المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

الاستراتيجية الوطنية للأمن السيبراني

NATIONAL CYBERSECURITY STRATEGY

2028 - 2024

هذه الاستراتيجية هي مسودة أولية مقترحة مفتوحة للنقاش مع أصحاب المصلحة، تم اعدادها من قبل المركز الوطني للأمن السيبراني بموجب المهام والمسؤوليات الموكلة له في قانون الامن السيبراني رقم 16 لعام 2019.

Contents

المقدمة

أن التهديدات السيبرانية في تزايد مستمر ويتعين علينا ان نعمل ونتحرك بشكل سريع وفعّال لمواجهتها والحد من تأثيرها على المجتمع الأردني الذي يواجه المزيد والمزيد من الهجمات السيبرانية، سواء من جماعات الجريمة السيبرانية المنظمة (Organized Cybercrime) او من جماعات التهديد المتطورة (Advance Persistent Threat)، الذين يرغبون في الوصول إلى بياناتنا وشبكاتنا لأغراض أحياناً مادية وأحياناً أخرى لأغراض التجسس والاضرار بخدماتنا الاساسية. وقد أظهرت الأرقام الصادرة عن المركز الوطني للأمن السيبراني زيادة في الهجمات السيبرانية في عام 2023 بنسبة 80% عن عام 2022.

لقد أصبحت الجرائم السيبرانية عملاً مربحًا لأولئك الذين يريدون سرقة بياناتنا أو إتلاف أنظمتنا وابتزازنا مقابل المال، وما كان حكراً على الدول أصبح الآن متاحاً للبيع أو الإيجار لكل من يريد الإضرار بنا، حيث تواصل جماعات التهديد الأجنبية استخدام الأدوات السيبرانية للتجسس علينا والاضرار باقتصادنا، ناهيك عن أنهم لا يستهدفون أجهزتنا وأفرادنا فحسب، بل يستهدفون أيضًا بنيتنا التحتية الحرجة وأنظمتنا الحكومية.

أدى التحول الرقمي في الأردن على مر السنين إلى دمج التقنيات والاستراتيجيات والابتكارات الرقمية في مختلف قطاعات اقتصاد الدولة والمجتمع، ومنذ تنفيذ "الاستراتيجية الوطنية للتحول الرقمي"[1]، يعمل الأردن بنشاط على الاستفادة من التكنولوجيا لتعزيز النمو الاقتصادي وتحسين الخدمات العامة ورفع نوعية الحياة الشاملة لمواطنيه. لقد أدت الجهود التي بذلتها الدولة لتبني التكنولوجيا إلى تشكيل مجتمع أكثر ترابطًا وتقدمًا من الناحية التكنولوجية بشكل تدريجي، ولا تزال الفرص غير محدودة.

خلال السنوات القليلة الماضية طرأ تحول كبير على مجتمعنا الأردني الذي أصبح يعتمد بشكل أكبر على الخدمات الرقمية ويستخدم الانترنت بشكل أوسع ويعتمد بتزايد على قنوات الدفع الرقمية، حيث ان نسبة نفاذية الانترنت في الأردن هي من أعلى النسب في المنطقة، حيث يتمتع 88% من الأردنيين بحرية الوصول الى الانترنت[2]، وبشكل او بآخر يعمل التحول الرقمي على تغيير مجتمعنا واقتصادنا بشكل أسرع من أي وقت مضى، حيث يتم ربط المزيد والمزيد من الأشخاص والمؤسسات والأجهزة والبيانات بالإنترنت، وهنالك ربط أكبر للأجهزة المحمولة و إنترنت الأشياء والسحابة، وهذا يعني أيضًا احتمالية التعرض أكثر لمزيد من الهجمات السيبرانية الخطيرة والمدمرة، حيث يمكن للقراصنة كشف البيانات الحساسة، مثل البيانات الشخصية وبيانات المؤسسات وقطاعات البنية التحتية الحرجة، ولهذا السبب نحتاج إلى الحفاظ على أمان هذه البيانات من خلال جعل البيئة الرقمية الاردنية آمنة، والفشل في الدفاع عن بلادنا من الهجمات السيبرانية سيكون له آثار مدمرة على مجتمعنا واقتصادنا الرقمي.

لقد نجحت الاستراتيجية السابقة (2018 – 2023) في تأسيس وحوكمة الامن السيبراني على المستوى الوطني وبناء النظام الايكولوجي السيبراني الوطني، حيث تم خلال هذه الفترة اعداد وإقرار "قانون الأمن السيبراني رقم 16 لعام 2019" وإنشاء المجلس الوطني للأمن السيبراني الذي أُنيطت به مهمة إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني، وكذلك تم إنشاء المركز الوطني للأمن السيبراني ليكون الأداة الرقابية والتنظيمية لقطاع الامن السيبراني على المستوى الوطني.

ونسعى من خلال هذه الاستراتيجية الجديدة إلى تأمين المشهد السيبراني الأردني على جميع المستويات ولجميع أصحاب المصلحة، والى خلق بيئة رقمية آمنة تشجع على الابداع والريادة، جاذبة للشركات العالمية ولرأس المال الأجنبي وداعمة لرؤية التحديث الاقتصادي، كما ونسعى من خلال هذه الاستراتيجية الى جعل الأردن مركزاً إقليمياً متميزاً في مجال الامن السيبراني.

تقع مسؤولية مراقبة وتنسيق والإشراف على تنفيذ استراتيجية الأمن السيبراني الوطنية على عاتق المركز الوطني للأمن السيبراني (NCSC)، وستتم مراجعتها وتعديلها بشكل دوري عند الضرورة.

الجمهور المستهدف

الأمن السيبراني ليس مسؤولية الحكومة فقط، انما جهد جماعي تعاوني يمكن لجميع أصحاب المصلحة المعنيين المساهمة فيه، وتأتي التحسينات وتتحقق النتائج المرجوة من خلال جهود الجميع. لذلك فإن هذه الاستراتيجية تركز على أربع فئات، هي:

- **المواطنون**

[1] الاستراتيجية الوطنية للتحول الرقمي والخطة التنفيذية 2021 – 2025، وزارة الاقتصاد الرقمي والريادة، https://modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/dts-2021-ar.pdf

[2] Digital 2023: Jordan, DataReportal and Ocla Report, https://datareportal.com/reports/digital-2023-jordan

المواطنون مسؤولون بالدرجة الأولى عن حماية معلوماتهم، ويشمل ذلك الهواتف الذكية وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية، وأيضاً التطبيقات الموجودة عليها (مثل التطبيقات المصرفية) وبالتالي البيانات التي تحتوي عليها. إن حماية أجهزتهم وتطبيقاتهم الخاصة واستخدامها بشكل مناسب يجعل من الصعب على الجهات التهديدية شن هجمات إلكترونية.

من خلال المنصات الحكومية، مثل منصة (Safeonline.jo) تقدم الحكومة الدعم والإرشاد للمواطنين حتى يكونوا أكثر مناعة ضد الهجمات وأعمال التحايل ويشعروا أنهم جزء من منظومة الحماية الوطنية.

- **قطاع الأعمال**

تلعب الشركات دورًا كبيرًا في حماية بنيتها التحتية وبيانات موظفيها، وتحتل الشركات الصغيرة والمتوسطة مكاناً مهماً في الاقتصاد الأردني، وتعمل الحكومة الأردنية على دعم أصحاب المشاريع الصغيرة والشركات الصغيرة،

تعاني معظم الشركات الاردنية من عدم القدرة على الاستثمار في الأمن السيبراني بسبب التكاليف المرتفعة وعدم إمكانية توظيف أشخاص لهذه الغاية فقط، لذلك فان الحوادث التي تتعرض لها هذه الشركات تكون كارثية أحياناً بسبب عدم وجود ضوابط من أي نوع.

حرصت الحكومة من خلال هذه الاستراتيجية على دعم الشركات الصغرى والمتوسطة من خلال النصح والإرشاد وتوفير الأدوات والوسائل التي تمكنها من حماية نفسها ولو بشكل غير كامل.

- **البنية التحتية الحرجة**

البنية التحتية الحرجة مستهدفة بشكل كبير، لهذا تركز هذه الاستراتيجية على ضمان صمود بُنانا التحتية الحرجة والخدمات الأساسية، من خلال إدارة فعّالة للمخاطر وتطبيق شامل للضوابط والمعايير الوطنية واتخاذ الإجراءات الاحترازية ووضع خطط التعافي من الحوادث وضمان استمرارية العمل.

حرصت الحكومة من خلال الهدف الاستراتيجي الثاني على تقديم الدعم والمساندة لمشغلي البُنى التحتية الحرجة وبناء علاقات تشاركية داخل كل قطاع وما بين القطاعات المختلفة، من ناحية تبادل المعلومات والتشارك في القدرات.

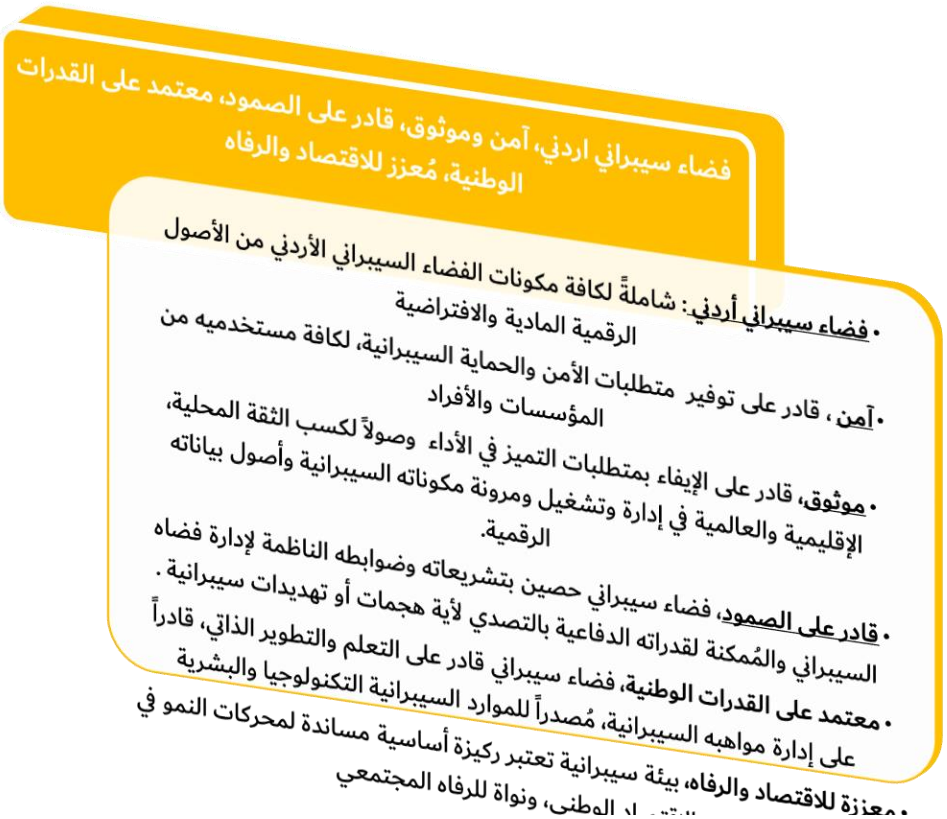
- **المؤسسات الحكومية**

تُعتبر المؤسسات الحكومية من البنُى التحتية الحرجة، وهي هدف دائم لجماعات التهديد المرتبطة بالدول بهدف سرقة المعلومات والتجسس، لذلك فقد أولت هذه الاستراتيجية عناية خاصة بضمان أمن الشبكات الحكومية ومناعتها، وقد حرصت الحكومة على الاستثمار في حماية المؤسسات الحكومية وفي تطوير الموارد البشرية وتحسين اداءها وتحسين الإجراءات

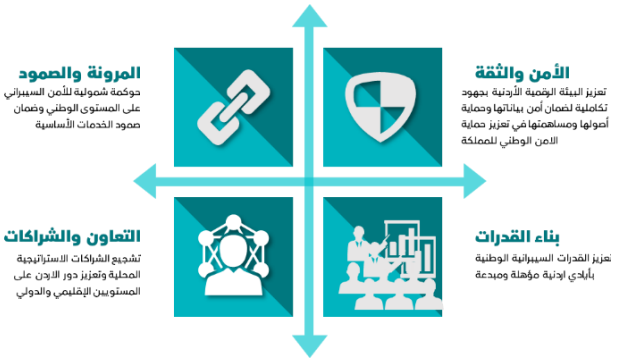
وتعزيزه.

رؤية الأردن السيبرانية 2024-2028

سوف نعمل بجهود تعاونية و تكاملية ما بين القطاعات الوطنية الحكومية والخاصة، لضمان استدامة أمن واستقرار الفضاء السيبراني الأردني، وبما يضمن تحقيق السيادة الرقمية على الأصول التكنولوجيا المادية والافتراضية للمملكة الأردنية الهاشمية، وحماية كافة مستخدميها من الأفراد والمؤسسات، وجعل المملكة درعاً منيعاً أمام التهديدات والهجمات السيبرانية من خلال تعزيز المرونة السيبرانية على المستوى الوطني، والتي تُعد اللبِنَة الأولى التي تجعل من فضاءنا الرقمي حصناً منيعاً قادر على الدفاع والصمود أمام النشاطات السيبرانية الهادفة للعبث بأمنه الرقمي واستقرار بيئته السيبرانية، وصولاً إلى :



أولويات الخطة الاستراتيجية الوطنية للأمن السيبراني 2024-2028



➢ الأولوية الأولى: الامن والثقة:

سنسعى من خلال هذه الاولوية لبناء الثقة بالفضاء السيبراني الأردني لكافة مستخدميه من الأفراد والمؤسسات المحلية والإقليمية والدولية، من خلال ايجاد بنية تحتية رقمية آمنة وموثوق بها تعزز كافة الجهود الوطنية الرامية لإدارة عمليات التحول الرقمي ورقمنه الخدمات، وترمي كذلك لحماية الأصول الرقمية المُشغلة والداعمة لهذه الخدمات، من خلال اتباع منهجية ترتكز على الإدارة الاستباقية للمعلومات السيبرانية الاستخباراتية، وتكوين فهم اكثر شمولية لأثرها وتهديداتها على الفضاء السيبراني الأردني، وبما يضمن أمن هذا الفضاء واستقراره.

