليات للتحقق من موثوقية المنتجات والحلول وضمان عدم استخدام منتجات غير موثوق بها، فقد جاءت هذه السياسة لتطبيق آليات اعتماد وتوظيف منتجات الأمن السيبراني في الجهات والوحدات الحكومية، ولتؤسس هذه السياسة في المرحلة اللاحقة لنظام وطني لاعتماد وترخيص جميع المنتجات والحلول الرقمية لضمان سلامة سلاسل التوريد واستخدام المنتجات الآتية من مصادر موثوق بها فقط.

2. السند القانوني للسياسة وبدأ العمل

1. يأتي إقرار هذه السياسة استناداً للفقرة (أ) من المادة (4) من قانون الأمن السيبراني رقم 16 لسنة 2019 والتي تنص على: يتولى المجلس المهام والصلاحيات التالية:

(أ. اقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني).

2. يعمل بهذه السياسة اعتبارا من تاريخ إقرارها من المجلس الوطني للأمن السيبراني، وتلتزم جميع الجهات المعنية بتطبيقها وذلك استناداً لأحكام المادة (8/ب/1) من قانون الأمن السيبراني التي تنص على (ب. تلتزم الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة والخاصة والاهلية بما يلي: 1. اتباع السياسات والمعايير والضوابط الصادرة عن المركز لكل قطاع وفقا لأحكام هذا القانون والانظمة والتعليمات الصادرة بمقتضاه).

3. التعريفات

أ. يكون للكلمات والعبارات والتالية حيثما وردت في هذه السياسة المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:

القانون: قانون الأمن السيبراني رقم 16 لسنة 2019.

المنتج: كافة الأجهزة والبرمجيات والحلول التقنية والخدمات التي تستخدم لحماية المعلومات أو لمنع أو كشف أو تحليل أي تهديدات سيبرانية أو في الاستجابة للحوادث التي تؤثر على المعلومات والأنظمة والشبكات

المعلوماتية والبنى التحتية، ويشمل كذلك أنظمة التشفير وأية أنظمة معلومات تشتمل على مكونات تتعلق بأمن المعلومات و/أو الأمن السيبراني.

ب. تعتمد التعريفات الواردة في القانون ونظام المشتريات الحكومية النافذين.

4. الغاية والأهداف

جاء إعداد هذه السياسة بهدف:

أ. اعتماد مرجعية موحدة للجهات والوحدات الحكومية فيما يتعلق باعتماد وترخيص منتجات الأمن السيبراني لتفادي الضرر الناتج من تهديدات الأمن السيبراني.

ب. ضمان جودة منتجات الأمن السيبراني والتأكد من ملاءمتها للاحتياجات الأمنية واستبعاد المنتجات التي لا تتوافق مع المعايير الوطنية والدولية.

ج. تفادي المخاطر السيبرانية المتأتية من سلاسل التوريد والمنتجين والموردين الغير موثوق بهم.

د. التمهيد لإعداد وإصدار إطار تنظيمي لترخيص واعتماد منتجات الأمن السيبراني بالاعتماد على الضوابط المعيارية العالمية (Common Criteria Scheme).

ه. ضمان وجود هيكلية أمن سيبراني موحدة (Unified Architecture) لجميع الجهات والوحدات لتسهيل مهمة حماية وتأمين المعلومات والشبكات والأنظمة وإدامتها.

و. ضبط النفقات من خلال شراء منتجات الأمن السيبراني المعتمدة وبشكل موحد لكافة الجهات والوحدات الحكومية في الحالات الخاصة التي تتطلب ذلك ويحددها المركز الوطني للأمن السيبراني.

5. نطاق التطبيق

يتم تطبيق هذه السياسة على كافة الجهات والوحدات الحكومية وشركات البنى التحتية الحرجة.

6. الالتزامات لتطبيق السياسة

تلتزم الجهات المعنية والتي تنطبق عليها هذه السياسة بما يلي:

أ. الامتثال لهذه السياسة ولقانون الأمن السيبراني والأنظمة والتعليمات والضوابط والمعايير الصادرة عن المركز وعدم استخدام أي من منتجات الأمن السيبراني سواء كانت عن طريق الشراء أو المنح والمساعدات إلا من خلال اتباع الإجراءات الموضحة في هذه السياسة.

ب. تزويد المركز بجميع المعلومات الضرورية التي تطلب منها لتطبيق هذه السياسة.

7. الحوكمة

يضمن نظام الحوكمة تنفيذ متطلبات هذه السياسة بشكل سلس ومرن، ويتكون من مجموعة الأدوار والمسؤوليات على النحو التالي:

أ. المركز الوطني للأمن السيبراني

(1) تقييم المخاطر الأمنية المرتبطة بمنتجات الأمن السيبراني كافة.

(2) وضع قوائم سوداء للمنتجات ذات المخاطر العالية بحيث يمنع استخدام أو توظيف هذه المنتجات بأي شكل من الأشكال.

(3) الطلب من جميع الشركات المنتجة ووكلائها في الأردن والموردين تزويد المركز بشهادات من مختبرات معتمدة وحاصلة على الاعتمادية من إحدى المؤسسات الدولية تثبت تحقيق منتجاتهم لاي من المعايير الدولية التالية:

(أ) Common Criteria for Information technology Security Evaluation (ISO/IEC 15408) .