➢ الأولوية الثانية: المرونة والصمود

سنعمل من خلال هذه الاولوية وبالتعاون والتنسيق ما بين كافة القطاعات الوطنية الحكومية والخاصة، على تمكين قدرة الفضاء السيبراني على التكييف مع أية تهديدات أو هجمات سيبرانية قد تتعرض لها الأصول الرقمية والتقنية المشغلة للقطاعات الوطنية الحرجة والأساسية في المملكة، وتطوير قدراته في مواجهة التهديدات السيبرانية، وتمكينه من إدارة المخاطر السيبرانية التي قد يتعرض لها من خلال الإدارة الاستباقية في التعامل مع التهديدات السيبرانية المتوقعة، المستحدثة والمتطورة، وبما يضمن استمرارية تشغيل العمليات الرقمية للقطاعات الوطنية بشكل آمن وفعال، وضمان قدرتها على استعادة النشاطات والعمليات المؤسسية في حال تعرضها للهجمات أو التهديدات السيبرانية، من خلال خطة وطنية مُحكمة للتعامل مع المواقف الطارئة.

➢ الأولوية الثالثة: بناء القدرات

نسعى من خلال هذه الاولوية لتعزيز وتقوية مفهوم الأمن السيبراني وعملياته التشغيلية لدى كافة القطاعات الوطنية بشقيه المادي والمعنوي، وذلك من خلال تطوير البنية التكنولوجيا والفنية المشغلة للعميات الرقمية والداعمة لمتطلبات الحماية السيبرانية، واستخدام التقنيات والأنظمة الحديثة التي توفر الحماية للأصول الرقمية. كما سنعمل من خلال هذا التوجه لخلق بيئة سيبرانية أردنية قادرة على التعلم المستمر مُحفزة لعمليات التطوير والتحسين والابداع والابتكار في الأمن السيبراني، مُسلحة برأس مالي بشري على قدرٍ عالٍ من المعرفة والاحترافية في الأداء، قادر على التعامل مع تحديات ومستجدات الفضاء السيبراني وتطويعها لحماية الفضاء السيبراني الأردني.

تعطي الاستراتيجية الوطنية للأمن السيبراني أهمية للحاجة إلى بناء القدرات (أولوية-3)" كأولوية أساسية لتحسين وتعزيز الفضاء السيبراني الأردني، وبالتالي فإن دمج أولوية المرونة والصمود (أولوية-2)، وأولوية الأمن والثقة (أولوية-1) يعزز ويضمن قدرتنا على حماية فضائنا السيبراني على أكمل وجه.

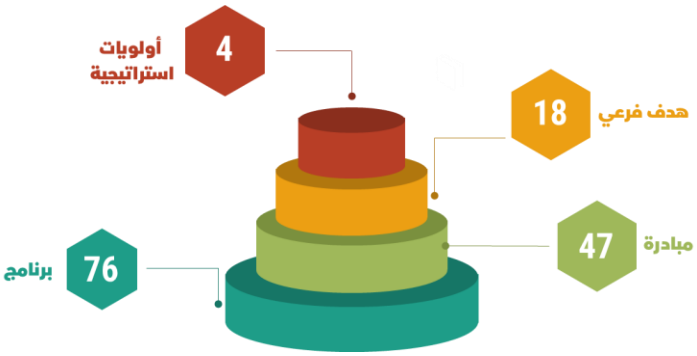
➢ الأولوية الرابعة : التعاون والشراكات

لإن الفضاء السيبراني الأردني لا يمكن تأطيره بحدود جغرافية ولا يمكن عزله عن العالم، ولأن المنظومة التقنية للفضاء السيبراني تجعل منه فضاءً عالمياً متاحاً للجميع، سنعمل من خلال هذه الاولوية على تأطير العلاقات المحلية والإقليمية والدولية، وبما يكفل للفضاء السيبراني الأردني ومكوناته التكنولوجيا والعملياتية والبشرية الانفتاح على الخبرات الإقليمية والعالمية، والاستفادة من قصص نجاح الاخرين وتحويلها لمعرفة صريحة قابلة للتداول والاستنتاج والتطوير. كما سندعم كل الجهود الدولية الرامية لتعزيز مبادئ الاستخدام المسؤول للفضاء السيبراني العالمي.

الأولويات الاستراتيجية

اشتملت هذه الاستراتيجية على:

- ✓ **(4) أولويات رئيسية،**
- ✓ **(18) هدف فرعي،**
- ✓ **(47) مبادرة،**
- ✓ **(76) برنامج.**



1 الأمن

أولوية-1: تطوير بيئة رقمية أردنية آمنة وموثوق بها

الأهداف الفرعية (عددها 4 أهداف):

أولوية 1	تطوير بيئة رقمية أردنية آمنة وموثوق بها
الأهداف الفرعية	1 تعزيز الثقة بأمن البيئة الرقمية الأردنية وتقديم خدمات رقمية آمنة
	2 مساعدة الشركات الصغيرة والمتوسطة في مواجهة التهديدات السيبرانية
	3 ادارة المخاطر المتأتية من استخدام المنتجات الرقمية وسلاسل التوريد
	4 تحقيق التنوع والشمول السيبراني للفئات الأضعف في المجتمع

1. تعزيز الثقة بأمن البيئة الرقمية الأردنية وتقديم خدمات رقمية آمنة

ان البيئة الرقمية الآمنة ضرورة أساسية في عالمنا المترابط اليوم وغيابها يؤثر على الأفراد والشركات على حد سواء، حيث يهدد كلًا من الرفاهية الشخصية والازدهار الاقتصادي، وبالنسبة للأفراد، تعني مساحة رقمية آمنة من الخوف من المتحرشين عبر الإنترنت، وسرقة الهوية، والاحتيال المالي .إنها تضمن حماية المعلومات الحساسة وتعزز الثقة في التفاعلات عبر الإنترنت، كما تتيح البيئة الرقمية الآمنة للأطفال الاستكشاف والتعلم عبر الإنترنت دون التعرض للمحتوى الضار وتمكن الجميع من المشاركة في الاقتصاد الرقمي بثقة.

بالنسبة للشركات، تترجم البيئة الرقمية الآمنة إلى أمان البيانات، حيث تحمي الملكية الفكرية الحيوية ومعلومات العملاء و تقلل من مخاطر الهجمات الإلكترونية التي يمكن أن تعطل العمليات وتضر بالسمعة وتتكبد خسائر مالية كبيرة، وهذا بدوره يعزز الاستثمار والابتكار، حيث تشعر الشركات بالأمان لتطوير وتقديم تقنيات وخدمات جديدة، كما توفر البيئات الرقمية الآمنة أيضًا تكافؤ الفرص بالنسبة للمؤسسات الصغيرة والمتوسطة، مما يسمح لها بالمنافسة بفعالية في السوق العالمية دون خوف من الهجمات الإلكترونية من المنافسين الأكبر.

إن الاستثمار في بيئة رقمية آمنة هو استثمار في مستقبل الأردنيين، فهو يحمي خصوصية الأفراد وأمنهم، ويخلق اقتصادًا رقميًا مزدهرًا وآمنًا، ويعزز الثقة والمشاركة عبر الإنترنت .من خلال العمل معًا لبناء مساحة رقمية مرنة وآمنة، يمكننا إطلاق العنان للإمكانات الكاملة للتكنولوجيا لصالح الافراد والمؤسسات.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

1.1. توفير بيئة انترنت أمنة للمجتمع الأردني من خلال مزودي خدمات الانترنت

ستعمل الحكومة مع مزودي خدمات الانترنت من أجل توفير خدمات انترنت آمنة ومحمية وحجب او التقليل من اعمال التحايل والخداع التي يتعرض لها المواطنون والمؤسسات على حدٍ سواء، ويمكن تحسين أمان البنية التحتية لشبكات الانترنت من خلال اعتماد معايير إنترنت أكثر أمانًا (أمان DNS، والتوجيه الآمن، والتشفير، وما إلى ذلك)، كما ستشجع الحكومة وتدعم جهود مزودي الخدمة في تبني واستخدام تقنيات متطورة لحجب التهديدات السيبرانية عن المستخدمين ومنع وصولها اليهم، وبالاستفادة من الاستخبارات السيبرانية المتوفرة لدى الحكومة والتي يمكن أن تشاركها مع مزودي الخدمة.

ستقوم الحكومة بتنفيذ **برنامج لمسح نطاقات عناوين الانترنت الوطنية** بهدف كشف اية ثغرات فيها وتنبيه أصحابها الى هذه الثغرات لمعالجتها وتحسين مستويات الأمن فيها. كما ستقوم الحكومة بتنفيذ **برنامج يُعنى بحماية المستخدمين من الهجمات المرتبطة بنظام اسم المجال**، او الـ (DNS) يهدف الى إيجاد خط دفاع أول ضد التهديدات المستندة إلى الإنترنت، وحماية المستخدمين عند اتصالهم باستخدام أي جهاز، في أي مكان، وفي أي وقت.

1.2. التأكد من تقديم خدمات الكترونية آمنة وموثوق بها

ستقوم الحكومة بالتأكد من فحص الخدمات الالكترونية الحكومية المقدمة للمواطنين والتأكد من سلامتها من أية ثغرات وستحث القطاع الخاص كذلك على فحص تطبيقاته وخلوها من أية نقاط ضعف يمكن استغلالها للتحايل على المواطنين او اختراق معلوماتهم، وهذا سيسهم في زيادة الاعتماد على الخدمات الالكترونية وفي انتشارها وخاصة خدمات الدفع الالكتروني التي تعتبر عنصر أساسي في الخدمات الالكترونية.

لتعزيز أمن الخدمات الالكترونية المقدمة للمواطنين، ستقوم الحكومة بتنفيذ فحوصات اختراق للخدمات الالكترونية وكذلك رفعها على منصة مكافأة الثغرات واختبارات الاختراق الأردنية (bugbounty.jo)، كما ستشجع الحكومة استخدام البنية التحتية للمفتاح العام (PKI) للمعاملات من/إلى الوزارات والدوائر الحكومية لتعزيز مستويات الأمن السيبراني العالية والثقة في تقديم الخدمات العامة.

كما سيقوم البنك المركزي بالرقابة على الجهات التي تقدم وتدير قنوات الدفع الالكتروني وتتأكد من اتباعها للمعايير والضوابط الصادرة عن الحكومة او اية جهات رقابية او تنظيمية أُخرى.

1.3. تعزيز قدرات مكافحة الجريمة السيبرانية لجهات انفاذ القانون

إن اتخاذ تدابير وقائية أمر بالغ الأهمية للحد من قدرة جهات التهديد على استغلال نقاط الضعف لدينا، حيث أن المواطنون والشركات والجهات الحكومية تكون أكثر قدرة على المواجهة عندما تتخذ كافة الإجراءات الوقائية مسبقاً، حيث تتناقص الجرائم السيبرانية مع كل استثمار في الاجراءات الوقائية، ونتيجة لذلك، ستتفرغ جهات انفاذ القانون والسلطة القضائية الى معالجة القضايا الجوهرية والأسباب الجذرية للجرائم السيبرانية بدلاً من التعامل مع الأعراض فحسب.

وفي الوقت نفسه، من الواضح أن الجرائم السيبرانية سوف تستمر، ولذلك لا تزال هناك حاجة إلى آلية فعالة تقوم بها جهات انفاذ القانون الأردنية لمعالجة الفئة المتبقية من الجرائم السيبرانية، بحيث يتم تحديد مرتكبي الجرائم وجمع الأدلة عن الدور الذي يلعبونه، وتحديد البنية التحتية الإجرامية وتفكيكها. وبما أن مجرمي الإنترنت يعملون بشكل رئيسي في سياق دولي، فإن هذا يتطلب أيضًا التنسيق مع البلدان الأخرى المتضررة.

والهدف هنا في المقام الأول هو بناء القدرات والخبرات المناسبة لدى جميع الجهات الوطنية المعنية بمكافحة الجرائم السيبرانية بحيث يمكن تحقيق قدرات التخطيط والتحقيق المتوقعة من كل جهة بشكل فعال وسريع، والهدف بعد ذلك هو التأكد من أن مكاتب الادعاء العام والمحاكم القضائية لديها ما يكفي من المدعين العامين وقضاة التحقيق والقضاة العاملين المهتمين بالأمن السيبراني والجرائم السيبرانية والذين يتم تأهليهم وتدريبهم تدريبيًا متسقًا لهذا الغرض، ويجب أن تسترشد أنشطة التحقيق والملاحقة القضائية التي تقوم بها السلطة القضائية بسياسة واسعة النطاق بشأن الجرائم السيبرانية منسجمة مع قانون الجرائم الالكترونية لسنة 2015 وتعديلاته.

2. مساعدة الشركات الصغيرة والمتوسطة في مواجهة التهديدات السيبرانية

تعاني الشركات الصغيرة والمتوسطة من نقص في الموارد والخبرات وبالتالي عدم قدرتها على حماية نفسها من أعمال الاختراق التي شهدت زيادة مضطردة في السنوات القليلة الماضية، حيث يشير تقرير[3] صدر حديثاً عن (Identity Theft Resource Center) الى أن 73% من أصحاب الأعمال الصغيرة الذين شملهم الاستطلاع تعرضوا لهجومات سيبرانية فى العام 2023، والحال كذلك ينطبق على الشركات الأردنية الصغيرة، حيث تشير عمليات التقييم المستمرة لنطاقات عناوين الانترنت الاردنية التى يجريها المركز الوطنى للأمن السيبراني والحوادث التى يتعامل معها بشكل شبه يومي، الى وجود ثغرات كثيرة لدى هذه الشركات وضعف ملحوظ في إجراءات الامن السيبراني.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

2.1. توفير منصة لدعم الشركات الصغيرة والمتوسطة

ستوفر هذه المنصة امكانية تقديم النصح والمشورة المباشرة حول أفضل الممارسات من خلال مجموعة من الخبراء فى المركز الوطنى للأمن السيبراني او من خلال شبكة المتطوعين الأعضاء فى نادي أصدقاء المركز، كما ستتيح هذه المنصة إمكانية عمل تقييمات أمنية للمخاطر ولتحديد مستوى نضوج هذه الشركات وبما يتلاءم مع الإطار الوطنى الأردني للأمن السيبراني (JNCSF)، ولتحديد كذلك نقاط الضعف والثغرات وكيفية معالجتها. كما وستوفر المنصة أدوات وحلول تقنية مفتوحة المصدر لمساعدة هذه الشركات فى مراقبة وكشف التهديدات والاختراقات التى تحدث على أنظمتها سواء كانت مُستضافة لديها او مُستضافة من خلال خدمات الحوسبة السحابية.

كما ستعمل الحكومة على توفير المواد التوعوية والمصادر التعليمية والنصائح والارشادات والتحذيرات الموجهة لقطاع الاعمال لتمكينه من مواجهة التهديدات والمخاطر، لا سيما تلك المتعلقة بهجمات الفدية وكيفية تفاديها والتعامل معها في حال وقوعها، وستقوم الحكومة بتطوير منصة (safeonline.jo) وزيادة محتواها التوعوي المخصص لقطاع الأعمال، وخصوصاً الشركات الصغيرة والمتوسطة.

كذلك ستقوم الحكومة باعداد "**دليل الأمن السيبراني**" بغرض أن يكون إطار عمل للأمن السيبراني يمكن للمؤسسة الاستدلال به لحماية أنظمتها وبياناتها من التهديدات السيبرانية وليكون مرجع لمسؤول أمن المعلومات (CISO) ولمسؤول تكنولوجيا المعلومات (CIO) والعاملين في دوائر الامن السيبراني وتكنولوجيا المعلومات وادراة المخاطر في أي مؤسسة.

كما ستقوم الحكومة بتشجيع الشركات الصغرى والمتوسطة على تطبيق الإطار الوطني الأردني للأمن السيبراني (JNCSF) الذي سيساعدها في رفع مستوى النضوج وتطبيق الضوابط الأمنية التي تتناسب مع ملف المخاطر الخاص بالشركة.

2.2. إطلاق برنامج الدفاع السيبراني الفعّال

ضمن برنامج "الدفاع السيبراني الفعّال" ستوفر الحكومة مجموعة من الخدمات المجانية لقطاع الاعمال والمؤسسات ليساعدها على معرفة مدى مرونتها في مواجهة الهجمات السيبرانية وقدرتها على الاستجابة للحوادث الأمنية، كما يساعدها في فحص أنظمتها والتأكد من تحقيقها للحد الأدنى من المعايير وأفضل الممارسات.

3. ادارة المخاطر المتأتية من استخدام المنتجات الرقمية وسلاسل التوريد

يمكن أن تشكل المنتجات والخدمات التى لم تراعى فيها متطلبات الامن فى مراحل التطوير والانتاج نقاط ضعف يمكن للجهات الخبيثة استغلالها بسهولة مما قد يؤدي إلى تقويض ثقة الجمهور فى التكنولوجيا، كما ان العديد من المنتجات الرقمية لا تحتوي على معايير أمان مضمنة في التصميم أو يتم تشغيلها بناء على الاعدادات الافتراضية، ونتيجة لذلك من الممكن أن يُعرض على المستهلكين والشركات منتجات

[3] Identity Theft Resource Center, ITRC Business Impact Report, https://www.idtheftcenter.org/publication/itrc-2023-business-impact-report/, October 2023

وخدمات أقل أماناً، مع عدم وجود خبرة كافية لإدارة المخاطر، وتظهر هذه الإخفاقات بشكل خاص في منتجات "إنترنت الأشياء" (IoT) العالمي وفي سوق الأجهزة الذكية التي تشمل منتجات مثل المركبات ذاتية القيادة وأجهزة الطاقة الموزعة.

من الضروري وضع إطار عمل لتقييم المخاطر الأمنية المتأتية من المنتجات الرقمية وسلاسل التوريد والداخلة الى السوق الأردني، وباستخدام هذا الإطار، ستساعد الحكومة الموردين والجهات الأخرى على إدارة مخاطر سلاسل التوريد واتخاذ قرارات شراء مستنيرة بشأن أمن المنتجات والخدمات، وسنقوم أيضًا بالتشاور مع القطاع الخاص بشأن الإجراءات التى من شأنها الحد من دخول المنتجات الرقمية غير الآمنة الى السوق المحلية.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

3.1. تطوير معايير أمن سيبراني للتقنيات الناشئة وسلاسل التوريد

ستقوم الحكومة بإعداد ضوابط ومعايير أمنية وطنية للتقنيات الرقمية الناشئة بهدف تنظيم عملية توظيف واستخدام هذه التقنيات فى الفضاء الرقمى الأردني وفى الشبكات الرقمية الحساسة والحيوية الوطنية، حيث ستقوم الحكومة بإعداد **ضوابط ومعايير أمنية سيبرانية لإنترنت الأشياء** (IoT)، و**ضوابط ومعايير أمنية سيبرانية لتقنيات الذكاء الاصطناعى** وهدفنا هو التأكد من وجود الحماية المناسبة لضمان ثقة مواطنينا فى أدوات الذكاء الاصطناعى التى يستخدمونها وغيرها من التقنيات الناشئة التى يكون لها تأثير مباشر على أمن الفضاء الرقمي الوطني.

3.2. تنفيذ برنامج للاعتماد وإصدار الشهادات في مجال الامن السيبراني

ستقوم الحكومة، واستناداً لقانون الامن السيبراني بتنفيذ برنامج للاعتماد وإصدار الشهادات في مجال الامن السيبراني بهدف ضمان تلبية متطلبات الامن الوطنى وحماية المستخدمين من أية مخاطر، ويشتمل هذا البرنامج بدايةً على اعتماد المركز الوطنى للأمن السيبراني كجهة وطنية معنية باعتماد وإصدار الشهادات والرُخص المتعلقة ب**المنتجات** و**الخدمات** و**الأشخاص** فى مجالات الأمن السيبراني، ، والعمل على تطوير وإنشاء **"المركز الاردني للكفاءات وشهادات الامن السيبراني"** (Jordan Cybersecurity Competence and Certification Center)، وسيشمل هذا البرنامج بناء الإطار الوطني الاردني لاعتماد المنتجات والخدمات الرقمية (Jordan Cybersecurity Certification Scheme) الذي سيقوم بمنح الشهادات للمنتجات التي تحقق متطلبات الإطار ومعاييره، وبحيث يستند هذا الاطار على المعايير الدولية وعلى أفضل الممارسات في هذا المجال، كما ستعمل الحكومة على **إنشاء مختبر لفحص وتقييم المنتجات الرقمية** يساعد في الاعتماد على القدرات الوطنية الذاتية

3.3. تشجيع الشركات على تطوير حلول رقمية آمنة

تحتاج الحكومة إلى تشجيع الشركات على تطوير حلول برمجية آمنة لأن الأمن السيبراني ضروري لحماية الأمن القومي، والازدهار الاقتصادي، والسلامة العامة، ويمكن أن تسبب البرمجيات التي لم تُبنى على معايير وأُسس أمنية ضررًا كبيرًا للبنية التحتية الحرجة والعمليات الحكومية والأنشطة التجارية والبيانات الشخصية. ستقوم الحكومة بدعم وتشجيع الشركات على تطبيق معايير التطوير الآمن للحلول الرقمية، لتقليل مخاطر نقاط الضعف فى البرامج التى يمكن استغلالها من قبل جهات التهديد الفاعلة، بالإضافة إلى ذلك، ستشجع الحكومة الابتكار والقدرة التنافسية في صناعة البرمجيات من خلال دعم اعتماد تقنيات آمنة وقابلة للتشغيل البيني.

4. تحقيق التنوع والشمول السيبراني للفئات الأضعف في المجتمع

يمكن للتنوع والشمول في أماكن العمل أن تحقق فوائد جمة للمؤسسات على المستوى المالي وعلى المستوى الوظيفي، وتساهم في زيادة الإبداع والابتكار، وزيادة رضا الموظفين، وتقليل التغيب عن العمل، والاحتفاظ بالمواهب بشكل أكبر.

سيتم مراعاة التنوع والشمول في مجال الأمن السيبراني، كجزء من التزام الحكومة بالشمول الرقمي الذي يمنح جميع فئات المجتمع فُرص متساوية سواء في الوصول للخدمات او في فُرص العمل وسيتم دعم مبادرات تحقق هذا الغرض، مثل تمكين المرأة في السايبر, أو مشاريع تشمل كافة فئات المجتمع بما في ذلك الفئات الأضعف في المجتمع، مثل كبار السن والأطفال والمرأة، ولا سيما لتشجيع الأشخاص من هذه الفئات السكانية لمتابعة التدريب أو العمل في مجال الأمن السيبراني

4.1. تمكين المرأة في السايبر

ستقوم الحكومة بتنفيذ برنامج يهدف الى تمكين المرأة في قطاع السايبر، من ناحية تشجيعها على الدخول فيه وتوفير التدريب والتوجيه والإرشاد المناسب ودعم إيصال عدد من النساء الى مواقع قيادية وإشرافية، كذلك دعم صاحبات الاعمال الريادية وتوفير النظام البيئي المناسب لتطورهن.

4.2. دعم القدرة على الوصول لخدمات الامن السيبراني للفئات الأضعف في المجتمع

تدرك الحكومة الأردنية مسؤوليتها في حماية الفئات الضعيفة، وخاصة الأطفال لأنهم عادة ما يفتقرون إلى القدرة على حماية أنفسهم، لذلك، ستسعى الحكومة إلى ضمان استخدام الفئات الضعيفة، وخاصة الأطفال، للفضاء الرقمي بطريقة آمنة ومسؤولة، كما ستنشر الحكومة تدابير تضمن أن تكون الفئات الضعيفة، وخاصة الأطفال، وكذلك القائمين عليهم أو أولياء أمورهم، على علم بالتهديدات والمخاطر السيبرانية، علاوة على ذلك، ستتعاون مع أصحاب المصلحة المعنيين لتطوير ونشر التدابير والأدوات اللازمة لحماية الضعفاء وضمان بقائهم آمنين على الإنترنت.

بالإضافة الى ذلك، ستقوم الحكومة بتخصيص جزء من برامجها في مجالات التوعية والتدريب للفئات المجتمعية الأضعف، كما ستحرص على قدرة هذه الفئات على الاستفادة من جميع البرامج والخدمات السيبرانية التي تقدمها الحكومة وبما يضمن العدالة وتحقيق مبدأ تكافؤ الفرص للجميع.

كذلك ستعمل الحكومة على تسهيل قدرة الافراد على ابلاغ وحدة الجرائم الالكترونية عن الحوادث والجرائم السيبرانية التي يتعرضون لها.

2	المرونة

أولوية-2: حوكمة شمولية للأمن السيبراني على المستوى الوطني وضمان صمود الخدمات الأساسية

الأهداف الفرعية (عددها 5 أهداف):

الأهداف الفرعية	أولوية 2	حوكمة شمولية للأمن السيبراني على المستوى الوطني وضمان صمود الخدمات الأس... ة
	5	تطوير الأطر التشريعية الناظمة للفضاء السيبراني الأردني
	6	توفير متطلبات المرونة السيبرانية لمشغلي البنية التحتية الحرجة والخدمات الوطنية الأساسية
	7	تعزيز صمود ومناعة الشبكات الرقمية الحكومية
	8	التوعية وتسهيل الوصول للمعلومات والمصادر
	9	الاستجابة لحوادث الامن السيبراني التي تهدد الأمن الوطني
	10	حماية وتامين المعلومات الاكثر حساسية للدولة والمجتمع
	11	إدارة استخباراتية فعالة ومنظومة وطنية لمشاركة المعلومات
	12	تعزيز القدرات السيبرانية لمؤسسات الدفاع الوطنية

5. تطوير الأطر التشريعية الناظمة للفضاء السيبراني الأردني

ان حوكمة الامن السيبراني تتطلب مراجعة مستمرة للتشريعات الناظمة لضمان موائمتها للعصر وللتغيرات السريعة وخصوصاً في المجال التكنولوجي الذي هو في تغير ديناميكي مستمر وسريع، وكذلك لسد الثغرات ونقاط الضعف في التشريعات الحالية، وخاصة تلك المرتبطة بقطاعات البُنية التحتية الحرجة، حيث ستعمل الحكومة على تقييم مدى الحاجة الى ضوابط وأطر قطاعية بناءً على حاجة كل قطاع ومتطلباته الخاصة.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

5.1. مراجعة القوانين والأنظمة والتعليمات ذلا العلاقة بالأمن السيبراني

ستعمل الحكومة على تحديد التشريعات المتعلقة بمنظومة الأمن السيبراني او تلك التي ترتبط بها او تؤثر عليها وعمل مراجعة شاملة لها والتأكد من تلبيتها للمتطلبات الأمنية الوطنية ومواكبتها للتطورات العلمية والتقنية المتسارعة ومواءمتها مع المتطلبات الإقليمية والدولية والمعاهدات والاتفاقيات التي يلتزم بها الأردن وكذلك موافقتها لرؤية المملكة للتحديث الاقتصادي 2030.

6. توفير متطلبات المرونة السيبرانية لمشغلي البنية التحتية الحرجة والخدمات الوطنية الأساسية

يجب أن تكون بنيتنا التحتية الحرجة قادرة على الصمود في مواجهة التهديدات السيبرانية والمخاطر الجيوسياسية المتزايدة، مثل جماعات التهديد المتطورة المرتبطة بالدول وجماعات الجريمة السيبرانية المنظمة، والتأكد من عدم تسبب الحوادث السيبرانية في حدوث تأثيرات متتالية عبر الاقتصاد الأردني بسبب الاعتماد المتزايد على خدمات هذه البُنى التحتية الحرجة وعلى الخدمات الالكترونية الاساسية.