(ب) Federal Information Processing Standard (FIPS 140-2) .

وهي معايير للمنتجات المعنية بالتشفير فقط.

(ج) أي معايير دولية أخرى يوافق عليها المركز.

(4) تطوير معايير وطنية لاعتماد وترخيص منتجات الأمن السيبراني بالاعتماد على المعايير الدولية (Common Criteria for Information technology Security Evaluation) والعمل على المدى المتوسط والبعيد على تأسيس أو اعتماد مختبر لفحص منتجات الأمن السيبراني.

(5) إنشاء منصة وإدارتها وتطويرها لغايات استقبال الطلبات من الجهات طالبة منتج الأمن السيبراني والرد على هذه الطلبات.

(6) رفع تقرير لمجلس الوزراء بمدى التزام الجهات والوحدات الحكومية بتنفيذ أحكام هذه السياسة.

ب. وزارة الاقتصاد الرقمي والريادة

(1) قيام لجنة تنظيم شراء البُنى التحتية التكنولوجية وأجهزة الحاسوب وتوابعها والبرمجيات المشكلة في الوزارة التأكد من أن منتجات الأمن السيبراني المطلوبة معتمدة وتم الموافقة عليها من المركز.

(2) استضافة المنصة المعنية بتقديم الطلبات على السحابة الحكومية التي تديرها الوزارة.

ج. ديوان المحاسبة

يتولى ديوان المحاسبة وبالاشتراك مع المركز في التدقيق على مدى التزام كافة الجهات المعنية بتطبيق هذه السياسة والتأكد من الالتزام بإجراءات وآليات تنفيذها.

د. الجهة طالبة منتج الأمن السيبراني

(1) التأكد من مدى الحاجة الأمنية والفنية للمنتج داخل الجهة.

(2) تحديد المتطلبات الفنية ومواصفات المنتج.

(3) تقديم طلب للمركز من خلال المنصة المعتمدة لديه لهذه الغاية.

(4) عدم استخدام أي منتج سيبراني غير معتمد من قبل المركز الوطني للأمن السيبراني سواء كان ذلك عن طريق الشراء أو قبول الهبات أو المساعدات على شكل منتج سيبراني.

هـ . الجهات الموردة/المصنعة

(1) الالتزام بالسياسات والتعليمات الصادرة عن المركز عند التعاقد لتوريد أي من منتجات الأمن السيبراني للجهات والوحدات الحكومية.

(2) تقديم/إرفاق الشهادات والوثائق وفق البند (3) الفقرة (أ) أعلاه.

8. آلية التنفيذ

يُتبع التسلسل التالي عند طلب أي من منتجات الأمن السيبراني:

أ. تقوم الجهة المعنية بتحديد الحاجة إلى أي من منتجات الأمن السيبراني بناءً على تقييم أمني ذاتي يقوم به مختصو الأمن السيبراني وتكنولوجيا المعلومات فيها كتحقيق الامتثال لضوابط الإطار الوطني للأمن السيبراني، أو لسد ثغرة أمنية أو فجوة أو لحاجة أمنية طارئة.

ب. تقوم الجهة المعنية بإعداد المتطلبات الفنية والمواصفات الخاصة بالمنتج.

ج. تقوم الجهة المعنية بتقديم الطلب للمركز من خلال المنصة المعتمدة لهذا الغرض وتعبئة المعلومات المطلوبة وإرفاق المتطلبات الفنية وأية وثائق داعمة يطلبها المركز.

د. يتولى المركز ومن خلال الوحدة التنظيمية المختصة باستلام الطلب وتدقيقه وتقييم مدى حاجة الجهة الطالبة وفيما إذا كان المنتج المطلوب معتمد لدى المركز وإصدار قرار بالقبول أو الرفض وذلك خلال (14) يوم عمل من تاريخ استلام الطلب ويجوز تمديدها في حالات خاصة ومبررة.

ه. تمنح صلاحية للجنة تنظيم شراء البُنى التحتية التكنولوجية وأجهزة الحاسوب وتوابعها والبرمجيات المشكلة في وزارة الاقتصاد الرقمي والريادة للدخول على المنصة المعتمدة لتقديم طلبات اعتماد منتجات الأمن السيبراني للتأكد من حالة الطلب على المنصة بالرفض أو القبول واتخاذ الأجراء المناسب بناءً عليه.

و. تقوم الجهة المتقدمة بالطلب بعد إتمام عملية الشراء بإعلام المركز بالمنتج الذي تم شراءه حتى يتسنى له أدامة سجلاته وتقدير مدى الحاجة الى ربط المنتج الجديد بمركز المراقبة الحكومي.

ز. في الحالات التي تستدعي استخدام منتج موحد في كافة الجهات الحكومية، يقوم المركز بالتنسيق مع وزارة الاقتصاد الرقمي والريادة وتجميع الطلبات من كافة الجهات والوحدات وإحالتها الى لجنة الشراء الخاصة المشكلة في المركز للسير في إجراءات الشراء عن طريقها ومن المخصصات المالية لكل جهة او وحدة وفق نظام المشتريات الحكومية.