تتكون البنية التحتية الحرجة من أنظمة من شأنها أن تسبب أضراراً كبيرة للاقتصاد الاردني والأمن القومي إذا تعرضت لهجوم سيبراني واسع النطاق وعميق، وللحد من مخاطر الاضطرابات الكبيرة التي قد تتعرض لها مجتمعاتنا وقطاعاتنا، يجب أن تكون هذه الأنظمة قادرة على تحمل الهجمات السيبرانية واسعة النطاق، وعندما يتم شن هجمات سيبرانية على بنيتنا التحتية الحرجة وأنظمتنا الحكومية، يجب أن نكون مستعدين للاستجابة من خلال خطة وطنية شاملة وواضحة تضمن التعافي من هذه الهجمات بسرعة وكفاءة عالية، ومع ذلك فإن الاستجابة لحادث سيبراني ما لا تتعلق فقط بالجوانب الفنية، بل تحتاج الحكومة ومشغلي البنية التحتية الحرجة كذلك للعمل معاً لإدارة العواقب المترتبة على الهجوم بشكل مناسب يضمن استمرارية الخدمات الأساسية وانسيابها بشكل معتاد.

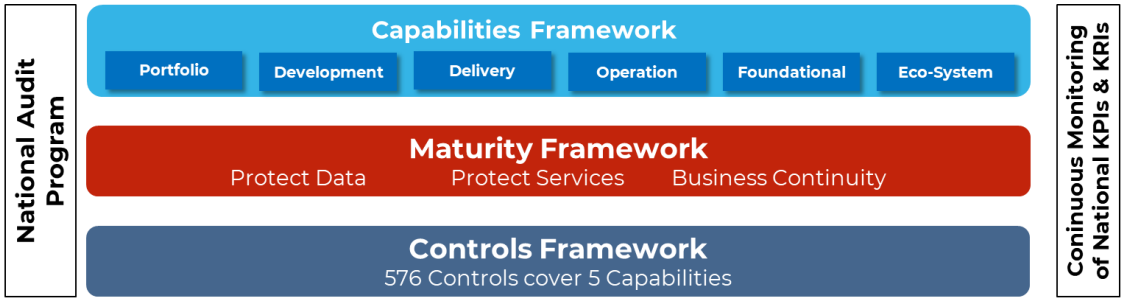
ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

6.1. تطبيق الإطار الوطني الأردني للأمن السيبراني على الحكومة وقطاعات البنية التحتية الحرجة

يمثل الإطار الوطني الأردني للأمن السيبراني (JNCSF)، (بانتظار اقراره من المجلس الوطني للأمن السيبراني)، المعايير الأساسية التي وبحسب نص المادة (8-ب) من قانون الامن السيبراني رقم 16 لعام 2019، يجب أن تلتزم باتباعها "**الوزارات والدوائر الحكومية والمؤسسات الرسمية والعامة والخاصة والأهلية**"[4]، وسيتم خلال العام 2024 وحسب هذه الخطة الاستراتيجية، البدء في تطبيق الإطار على المؤسسات الحكومية ومشغلي قطاعات البنية التحتية الحرجة، ويركز الاطار الأردني على بناء القدرات لدى المؤسسات، حيث تم تحديد (6) قدرات أساسية و (41) قدرة فرعية يجب على المؤسسات ان تلتزم ببنائها خلال مدة زمنية يتم تحديدها بالاتفاق ما بين المؤسسة المعنية والمركز الوطني للأمن السيبراني، وسيمكن بناء هذه القدرات المؤسسات من رفع مستوى نضوجها، حيث ان الاطار الأردني قد اعتمد خمسة مستويات للنضوج (5-1) ونطمح أن تحقق أغلب مؤسساتنا الوطنية مستوى النضوج الرابع على الأقل خلال أول سنتين من تطبيق الاطار.

ستقوم الحكومة بتنفيذ برنامج لمساعدة المؤسسات الحكومية ومشغلي البُنى التحتية الحرجة على فهم وتطبيق الإطار الأردني خلال العام 2024، وسيتم خلال الأعوام اللاحقة تقييم الامتثال لهذه المؤسسات وفي نفس الوقت مساعدتها على تحقيق الامتثال من خلال تقديم الارشادات والدعم اللذين تحتاجهما المؤسسات.

[4] قانون الامن السيبراني رقم 16 لعام 2019



الهيكل العام للإطار الوطني الأردني للأمن السيبراني

6.2. تعزيز وتطوير المنظومة الوطنية للتدقيق ومراقبة الالتزام

يُعد الالتزام بقانون الامن السيبراني والأنظمة والتعليمات، وكذلك بالسياسات والمعايير والضوابط الصادرة عن المركز عُنصر أساسي في تعزيز صمود المؤسسات الحكومية والبُنى التحتية الحرجة، كما أن القانون قد منح المركز صلاحية اتخاذ الإجراءات المنصوص عليها في المادة (16) من القانون بحق الجهات المخالفة والتي تم توضيحها بموجب "تعليمات مخالفات الا من السيبراني"[5] الصادرة عن المركز عام 2023.

ستتأكد الحكومة من فهم الجهات المُلزمة بموجب قانون الامن السيبراني رقم 16 لعام 2019، بما في ذلك مشغلي قطاعات البنية التحتية الحرجة، لالتزاماتهم بموجب الإطار الوطني الأردني للأمن السيبراني (JNCSF)، بما في ذلك الالتزام بتطوير برنامج إدارة مخاطر البنية التحتية الحرجة وادامته والامتثال له.

وستقوم الحكومة **بإطلاق جائزة التميز في الأمن السيبراني** للمؤسسات والافراد، بهدف تحفيز المؤسسات العامة والخاصة على تطوير بيئاتها السيبرانية وتطبيق الأطر والمعايير الوطنية والامتثال لها، وهذا سيساعد في رفع نضوج المؤسسات والافراد وتحقيق هدف المرونة والصمود.

6.3. تطوير إطار عمل وضوابط خاصة بقطاعات البُنية التحتية الحرجة

لحماية بُنانا التحتية الحرجة، ستعمل الحكومة على تطوير إطار عمل وضوابط سيبرانية لمشغلي البنية التحتية الحرجة، وسيتضمن الإطار تحديد التزامات الأمن السيبراني للمشغلين، مما يتطلب منهم اتخاذ تدابير معززة لضمان تعافي البُنى التحتية الحرجة بسرعة وكفاءة من أي هجوم سيبراني قد تتعرض له.

كما ستعمل الحكومة من خلال المركز الوطني للأمن السيبراني والهيئات التنظيمية القطاعية على تطوير وتنفيذ برنامج لتقييم البُنى التحتية الحرجة ووضع "خطة حماية" لكل قطاع من هذه القطاعات

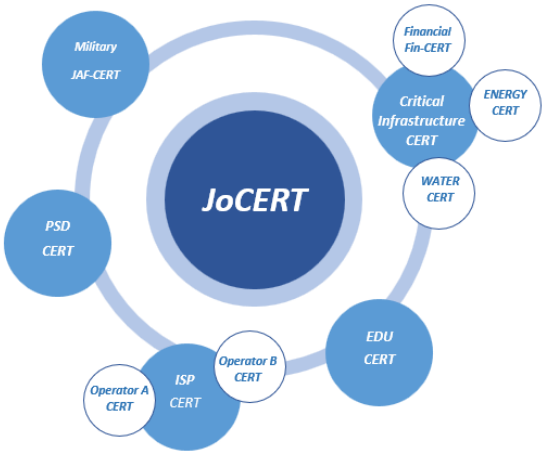
6.4. تطوير قدرات المراقبة وفرق الاستجابة القطاعية[6]

توفر فرق الاستجابة القطاعية (Sectoral CERTs) المساعدة في حل الحوادث السيبرانية داخل القطاع باستخدام مصادره المتوفرة، ويتم ذلك غالبًا عبر تقنيات متخصصة تتطلب معالجة محددة، فعلى سبيل المثال، يستخدم القطاع العسكري في كثير من الأحيان تقنيات أو أدوات تحكم في القيادة والسيطرة تتطلب مستوى معينًا من الخبرة في الاستجابة لحادث ما، وهذا الوضع يختلف عند الحديث عن فريق استجابة يتبع إلى شركة من القطاع الخاص او الى قطاع حرج، حيث لا تختلف تقنياتها فقط ولكن تختلف أيضاً اهتماماتها.

[5] تعليمات مخالفات الامن السيبراني،

وجود فرق استجابة قطاعية ترتبط أفقياً مع بعضها البعض وعامودياً مع فريق الاستجابة الوطني، هي من أفضل الممارسات في النظام البيئي التي تتعايش فيها منظومة هرمية من فرق الاستجابة، وهي الممارسة التي توجد فيها بيئة تعاونية للتنسيق المستمر وتبادل المعلومات؛ وهذا يسمح لفريق الاستجابة الوطني بالوصول إلى بانوراما حقيقية ومحدثة حول تهديدات الأمن السيبراني التي تواجه أي بلد عبر قطاعاته، وبالتالي إنشاء نهج وطني للأمن السيبراني، والذي يصبح بعد ذلك جزءًا من الحوكمة الرقمية.

ستقوم الحكومة بتشجيع انشاء فرق استجابة قطاعية بناءً على احتياجات كل قطاع ومتطلباته الخاصة، كما ستشجع الحكومة بناء مراكز عمليات أمنية (Security Operation Centers) قطاعية ودعم وتحسين القائم منها، بحيث ترتبط جميعها بمركز عمليات وطني واحد وبشكل هرمي بهدف تسهيل وتعزيز إجراءات الاستجابة وتبادل المعلومات بشكل انسيابي وسريع وخلق المعرفة الجماعية وتبادل أفضل الممارسات.



هيكلية فرق الاستجابة القطاعية وارتباطها مع فريق الاستجابة الوطني

وستكون شبكة مراكز العمليات بمثابة درع حقيقي للأمن السيبراني للمملكة، حيث ستوفر شبكة قوية من مراكز المراقبة، القادرة على اكتشاف التهديدات المحتملة قبل أن تتسبب في أضرار واسعة النطاق.

7. تعزيز صمود ومناعة الشبكات الرقمية الحكومية

على مدى السنوات الماضية، استثمرت الحكومة الأردنية ممثلةً بوزارة الاقتصاد الرقمي والريادة بشكل كبير في بناء شبكة قوية في جميع أنحاء المملكة لخدمة الهدف الذهبي المتمثل في ربط جميع الجهات الحكومية لتقديم خدمة أفضل للمواطنين الأردنيين، وتُعتبر الشبكة الحكومية الآمنة (SGN) العصب والشريان والمحرك الداعم لعملية التحول الرقمي والذd تعتمد عليه أغلب الخدمات الرقمية في القطاعين العام والخاص، ولذلك فإن صمود الشبكة الحكومية الآمنة أمر حيوي وأساسي في صمود باقي الخدمات الأساسية الوطنية.

ولا يمكن حقيقة أن المعلومات والخدمات الحكومية أهدافًا عالية القيمة لجهات التهديد الفاعلة، ويمكن أن تهدد الحوادث السيبرانية سلامة المعلومات التي تحتفظ بها الحكومة، ويمكن ان تهز ثقة الجمهور في مؤسساتنا وفي الخدمات الرقمية المختلفة التي تقدمها الحكومة، وهذا يدلل ان الحكومة بحاجة ماسة إلى اتباع نهج جديد للأمن السيبراني الحكومي.

من مبدأ الشفافية والمعاملة بالمثل، فإن الحكومة ستلتزم بنفس المعايير التي تفرضها على قطاعات البنية التحتية الحرجة، كون الحكومة هي أيضاً مشغل ومالك لبعض منشآت البنية التحتية الحرجة، كما أنها تحتفظ ببعض البيانات الأكثر حساسية حول المواطنين والاقتصاد والامن كجزء من وظائفها الأساسية، ولهذا فستقوم الحكومة بتعزيز المسائلة القانونية ومحاسبة الجهات المقصرة في الامتثال للأطر والضوابط والمعايير الوطنية.

لقد كشفت التقييمات الأمنية التي نفذتها الحكومة خلال عام 2023 لأكثر من (47) مؤسسة حكومية ووطنية، وكذلك الشبكة الحكومية الآمنة، الى انخفاض مستويات النضوج السيبراني للعديد من المؤسسات الحكومية ووجود ثغرات أمنية بحاجة الى معالجة آنية، والى وجود مخاطر جدية تتعلق بإمكانية سرقة المعلومات وإمكانية حدوث تعطل للخدمات الرقمية الأساسية، كما أشارت هذه التقييمات الى وجود نقص كبير في المهارات السيبرانية لدى المؤسسات الحكومية.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

7.1. وجود رؤية وفهم وسيطرة على الأصول الرقمية الحكومية

بدون رؤية للأصول الرقمية الحكومية وأصول البيانات، وكذلك المستخدمين، فإن مخاطر الأمن السيبراني تظل غير معروفة ولا يمكن إدارتها، ولا يقتصر الأمر على تقييد هذه الرؤية المحدودة من قدرة المنظمة على حماية ممتلكاتها، بل إنها تقلل من قدرة الحكومة على تحديد المخاطر التي يمكن أن تعالجها أو تتصرف بشأنها.

ستعمل الحكومة على أن يكون لدى جميع المؤسسات الحكومية طريقة نشطة ومؤتمتة لاكتشاف الأصول وإدارتها لتحديد الأنظمة والأجهزة والبرامج التي يمتلكونها ويعملون عليها بشكل مستمر. كذلك ستعمل الحكومة على إيجاد الآليات المناسبة لتمكين تحديد نقاط الضعف وتقييمها وإدارتها بسرعة، ووضع برامج قوية لإدارة الثغرات الأمنية في جميع المؤسسات الحكومية لضمان إدارة نقاط الضعف المحددة بشكل فعال.

7.2. وجود رؤية شاملة للبيانات التي تتعامل معها الحكومة وتشاركها مع الآخرين

سيكون لدى المؤسسات الحكومية رؤية شاملة لأصول البيانات الخاصة بها، من البيانات الشخصية إلى المعلومات السرية، وسيتم حمايتها بما يتناسب مع المخاطر وبما يتوافق مع تشريعات حماية البيانات، وبالتالي، سيكون لدى المؤسسات الحكومية فهم ناضج لأصول البيانات التي تتعامل معها، وكيفية تخزينها أو استضافتها، ومكان مشاركتها، حتى تتمكن من تقييم المخاطر التي تمثلها بشكل مناسب والتأكد من وضع وسائل حماية كافية لإدارتها.

7.3. إدارة المخاطر الناجمة عن الموردين التجاريين على الحكومة

بهدف إدارة المخاطر المتأتية من سلاسل التوريد، أصدرت الحكومة "*سياسة اعتماد منتجات الامن السيبراني*"[7] التي تحدد الإجراءات التي يجب على المؤسسات اتباعها في عمليات شراء منتجات وخدمات الامن السيبراني، كذلك أصدرت الحكومة "*معايير وضوابط الأمن السيبراني للجهات المتعاقدة مع الحكومة*"[8]، وهي ضوابط تلزم الشركات الموردة والمتعاقدة مع الحكومة بالامتثال للمعايير الوطنية فيما يتعلق بتداول المعلومات الحكومية وكيفية التعامل معها.

ستتخذ الحكومة خطوات لدراسة وفهم درجة اعتمادها على الموردين وعلى سلاسل التوريد بشكل أفضل والتأكد من دمج منتجاتهم وخدماتهم في الأنظمة الحكومية بطريقة تأخذ في الاعتبار تأثيراتها على الأمن الوطني والقدرة على الصمود، وستقدم الحكومة نموذجاً يحتذى به في شراء واستخدام المنتجات والخدمات الرقمية.

7.4. التأكد أن التقنيات الحكومية مهيئة بشكل صحيح

من المعروف أن التكنولوجيا والخدمات الرقمية آمنة فقط بقدر ما تسمح به بنيتها وتكوينها، ولهذا ستعمل الحكومة على تطوير تكوينات الأمان الأساسية (Baseline Security Configuration) لجميع الأنظمة والأصول الرقمية لديها، وحتى تتمكن المؤسسات الحكومية من اعتمادها وتطبيقها لديها بشكل متجانس على مستوى الحكومة، وهذا سيؤدي الى توفير مستوى أساسي من الأمن السيبراني، مما سيقلل بشكل كبير من المخاطر الشائعة الناجمة عن التكوين الخاطئ.

7.5. تصنيف البيانات الحكومية والتعامل معها بشكل مناسب

[7] سياسة اعتماد منتجات الأمن السيبراني، https://ncsc.jo/Ar/List/Policies_and_Strategies_AR

[8] معايير وضوابط الامن السيبراني للجهات المتعاقدة مع الوزارات والدوائر الحكومية https://www.ncsc.jo/Ar/List/Laws_AR

ستقوم الحكومة بتحديث سياسة تصنيف البيانات المعمول بها حالياً، لتحسين التعامل مع المعلومات في المستوى الرسمي والتأكد من أن المعلومات الأكثر حساسية الموجودة في هذا المستوى محمية بشكل مناسب ومستمر، كما ستوفر الحكومة للمؤسسات الحكومية إرشادات حول كيفية التعامل مع المعلومات المصنفة والغير مصنفة من ناحية حفظها وتخزينها وارسالها واتلافها ومشاركتها، حتى يتمكنوا من حماية المعلومات السرية بشكل أفضل.

7.6. مراقبة الشبكات والأنظمة والتطبيقات والأجهزة الطرفية الحكومية لكشف التهديدات

تتوفر لدى الحكومة، من خلال مركز المراقبة الحكومي (GovSOC) القدرة على مراقبة الشبكات الحكومية والقدرة على الاحتفاظ بالسجلات لتسهيل اكتشاف التهديدات السيبرانية، وستستمر الحكومة في تنفيذ مراقبة شاملة قدر الإمكان، بدءاً من مراقبة البنية التحتية الأساسية، مثل النطاقات، وحتى مراقبة الأجهزة الطرفية وأجهزة الشبكة والخدمات المستندة إلى السحابة، وكذلك مراقبة الحسابات وخاصة تلك التي تتمتع بصلاحيات مدير النظام.

ستسعى الحكومة دائماً لتطوير عملياتها السيبرانية وتحديثها وكذلك تطوير العاملين فيها وتطبيق أفضل الممارسات العالمية لضمان الكشف المبكر عن التهديدات.

7.7. تطوير قدرات الاستجابة لدى الحكومة

ستعمل الحكومة على تطوير قدرات فرق الاستجابة الحكومية والتأكد من امتلاكها الأدوات والخبرات اللازمة للتعامل مع الحوادث المعقدة والتحقيق فيها وكشف الجهات المهاجمة ومعرفة تبعيتها. سيقود فريق الاستجابة الوطني (**JoCERT**) بالتعاون مع فرق الاستجابة الأخرى عمليات الاستجابة للحوادث السيبرانية وسيتأكد من جاهزية باقي الفرق وسيتبادل معها المعلومات والخبرات.

7.8. تحسين وتعزيز قدرات الامن السيبراني في الوزارات والدوائر الحكومية

ستقوم الحكومة الأردنية خلال العام 2024 بالاستثمار بشكل كبير لمعالجة الثغرات التي كشفتها التقييمات الأمنية التي قام بها المركز، حيث ستطلق الحكومة "**برنامج تعزيز قدرات الامن السيبراني في الوزارات والدوائر الحكومية**" بهدف تعزيز مناعة كل من الشبكة الحكومية الآمنة وشبكات الوزارات والدوائر الحكومية. وسيشمل البرنامج مراجعة شاملة للإجراءات الأمنية والتأكد من وجود سياسات وخطة أمنية سيبرانية لكل مؤسسة بالتوازي مع البرنامج المذكور في (الهدف رقم 6.1) والمتعلق بتطبيق الإطار الوطني الأردني في المؤسسات الحكومية.

7.9. رفع المهارات السيبرانية للعاملين في دوائر تكنولوجيا المعلومات

ستقوم الحكومة بتنفيذ برنامج تدريبي لكافة العاملين في أمن المعلومات والامن السيبراني في الوزارات والدوائر الحكومية بهدف رفع كفاءاتهم واعطاؤهم المهارات التي يحتاجونها لحماية المعلومات التي يديرونها ويشرفون عليها.

7.10. إنشاء شبكة اتصالات معلوماتية حكومية مشفرة وآمنة

تعتمد الحكومة بشكل كبير على الشبكة الحكومية الآمنة (SGN) في تبادل المعلومات بين الوزارات والدوائر الحكومية، ولهذا ستعمل الحكومة لضمان سرية هذه الشبكة من خلال اعتماد منظومة تشفير حكومية تعتمد على تقنيات متطورة قادرة على مواجهة تحديات عصر ما بعد الحوسبة الكمية (Quantum Computing) التي أصبحت بعده أغلب خوارزميات التشفير ضعيفة ولا تصلح للاستخدامات الحكومية واستخدامات القطاعات الحرجة.

8. التوعية وتسهيل الوصول للمعلومات والمصادر

سوف نسعى إلى رفع مستوى الوعي بين الافراد والشركات ليس فقط حول المخاطر التي قد يتعرضون لها، ولكن أيضًا حول الحاجة إلى فهم الإجراءات التي يمكنهم القيام بها بأنفسهم أو من خلال الموارد التي توفرها المؤسسات الوطنية، كمنصة (safeonline.jo) لفهم المخاطر وطرق الحماية منها.

كما تلتزم الحكومة الاردنية من خلال مؤسساتها المختلفة بتنفيذ حملات توعوية على مدار السنة، كما سنقوم بنشر التحذيرات المتعلقة بالتهديدات والثغرات الأمنية من خلال موقع الفريق الوطني للاستجابة لحوادث الامن السيبراني[9] ومنصات مديرية الامن العام والمنصات الأخرى التي تتبع فرق الاستجابة القطاعية.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

8.1. التوعية بالمخاطر المتأتية من الفضاء السيبراني

بالبناء على النتائج الإيجابية والتفاعل الكبير مع حملات التوعية للأعوام السابقة، مثل حملة "تلميحه رقمية" التي نفذها المركز الوطني للأمن السيبراني في الأعوام 2022 و2023، وكذلك حملة "المناعة الرقمية" التي تبنتها أمانة عمان للعام 2023، سنستمر في تنفيذ حملات وطنية مدروسة ضمن برنامج وطني أشمل يهدف للوصول الى اكبر شريحة من المجتمع، وبالأخص تلك الشرائح الأكثر عُرضة والاقل قدرة على التعامل مع المخاطر، كفئات الأطفال والنساء وكبار السن، كما سنقوم بتشجيع المحتوى التوعوي ودعمه، كما سنشجع على تنفيذ الحملات المشتركة بين أكثر من قطاع بهدف بث رسالة واحدة واضحة، وفي هذا السياق سيقوم المركز الوطني للأمن السيبراني بإثراء منصة (Safeonline.jo) ودعمها وتوسيع الشرائح التي تغطيها وتنويع محتواها والترويج لها للوصول الى عدد أكبر من المتلقين.

8.2. تسهيل الوصول للمعلومات والتحذيرات

سيتم من خلال منصات فرق الاستجابة الحكومية والقطاعية ومنها منصة الفريق الوطني للاستجابة لحوادث الأمن السيبراني (JoCERT) تزويد الجهات الوطنية بالتحذيرات الأمنية حول التهديدات وكذلك المعلومات المتعلقة بالثغرات الأمنية التي يتم نشرها من قبل الجهات والشركات الصانعة والمنصات الدولية المتخصصة، كما سيتم انشاء نظام انذار مبكر (Early Warning System) لتوزيع هذه التحذيرات بشكل سريع وفوري للقطاعات الحيوية ومؤسسات البنى التحتية الحرجة.

9. الاستجابة لحوادث الامن السيبراني التي تهدد الأمن الوطني

لقد حدد المركز الوطني للأمن السيبراني معايير لتصنيف حوادث الامن السيبراني تم بموجبها تصنيف حوادث الأمن السيبراني الى أربع فئات هي: "**المنخفض**" و "**المتوسط**" و "**الخطير**" و "**شديد الخطورة**". وتستلزم الحوادث التي تشكل خطراً على أمن المملكة وسلامتها"[10] استجابة وطنية موحدة يتم ادارتها بالتعاون مع جميع أصحاب العلاقة وبإشراف "المركز الوطني للأمن وإدارة الازمات" بصفته الجهة المعنية بإدارة الازمات والكوارث التي تؤثر على الامن الوطني، الذي سيشكل خلية أزمة للتعامل مع "تداعيات" الحادثة.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

9.1. خطة الطوارئ للاستجابة لحوادث الأمن السيبراني

تحدد خطة الطوارئ للاستجابة لحوادث الأمن السيبراني الخطوات والإجراءات للتعامل مع الحوادث السيبرانية المصنفة بدرجة "خطير" و "شديد الخطورة"، وهي أداة حيوية لتعزيز المرونة الوطنية والاستعداد ضد التهديدات السيبرانية، ولحماية البنية التحتية الحرجة.

وتساعد خطة الطوارئ الوطنية في تنسيق جهود أصحاب المصلحة في جميع القطاعات للاستجابة للحوادث السيبرانية في الوقت المناسب وبطريقة فعالة، كما أنها تحدد الأدوار والمسؤوليات والقدرات وقنوات الاتصال لكل أصحاب المصلحة لتجنب الارتباك وازدواجية الجهود.

كما توفر إطاراً ولغة مشتركة لتقييم مدى خطورة الحوادث السيبرانية وتأثيرها ونطاقها، وتحديد أولويات إجراءات الاستجابة، كما أنها تسهل تبادل المعلومات والاستخبارات وأفضل الممارسات بين أصحاب المصلحة لتعزيز الوعي الظرفي والدفاع الجماعي. كما تساعد خطة الطوارئ الوطنية في استعادة الأنظمة والخدمات المتضررة، وتحديد وتنفيذ الدروس المستفادة وإجراءات التحسين.

---

[9] JoCERT website, https://jocert.ncsc.jo

[10] المادة 9/أ من قانون الأمن السيبراني

ستقوم الحكومة **بتطوير خطة طوارئ وطنية للاستجابة لحوادث الامن السيبراني** الخطرة وشديدة الخطورة التي يكون لها بُعد أمني او اقتصادي او تؤثر على قدرة المواطنين على الوصول للخدمات الأساسية في الدولة.

9.2. تمارين سيبرانية لفحص صمود البنية التحتية الحرجة

التمارين السيبرانية هي سيناريوهات محاكاة تختبر قدرة مشغلي البنية التحتية الحرجة على منع الهجمات السيبرانية واكتشافها والاستجابة لها والتعافي منها. وهي مصممة لتعزيز أمن ومرونة البنى التحتية الوطنية الحرجة (CNIs)، وهي الأنظمة التي تدعم الخدمات والوظائف الأساسية للمجتمع والاقتصاد، وتساعد التمارين السيبرانية مشغلي البنية التحتية الحرجة على تحديد نقاط الضعف والثغرات وأفضل الممارسات والدروس المستفادة في دفاعاتهم السيبرانية، بالإضافة إلى تحسين التنسيق والتعاون مع أصحاب المصلحة الآخرين، مثل المؤسسات الحكومية والقطاع الخاص.

ستقوم الحكومة بتنفيذ **برنامج للتمارين السيبرانية** يغطي كافة القطاعات ويكون بشكل دوري وستشجع الحكومة وتدعم المشاركة الفعالة في هذه التمارين وستعمل ما بوسعها لأن تكون هذه التمارين شمولية وواقعية وستضع مؤشرات لقياس مدى تأثير هذه التمارين على جاهزية القطاعات واستعدادها.

10. حماية وتامين المعلومات الاكثر حساسية للدولة والمجتمع

تعد البيانات مصدرًا مهماً لنمو الاقتصاد الأردني وحجر أساس في عمليات التحول الرقمي، حيث تساعد المؤسسات على إجراء المعاملات واتخاذ قرارات أفضل وتحسين منتجاتها وخدماتها، ويساعد حوكمة البيانات بشكل فعّال المواطنين في الوصول إلى السلع والخدمات المصممة خصيصًا لتلبية احتياجاتهم، لكن في نفس الوقت فإن وقع هذه البيانات في الأيدي الخطأ قد يسمح للجهات الخبيثة بإلحاق الضرر بنا، كاستخدامها في الابتزاز للحصول على فدية، كما أن سوء التعامل مع البيانات الحساسة والحرجة قد يؤدي إلى إلحاق ضرر جسيم بالمصالح الوطنية.

10.1. حفظ البيانات الوطنية الحساسة

في حين تخطط وزارة الاقتصاد الرقمي والريادة لتطوير مركز البيانات الحكومي الحالي وانشاء مراكز بيانات جديدة تتمتع بتوافريه عالية للبيانات (High Availability)، يقدم المركز الوطني للأمن وادرة الازمات مركز تعافي من الكوارث (Disaster Recovery) ضمن أعلى المواصفات العالمية ليشمل بخدماته كافة القطاعات الوطنية، كما تقدم عدد من الشركات خدمات الاستضافة وخدمات الحوسبة السحابية للقطاع الخاص.

هنالك بيانات حساسة لدى القطاعين العام والخاص لا يمكن لنا القبول بضياعها او فقدها او تلفها، وبشكل فقدها او تلفها تهديد للأمن الوطني والسلم المجتمعي، وفي حين تتخذ المؤسسات الوطنية الاحتياطات اللازمة لضمان حماية معلوماتها من الضياع او التلف، الا اننا لا زلنا بحاجة الى استراتيجية موحدة تضمن بشكل قطعي ان أكثر معلوماتنا حساسية تتمتع بأعلى درجات الحفظ والعناية. وبالنظر الى هذا الواقع نرى ضرورة لوجود مركز مفصول (offline) تكون مهمته الأساسية حفظ البيانات الوطنية الأكثر حساسية وأهمية ضمن بيئة توفر أعلى معايير الحفظ وتضمن عدم ضياعها او تلفها تحت أي ضرف من الظروف.

لهذا الغرض، ستقوم الحكومة **بإنشاء مركز حفظ البيانات الوطنى (NDV)** بحيث يتبع تنظيمياً المركز الوطنى للأمن السيبراني ويقدم خدماته للقطاعين العام والخاص، كما ستعمل الحكومة على وضع الضوابط والمعايير التى تحديد البيانات الأكثر حساسية وأهمية فى الأردن والتي ستلتزم الجهات بحفظها في "مركز حفظ البيانات الوطني"، وكذلك وضع الأطر التشريعية اللازمة لذلك.

كما ستقوم الحكومة **بمراجعة سياسات حفظ المعلومات الحكومية** وعمل ما بوسعها من أجل ضمان عدم ضياعها او فقدانها.

10.2. ضوابط أمنية لخدمات الاستضافة

ستقوم الحكومة بتحديث وتطوير الضوابط والمعايير الأمنية التي تنظم عملية استضافة المعلومات الحكومية لدى مقدمي خدمات الاستضافة (data Center Providers) او مقدمى خدمات الحوسبة السحابية (Cloud Service Providers) المرخصين فى المملكة، وفي الوقت الحالي فإن "سياسة المنصات السحابية وخدماتها 2020" التي أصدرتها وزارة الاقتصاد الرقمي والريادة هي

السياسة الوحيدة في هذا المجال وهي تهدف بالأساس الى بناء منظومة متكاملة للسحابة الأردنية وتطويرها بشكل يسهم في نمو الاقتصاد الرقمي في الأردن وتوجيه الجهات الحكومية نحو الاستخدام الأمثل للخدمات السحابية، وفيما ان السياسة حددت تصنيفات المعلومات التى يمكن استضافتها لدى كل من السحابة الحكومية والقطاع الخاص داخل الأردن ولدى كذلك القطاع الخاص خارج الأردن، الا ان هنالك حاجة لوضع ضوابط حول أمن المعلومات فى السحابة تحدد المبادئ العامة لأمن معلومات المستفيدين والتى يتم تخزينها ونقلها ومعالجتها في النظم السحابية وتوضيح جميع التزامات مزودي الخدمات السحابية في الأمن السيبراني وضمان أمن البيانات التي يتم الاحتفاظ بها في خدمات الحوسبة السحابية بطريقة فعالة.

كما سنعمل على إصدار تعليمات ترخيص لخدمات الامن السيبراني السحابية، مثل خدمات (SASE, SWG, CASB, FWaaS, and ZTNA)، وغيرها من الخدمات التي قد ترغب المؤسسات الوطنية الاستفادة منها.

11. إدارة استخباراتية فعالة ومنظومة وطنية لمشاركة المعلومات

تعد المراقبة والتقييم المستمر للتهديدات السيبرانية الدولية أمراً بالغ الأهمية للحد من مخاطر الهجمات والحوادث السيبرانية، وهى الخطوة الأولى فى أي عملية دفاعية، ويجب تحديد النوايا السيبرانية وقدرات الجهات النشطة ضد مصالحنا الأساسية والحيوية، كما يجب مراقبة مصادر التهديدات المحتملة، ومن أجل حماية شبكاتنا المعلوماتية، يجب معرفة تطور تكتيكات هذه الجهات وتقنياتها وإجراءاتها التقنية قدر الإمكان، كما يجب تقييم وسائل حمايتنا المتعلقة بها.

ومن المعلوم ان جماعات التهديد تستخدم في كثير من الأحيان برمجيات خبيثة معروفة ومتداولة على شبكة الإنترنت المظلم ويعيدون تكييفها بحيث تناسب أهدافهم، بالإضافة الى تطويرهم أحياناً برمجيات خبيثة خاصة بهم عالية التقنية بهدف التخفي وتفادي الكشف والبقاء مجهولين، كما انهم يديرون ويشغلون بُناً تحتية منتشرة فى جميع إنحاء العالم مستغلين غياب الرقابة والتدقيق فى كثير من الدول وصعوبة تتبع هذه الشبكات كونها تمتد فى أكثر من دولة وبالتالى يصعب على جهات انفاذ القانون تتبعها وكشفها. وضمن هذه المعطيات ستقوم الحكومة بكل ما فى وسعها لكشف وتعطيل نماذج عمل جماعات التهديد من خلال كشف تكتيكاتها وتقنياتها واجراءاتها، وكذلك الكشف الاستباقي لنواياها ومراقبة نشاطاتها على شبكة الانترنت المظلم والتعاون مع المنظمات الدولية وجهات انفاذ القانون الدولية لتعقب نشاطاتها وجلبها للعدالة.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

11.1. تعزيز وتأطير الجهود الوطنية لتبادل المعلومات

مع تزايد التهديدات السيبرانية من حيث الحجم والتعقيد، فإن فهم صورة التهديد على مستوى المملكة بأكملها أمر بالغ الأهمية للاستعداد وتخفيف المخاطر، ومن هذا المنطلق فقد أنشأ المركز الوطني للأمن السيبراني منصة (شارك)[11] لتبادل المعلومات على المستوى الوطني، حيث ستساعد هذه المنصة الوطنية في رسم صورة متكاملة وفهم موحد للحوادث والتهديدات والثغرات على مستوى المملكة وكذلك آلية للتواصل وبناء العلاقات بين العاملين في قطاعات الامن السيبراني في القطاعين العام والخاص.

ستسعى الحكومة الى تأطير الجهود الوطنية لتبادل المعلومات حول التهديدات والمخاطر والحوادث السيبرانية بين مختلف القطاعات من خلال وضع السياسات والتشريعات وكذلك الأدوات الإجرائية والفنية الضرورية لتحقيق ذلك، كما **ستشجع الحكومة على تبادل المعلومات على المستوى القطاعى** وإنشاء منصات قطاعية لتبادل المعلومات (ISAC)[12]، وكذلك ما بين القطاعات وبشكل لا يضر بمصلحة أي قطاع او أي جهة.

12. تعزيز القدرات السيبرانية لمؤسسات الدفاع الوطنية

[11] "Sharek" Information Sharing Platform, https://Sharek.ncsc.jo

[12] Information Sharing and Analysis Centers provide a central resource for gathering information on cyber and related threats to critical infrastructure and provide two-way sharing of information between the private and public sectors.

لقد أصبح الفضاء السيبراني بشكل متزايد هدفًا وأداة في الصراعات الدولية، كما ان العديد من الدول قد حددت الفضاء السيبراني باعتباره مجالًا عملياتياً جديدًا (بالإضافة إلى المجالات البرية والجوية والبحرية التقليدية) يمكن من خلاله إجراء العمليات العسكرية والاستخباراتية[13]، كما يستغل خصومنا كل فرصة في الفضاء السيبراني وعبره لتعزيز موقعهم المعلوماتي وتعطيل أنظمتنا المدنية والعسكرية وتقويض الثقة في المعلومات التي تدعم قدرتنا على تنفيذ عملياتنا، ولهذا فإن التوسع في القدرات السيبرانية لدى القوات المسلحة الأردنية- الجيش العربي يجب ان يكون إحدى الأولويات في الخطة الإستراتيجية الدفاعية، والتي ستؤدي في النهاية إلى إنشاء مكون يركز بشكل خاص على التهديد السيبراني ويهدف الى فهم أفضل للتهديد السيبراني والحماية منه، وفهم أفضل للفرص، وستحدد الاستراتيجية السيبرانية للقوات المسلحة الاردنية هذه الأهداف بشكل واضح وملموس.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

12.1. تطوير استراتيجية القوات المسلحة للأمن السيبراني

إن القوات المسلحة الأردنية هي الحصن الوطني المنيع وحامية التنمية والنهضة وصانعة أجواء الامن والأمان والاستقرار، وهي الموكل لها مهمة الدفاع عن الوطن وحمايته من أي عدوانٍ خارجي، وحيث أن القوات المسلحة تواكب التطور العلمي والتقني وتحدث بشكل مستمر وتطور قدراتها الدفاعية بما يتلاءم مع مستويات التهديد وتطورها، وحيث أن الفضاء السيبراني اصبح مسرحاً عملياتياً جديداً تستخدمه وتوظفه العديد من دول العالم في تحقيق أهدافها السياسية والعسكرية والاقتصادية واصبح أداه للتأثير في ساحة المعركة وتوظفه قبل واثناء وبعد تنفيذ العمليات العسكرية، تدرك القوات المسلحة أهمية وضع استراتيجية دفاعية للأمن السيبراني، تحدد من خلالها أولوياتها الدفاعية السيبرانية ضمن المتغيرات والمعادلات الإقليمية الجيوسياسية والتهديدات الإقليمية والعالمية.

ستقوم القوات المسلحة من خلال استراتيجيتها الدفاعية للأمن السيبراني بتطوير قدراتها السيبرانية.

[13] Cyberspace Domain of Operations Remains Top Priority for ACT, NATO website, https://www.act.nato.int/article/cyberspace-domain-of-operations-remains-top-priority-for-act/, December, 2022.

أولوية-3: تعزيز القدرات السيبرانية الوطنية بأيادي اردنية مؤهلة ومبدعة

الأهداف الفرعية (عددها 4 أهداف):

أولوية 3	تعزيز القدرات السيبرانية الوطنية بأيادي اردنية مؤهلة ومبدع	
الأهداف الفرعية	13	تطوير وبناء القدرات والمعارف والمهارات السيبرانية على المستوى الوطني
	14	الأردن بيت خبرة ومصدر للمواهب السيبرانية
	15	تعزيز النظام البيئي للأعمال في قطاع الأمن السيبراني
	16	تعزيز وتطوير بيئة البحث والتطوير

13. تطوير وبناء القدرات والمعارف والمهارات السيبرانية على المستوى الوطني

يواجه العالم والأردن كذلك نقصاً حاداً في الخبرات في مجال الامن السيبراني وهذا يعطل في كثير من الأحيان الجهود المبذولة لمواجهة التحديات والمخاطر السيبرانية كون العنصر البشري هو الحلقة الأهم في المنظومة الدفاعية، وبالرغم من اطلاق الجامعات الأردنية عدد لا بأس به من البرامج الاكاديمية (أكثر من 30 برنامج على مستوى البكالوريوس) في تخصص الامن السيبراني خلال السنوات القليلة الماضية، الا ان القطاع لا يزال يعاني من نقص في الخبرات، كون هذه البرامج الاكاديمية بحاجة الى تجويد مخرجاتها والتركيز أكثر على التعليم العملي والتطبيقي الذي يكفل منح الخريجيين المهارات التي يحتاجها السوق.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

13.1. تعزيز وتطوير منظومة المهارات والمهن السيبرانية

ستوفر الحكومة من خلال منظومة التعليم والتدريب المهني (VET) بتوفير التدريب المناسب لسوق العمل الاردني ومواكبة احتياجات المهارات في مجال الأمن السيبراني. كما ستقوم الحكومة بتطوير "الإطار الأردني للمهارات السيبرانية" الذي يهدف الى تحديد وتصنيف وظائف الامن السيبراني ووضع المعايير التي تحدد المهارات والقدرات اللازمة لأداء المهام الوظيفية، وسيؤدي ذلك إلى إنشاء مسارات واضحة لأدوار الأمن السيبراني، وتقليل الحواجز أمام الدخول للقطاع وبناء قدر أكبر من التناسق عبر القوى العاملة السيبرانية. كما سيوفر إطار المهارات السيبرانية لأصحاب العمل ضماناً بأن القوى العاملة السيبرانية تتمتع بالمهارات المناسبة، وسيمنح العمال الثقة في أن مؤهلاتهم وخبراتهم ذات الصلة معترف بها وملائمة للغرض.

13.2. الاستثمار في التدريب وتطوير رأس المال البشري

ستقوم الحكومة بالاستثمار في التدريب على أكثر من مستوى، مثل تدريب طلاب المدارس الجامعات، معسكرات تدريبية للخريجين، برامج تدريب للعاملين في قطاعات التكنولوجيا. كما ستقوم الحكومة بإنشاء **"الاكاديمية الوطنية للأمن السيبراني"** لتكون مركز تميز محلي واقليمي، تهدف إلى رفع مهارات المتخصصين في مجال الأمن السيبراني وتطوير المهارات التقنية وغير التقنية وتلبية حاجة السوق الأردني والأسواق المجاورة من الخبرات.

كذلك، ستعمل الحكومة تطوير وتنفيذ برامج تنمية القدرات والمهارات في مجال الأمن السيبراني للمهنيين والمسؤولين رفيعي المستوى في المؤسسات العامة، وللمهنيين الذين يقومون بحماية البنى التحتية الحيوية الوطنية ومشغلي الخدمات الأساسية، بالإضافة الى تطوير وتنفيذ برامج تنمية القدرات والمهارات في مجال الأمن السيبراني للعاملين في مجال إنفاذ القانون لتدريبهم على القضايا التي تتعلق بالتعامل مع الجرائم السيبرانية التي تتعرض لها المؤسسات والافراد على حد سواء.

14. الأردن بيت خبرة ومصدر للمواهب السيبرانية

نحتاج الى تنفيذ إصلاحات لدعم وتطوير نظام تعليم وتدريب أكثر فعالية يلبي احتياجات القوى العاملة في مجال الأمن الرقمي والسيبراني في الأردن وفي المنطقة وجعل الأردن مركز إقليمي للتميز السيبراني، وسنعمل لتحديد احتياجات القوى العاملة المستقبلية وتلبيتها، وسنشجع الشباب على الدراسة والعمل في مجال الامن السيبراني، كما سنعمل على ادخال مواد دراسية تتعلق بالأمن السيبراني في المناهج المدرسية للصفوف الابتدائية والثانوية.

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

14.1. تشجيع وتحفيز المواهب الوطنية

يشكل نقص المتخصصين عبئًا على المجتمع وعلى صناعة الأمن السيبراني، ولهذا من الضروري تطوير الخطط لاكتشاف ورعاية المواهب المتخصصة في مجال الأمن السيبراني ووضع البرامج لتطوير قدراتهم وتوفير البيئة لاستثمار مواهبهم ومهاراتهم في خدمة البلد والمجتمع. وقد تم خلال السنوات الماضية اطلاق عدد من المبادرات الوطنية التي استهدفت اكتشاف المواهب وتنميتها، مثل مسابقة "محارب السايبر" التي أطلق نسختها الاولى المركز الوطني للأمن السيبراني في عام 2022، وكذلك عدد من المبادرات التي تبنتها مجموعة من الجامعات الأردنية لنفس الغرض، وقد كان لهذه المبادرات دور مهم في تشجيع أصحاب المواهب للانخراط في هذا المجال مما وفر للدولة مجموعة لا بأس بها من الهاكرز الاخلاقيين الذين ساعدوا ولا يزالون في فحص الخدمات والمواقع الالكترونية الوطنية وكذلك من خلال مشاركتهم الفاعلة في برنامج صائدي الجوائز الوطني (Bugbounty.jo).

كذلك ستقوم الحكومة بتوفير منصة تدريب رقمية مجانية لتوفير تدريب عالي المستوى للمهتمين من أصحاب المواهب والمهارات في مواضيع الأمن السيبراني.

14.2. تجويد مخرجات التعليم الأكاديمي في مجال الامن السيبراني

ستقوم الحكومة بمراجعة أسس اعتماد برامج الامن السيبراني في الجامعات الأردنية بشكل يضمن تجويد هذه البرامج وتحقيقها لمعايير عالية تضاهي أفضل الجامعات في العالم، وبحيث تخلق شباب مؤهل يمتلك المهارات التي يحتاجها السوق وينافس على الوظائف على مستوى المنطقة. كما سيقوم المركز الوطني للأمن السيبراني بتطوير **إطار شهادات وطني** يستهدف برامج الامن السيبراني في الجامعات الأردنية، بالإضافة الى **إطار شهادات للمحترفين** في مختلف مهن ووظائف الامن السيبراني.

14.3. التركيز على المدارس

ستقوم الحكومة بإدماج مواد تتعلق بالأمن السيبراني بالمناهج الدراسية للصفوف الابتدائية والثانوية، كما ستقوم بإعداد برامج ونشاطات لا منهجية تركز على تطوير مهارات الطلاب الموهوبين ومنحهم بيئة تعليمية وتفاعلية.

15. تعزيز النظام البيئي للأعمال في قطاع الأمن السيبراني

يستجيب هذا الهدف للحاجة إلى المساهمة في تعزيز السيادة الوطنية فيما يتعلق بالاعتماد على منتجات وحلول الامن السيبراني الوطنية مع الأخذ في الاعتبار تعزيز الفرص الاقتصادية وفرص العمل وتعزيز الشركات في قطاع الأمن السيبراني في الاردن كمحور رئيسي لها، لذلك فان الحكومة ستعمل على مواصلة تحفيز إنشاء الأعمال والشركات الناشئة من خلال تشجيع صناعة الامن السيبراني وتعزيزها وتشجيع البحث والتطوير ودعم المواهب لتلبية الطلب الكبير على المهنيين في هذا القطاع، كما سنعمل على دعم انشاء مسرعات الاعمال والحواضن التي من

شأنها تشجيع ودعم الأفكار الإبداعية والريادية. وتعد صناعة الأمن السيبراني الوطنية ضرورة للتطور الطبيعي للاقتصاد الوطني في مستقبل يتسم بشكل متزايد بالرقمنة والتطورات التكنولوجية السريعة، لذلك لا بُد من تحفيز ودعم جهود القطاع الخاص والقطاع الأكاديمي لتطوير حاضنات الأعمال والشركات الجديدة الناشئة (Startups).

ستعمل الحكومة على تنفيذ هذا الهدف من خلال المبادرات التالية:

15.1. دعم وتشجيع صناعة الامن السيبراني الأردنية

ان تعزيز ودعم الابتكار في مجال الأمن السيبراني يعد أمراً حيوياً لتعزيز وتطوير صناعة الأمن السيبراني في الاردن ويتطلب تعاوناً بين القطاعات الوطنية، ولذلك سنقوم بدعم المبادرات والمشاريع الريادية من خلال إنشاء حاضنة أعمال الامن السيبراني كمبادرة مشتركة مع القطاع الخاص والقطاع الأكاديمي، كذلك ستقوم الحكومة بدعم الشركات الناشئة والشركات الصغيرة والمتوسطة بهدف تجويد منتجاتها وتعزيز قدرتها على المنافسة على الصعيدين الوطني والدولي وتقديم التسهيلات الإجرائية ودعم ترويجها وانتشارها وتوسعها في الخارج.

ستعمل الحكومة على **إنشاء صندوق لدعم الأفكار الريادية والشركات الناشئة** وإطلاق **مسابقة للأمن السيبراني** تهدف الى تحفيز الشركات الناشئة وتشجيعها وخلق بيئة تنافسية داعمة من شأنها ان تسهم في تطوير صناعة الامن السيبراني الأردنية وتعزيز دورها في الاقتصاد الوطني.

هذا بالإضافة الى أن كل من "نظام ترخيص خدمات الأمن السيبراني" و "الإطار الوطني لاعتماد المنتجات والخدمات الرقمية" سيسهمان بشكل إيجابي في تطوير منتجات وخدمات سيبرانية وطنية قادرة على ولوج الأسواق الخارجية بسبب تطبيقها والتزامها بالمعايير والضوابط المحلية والدولية.

إن جذب الاستثمار الأجنبي في مجال الأمن السيبراني بالإضافة إلى تقديم الحوافز للشركات الصغيرة والمتوسطة المحلية سيساهم في بناء صناعة الأمن السيبراني، لذلك ستعمل الحكومة على تشجيع استقطاب الشركات الكبرى وتأسيس وجود لها في الأردن للاستفادة من رأس المال البشري والمواهب والخبرات والمهارات التي يتمتع بها الشباب الأردني، وهذا سيساعد هذه الشركات في تقديم خدماتها بشكل أفضل في المنطقة وخاصة في منطقة الخليج العربي.

16. تعزيز وتطوير بيئة البحث التطوير

يساهم البحث والتطوير بشكل كبير في تحسين المستوى العام للأمن السيبراني لدينا، وبالتالي يلعبان أيضاً دوراً مهماً في المساعدة على تحديد أحدث الاتجاهات والتقنيات، وتطوير حلول الأمن السيبراني.

16.1. دعم وتشجيع البحث العلمي والتطوير

ان خلق بيئة متطورة للبحث والتطوير لدى القطاعين العام والخاص موضوع أساسي ومهم في إيجاد ودعم صناعة الامن السيبراني الأردنية، ولهذا ستعمل الحكومة على دعم نمو قطاع الأمن السيبراني من خلال تدابير تعكس التزامنا بدعم البحث والتطوير، بما في ذلك من خلال مراكز البحوث في الجامعات الأردنية وفي القطاع الخاص، كما ستدعم الحكومة الخيارات المتاحة لمزيد من الجهود البحثية لدفع الابتكار بدءاً من الأبحاث الأساسية وحتى تقديم منتجات محددة إلى السوق.

ستعمل الحكومة على تشجيع الفرق البحثية والمشاريع البحثية في مجال الأمن السيبراني وفقاً للحاجات الوطنية ذات الأهمية الاستراتيجية للملكة من حيث البحث والتطبيق العملي وتمكين الأردن استراتيجيًا من امتلاك قدرات البحث والتطوير والإنتاج والتحقق والتقييم وتقييم الخبراء في مجال الامن السيبراني، تحسين التواصل بين القطاعات الأكاديمية والاقتصادية والعامة وتبادل المعلومات المتعلقة بأمن المعلومات.

أولوية-4: تشجيع الشراكات الاستراتيجية المحلية وتعزيز دور الأردن على المستويين الإقليمي والدولي

الأهداف الفرعية (عددها 2 أهداف):

أولوية 4	تشجيع الشراكات الاستراتيجية المحلية وتعزيز دور الأردن على المستويين الإقليمي والدولي
الأهداف الفرعية	17 تعزيز الدور الأردني والمشاركة في المبادرات الاقليمية والدولية
	18 تعزيز الالتزام والتعاون والتنسيق محلياً، ما بين أصحاب المصلحة

17. تعزيز الدور الأردني والمشاركة في المبادرات الاقليمية والدولية

إن النظرة الإيجابية عن الأردن كدولة معتدلة تحترم المواثيق والمعاهدات الدولية وتسعى للسلم العالمي يمكن ترسيخها من خلال عنايتها واهتمامها بأمن فضاءها السيبراني الوطني وعدم استخدامه في الاعمال العدائية والتزامها بالسلوك المسؤول في استخدام التكنولوجيا وعدم الاضرار بالآخرين. كما أن الثقة بأمن الفضاء السيبراني الأردني والمحافظة علية كبيئة تفاعلية رقمية آمنه، تشجع المستثمرين والشركات الكبرى على الاستثمار في الأردن وتساعد على استقطاب الكفاءات ورؤوس الأموال. لهذا فأنه من المفيد المشاركة بفاعلية وحضور قوي في المحافل الدولية والعمل عن قرب مع كافة الشركاء المحليين والاقليميين والدوليين.

17.1. المشاركة الإيجابية الفاعلة في المحافل الدولية

ستعمل الحكومة من خلال مشاركتها وتفاعلها الإيجابي مع النقاشات الإقليمية والدولية على عكس صورة إيجابية عن المنظومة السيبرانية الأردنية والجهود الأردنية في الحفاظ على الفضاء السيبراني العالمي بعيداً عن النزاعات الإقليمية والدولية، كما ستشارك الحكومة في المنتديات والتجمعات الدولية الداعمة للأمن والسلم السيبراني وستطرح وجهة نظرها في مختلف القضايا المطروحة، سواء على مستوى الأمم المتحدة فيما يتعلق باجتماعات مجموعة العمل مفتوحة العضوية لأمن واستخدام الاتصالات وتكنولوجيا المعلومات، و الاجتماعات المتعلقة بالاتفاقية الدولية لمكافحة الجريمة السيبرانية، او المحافل الأخرى على المستويات الإقليمية، مثل جامعة الدول العربية ومنظمة الدول الإسلامية.

ستبذل الحكومة قصارى جهدها لتعزيز المشاركة الفعالة في جميع أنشطة الأمن السيبراني الدولية ذات الصلة، كما ستستضيف **قمة الأردن السنوية للأمن السيبراني** (DotCyber Summit)، كما ستعمل الحكومة على استضافة النشاطات والتمارين السيبرانية والاجتماعات الدولية والإقليمية

17.2. تعزيز مشاركة فرق الاستجابة الأردنية في النشاطات الإقليمية والدولية

تشارك الحكومة الأردنية من خلال فرق الاستجابة الوطنية في النشاطات الإقليمية لمنظمة الاتصالات الدولية (ITU) وهي عضو في المركز العربي الإقليمي للأمن السيبراني، وكذلك عضو في تحالف فرق الاستجابة التابع لمنظمة دول العالم الإسلامي (OIC-CERT)، بالإضافة لعضويته في كل من منظمة (FIRST) ومنظمة (Trusted Introducer).

ستستمر الحكومة في هذا النهج وستعمل على توسيع دائرة مشاركتها في النشاطات الإقليمية والدولية المختصة بفرق الاستجابة وستستضيف اجتماعات كل من المركز العربي الإقليمي للأمن السيبراني واجتماعات الفرق التي تتبع لمنظمة دول العالم الإسلامي خلال السنوات القادمة.

17.3. التعاون في مجال مكافحة الجريمة السيبرانية

ستعمل الحكومة على تطوير التعاون مع مؤسسات انفاذ القانون الدولية، مثل المنظمة الدولية للشرطة الجنائية (الانتربول) والمكتب العربي للشرطة الجنائية، في مجالات التحقيق والملاحقة القضائية للجرائم السيبرانية، والانخراط في عمليات مشتركة وتعاونية لتفكيك شبكات الجرائم السيبرانية الإقليمية والدولية وحماية ضحاياها، كما ستعمل على تطوير قدرات ومهارات العاملين في مؤسسات انفاذ القانون لدينا.

سيمكننا التعاون مع الجهات الدولية في تمكين جهات انفاذ القانون الاردنية من الرد بسرعة على الجرائم السيبرانية العابرة للحدود، وخاصة تلك التي تؤثر على الأردن، وهذا من شأنه أن يعزز مكافحة الجريمة السيبرانية الدولية ويحسن الخيارات المتاحة لإنفاذ القانون.

17.4. دعم المبادرات الدولية الداعية للعمل من أجل السلوك المسؤول للدول في الفضاء السيبراني

تساهم هذه المبادرات في الحد من المخاطر التي تهدد السلم والأمن الدوليين وفي منع نشوب الصراعات، لذلك ستعمل الحكومة على تعزيز مشاركتنا في النقاشات الدولية الهادفة الى سلوك الدولة المسؤول في الفضاء السيبراني، والحكومة من خلال وزارة الخارجية وشؤون المغتربين على اطلاع دائم بالمناقشات الدولية بهذا الخصوص، بما في ذلك تنفيذ المعايير السيبرانية فضلاً عن تعزيز الثقة السيبرانية وبناء القدرات.

17.5. تعزيز وتطوير العلاقات التعاونية والتشاركية على المستوى الثنائي والمتعدد الاطراف

تلعب الشراكات والعلاقات الثنائية والمتعددة الأطراف دوراً مهماً في تعزيز الثقة وتبادل الخبرات والمعلومات والتنسيق القريب في مكافحة الجرائم السيبرانية العابرة للحدود، ولهذا السبب فقد وقعت الحكومة الأردنية عدداً من الاتفاقيات الثنائية مع عدد من الدول خلال الفترة الماضية، وستستمر الحكومة في تعزيز العلاقات والشراكات الثنائية مع بقية الدول التي تشاركنا نفس المبادئ والقيم ونلتقي معها في ضرورة المحافظة على أمن وسلامة الفضاء السيبراني العالمي، وهدفنا هو تعزيز التعاون الثنائي والمتعدد الأطراف بحيث يمكن استغلال الإمكانات الكاملة للتكنولوجيا الرقمية والحد من نقاط الضعف في دولنا، والدفع باتجاه أن يكون الأمن السيبراني جزءاً لا يتجزأ من البرامج الداعمة للأمن والسلم بيننا وبين هذه الدول.

18. تعزيز الالتزام والتعاون والتنسيق محلياً ما بين أصحاب المصلحة

تلعب كل جهة من أصحاب المصلحة دوراً مهماً وحيوياً في منظومة الامن السيبراني الوطنية، وتتحمل كل جهة مسؤوليات واضحة حددتها القوانين والأنظمة والتعليمات والقرارات الصادرة بهذا الخصوص، الا ان ذلك لا يمنع من الناحية التنفيذية ان تكون هنالك جهة مركزية، هي المركز الوطني للأمن السيبراني كجهة تنفيذية منسقة وموحدة وجامعة لكافة الجهود الوطنية تحت مظلة المجلس الوطني للأمن السيبراني بصفته مجلساً ممثلاً للقطاعات الحكومية والخاصة والأكاديمية الوطنية. ولتحقيق ذلك ستقوم الحكومة بتشجيع التعاون والشراكة ما بين القطاعات المختلفة ودعم بناء وتنفيذ مبادرات مشتركة وستحرص على التشاور بشكل مستمر مع القطاع الخاص والقطاعات المتأثرة عند أي إقرار أو أي تشريعات تتعلق بالأمن السيبراني.

18.1. تشجيع الشراكات والمبادرات القطاعية

ستشجع الحكومة قيام شراكات تجمع مؤسسات اكاديمية وخاصة وحكومية بهدف تعظيم أعمالهم في محاربة التهديدات السيبرانية التي تستهدف الفضاء الرقمي الأردني، وذلك من خلال تبادل الخبرات والمعرفة، وتبني المبادرات المشتركة بين أكثر من قطاع، ورفع درجة الوعي،

واقتراح السياسات والتشريعات. كما ستعمل الحكومة على تعزيز تحالفات القطاع العام مع القطاع الخاص ومنظمات المجتمع المدني والأوساط الأكاديمية، وإنشاء آليات تعاون محددة مع مشغلي البنية التحتية الحيوية الوطنية ومشغلي الخدمات الأساسية.

18.2. مبادرة الشراكة ما بين القطاعين العام والخاص لتعزيز الامن السيبراني الأردني

تم تصميم هذه المبادرة لتكون شاملة تجمع نقاط القوة في كلا القطاعين. ومن خلال الجمع بين سرعة الحركة والابتكار والبراعة التكنولوجية للقطاع الخاص والرقابة الاستراتيجية والسلطة التنظيمية للقطاع العام، يستطيع الأردن صياغة دفاع قوي ضد التهديدات السيبرانية، وهذه المبادرة تهدف لأن تكون الجسر الذي يسهل هذا التعاون المهم.

هنالك جوانب متعددة لأهمية هذه المبادرة. أولاً، هي تضمن أن تظل البنية التحتية الحرجة السيبرانية الوطنية قادرة على الصمود في مواجهة التهديدات الحالية والناشئة. ومن خلال معلومات التهديدات المشتركة والبحث والتطوير التعاوني، سنصبح في وضع أفضل لتوقع التهديدات السيبرانية والاستجابة بسرعة. ثانيًا، من خلال دمج حملات التدريب والتوعية، فإننا نعمل على تنمية ثقافة الوعي بالأمن السيبراني، مما يضمن أن يصبح كل فرد، بغض النظر عن دوره، خط دفاع بذاته. وأخيرًا، من خلال المراقبة والتقييم الدوري، فإننا نضمن أن تظل استراتيجياتنا ملائمة وفعالة وتتكيف في بشكل وقتي مع المشهد السيبراني المتطور.

الخطة التنفيذية

أولوية-1: الأمن والثقة			
	المبادرات	البرامج	الجهة المسؤولة
1. تعزيز الثقة بأمن البيئة الرقمية الأردنية وتقديم خدمات رقمية آمنة			
A	**توفير بيئة انترنت أمنة للمجتمع الأردني من خلال مزودي خدمات الانترنت**	دفع شركات الاتصالات ومزودي خدمات الانترنت لتوفير خدمات انترنت آمنة ومحمية واستخدام تقنيات متطورة لحجب التهديدات السيبرانية عن المستخدمين ومنع وصولها إليهم	TBD
		برنامج لمسح نطاقات عناوين الانترنت الوطنية بهدف كشف اية ثغرات فيها وتنبيه أصحابها الى هذه الثغرات لمعالجتها وتحسين مستويات الأمن فيها	TBD
		برنامج يُعنى بحماية المستخدمين من الهجمات المرتبطة بنظام اسم المجال	TBD
B	**التأكد من تقديم خدمات الكترونية آمنة وموثوق بها**	فحص الخدمات الالكترونية الحكومية المقدمة للمواطنين والتأكد من سلامتها من أية ثغرات وإلزام القطاع الخاص على فحص خدماته الرقمية.	TBD
		تشجيع استخدام البنية التحتية للمفتاح العام (PKI) للمعاملات من/إلى الوزارات والدوائر الحكومية لتعزيز مستويات الأمن السيبراني العالية والثقة في تقديم الخدمات العامة	TBD
		سيقوم البنك المركزي بالرقابة على الجهات التي تقدم وتدير قنوات الدفع الالكتروني وتتأكد من اتباعها للمعايير والضوابط الصادرة عن الحكومة او اية جهات رقابية او تنظيمية أُخرى	TBD
C	**تعزيز قدرات مكافحة الجريمة السيبرانية لجهات انفاذ القانون**	بناء القدرات والخبرات المناسبة لدى جميع الجهات الوطنية المعنية بمكافحة الجريمة السيبرانية بحيث يمكن تحقيق قدرات المكافحة والتحقيق المتوقعة من كل جهة بشكل فعال وسريع	TBD
2. مساعدة الشركات الصغيرة والمتوسطة في مواجهة التهديدات السيبرانية			
A	**توفير منصة لدعم الشركات الصغيرة والمتوسطة**	أنشاء منصة لتقديم النصح والإرشاد والمساندة للمؤسسات الصغيرة والمتوسطة، وتوفير أدوات وحلول تقنية مفتوحة المصدر لمساعدة هذه المؤسسات في مراقبة وكشف التهديدات والاختراقات.	TBD
		توفير المواد التوعوية والمصادر التعليمية والنصائح والارشادات والتحذيرات الموجهة لقطاع الاعمال	TBD

		لتمكينه من مواجهة التهديدات والمخاطر، وكذلك إعداد "دليل الأمن السيبراني".	
		تشجيع ومساعدة الشركات الصغرى والمتوسطة على تطبيق الإطار الوطني الأردني للأمن السيبراني (JNCSF)	TBD
B	**إطلاق برنامج الدفاع السيبراني الفعّال**	توفير مجموعة من الخدمات المجانية لقطاع الاعمال والمؤسسات ليساعدها على معرفة مدى مرونتها في مواجهة الهجمات السيبرانية وقدرتها على الاستجابة للحوادث الأمنية	TBD
3. ادارة المخاطر المتأتية من استخدام المنتجات الرقمية وسلاسل التوريد			
A	**تطوير معايير أمن سيبراني للتقنيات الناشئة وسلاسل التوريد**	إعداد ضوابط ومعايير أمنية سيبرانية لإنترنت الأشياء (IoT)، كذلك اعداد ضوابط ومعايير أمنية سيبرانية لتقنيات الذكاء الاصطناعي	TBD
		ضمان حوكمة وتنظيم سلاسل التزويد لقطاعات البنية التحتية الحرجة	TBD
B	**تنفيذ برنامج للاعتماد وإصدار الشهادات في مجال الامن السيبراني**	تطوير وإنشاء **"المركز الاردني للكفاءات وشهادات الامن السيبراني"** (Jordan Cybersecurity Competence and Certification Center	TBD
		بناء الإطار الوطني الاردني لاعتماد المنتجات والخدمات الرقمية (Jordan Cybersecurity Certification Scheme)	TBD
		إنشاء مختبر لفحص وتقييم المنتجات الرقمية	TBD
C	**تشجيع الشركات على تطوير حلول رقمية آمنة**	دعم وتشجيع الشركات على تطبيق معايير التطوير الآمن للحلول الرقمية، وتشجيع الابتكار والقدرة التنافسية في صناعة البرمجيات من خلال دعم اعتماد تقنيات آمنة وقابلة للتشغيل البيني	TBD
4. تحقيق التنوع والشمول السيبراني للفئات الأضعف في المجتمع			
A	**تمكين المرأة في السايبر**	تنفيذ برنامج يهدف الى تمكين المرأة في قطاع السايبر، من ناحية تشجيعها على الدخول فيه وتوفير التدريب والتوجيه والإرشاد المناسب ودعم إيصال عدد من النساء الى مواقع قيادية وإشرافية	TBD
B	**دعم القدرة على الوصول لخدمات الامن السيبراني للفئات الأضعف في المجتمع**	تخصيص برامج للتوعية والتدريب للفئات المجتمعية الأضعف، والحرص على قدرة هذه الفئات على الاستفادة من جميع البرامج والخدمات السيبرانية التي تقدمها الحكومة	TBD
		ضمان استخدام الفئات الضعيفة للفضاء الرقمي بطريقة آمنة ومسؤولة، ونشر تدابير تضمن أن تكون هذه الفئات، وخاصة الأطفال، وأولياء أمورهم، على علم بالتهديدات	TBD

		تسهيل قدرة الافراد على ابلاغ وحدة الجرائم الالكترونية عن الحوادث والجرائم السيبرانية التي يتعرضون لها	TBD

أولوية-2: المرونة والصمود			
	المبادرات	البرامج	الجهة المسؤولة
5. تطوير الأطر التشريعية الناظمة للفضاء السيبراني الأردني، وموائمتها مع التطورات التكنولوجيا الحديثة			
A	**مراجعة القوانين والأنظمة والتعليمات ذلا العلاقة بالأمن السيبراني**	تحديد التشريعات المتعلقة بمنظومة الأمن السيبراني او تلك التي ترتبط بها او تؤثر علياه وعمل مراجعة شاملة لها والتأكد من تلبيتها للمتطلبات الأمنية الوطنية ومواكبتها للتطورات العلمية والتقنية المتسارعة	TBD
6. توفير متطلبات المرونة السيبرانية لمشغلي البنية التحتية الحرجة والخدمات الوطنية الأساسية			
A	**تطبيق الإطار الوطني الأردني للأمن السيبراني على الحكومة وقطاعات البنية التحتية الحرجة**	البدء في تطبيق الإطار على المؤسسات الحكومية ومشغلي قطاعات البنية التحتية الحرجة	TBD
		تنفيذ برنامج لمساعدة المؤسسات الحكومية ومشغلي البُنى التحتية الحرجة على فهم وتطبيق الإطار الأردني	TBD
B	**تعزيز وتطوير المنظومة الوطنية للتدقيق ومراقبة الالتزام**	التأكد من فهم الجهات المُلزمة لالتزاماتهم بموجب الإطار الوطني الأردني للأمن السيبراني (JNCSF)، بما في ذلك الالتزام بتطوير برنامج إدارة مخاطر البنية التحتية الحرجة وادامته والامتثال له.	TBD
		إطلاق جائزة التميز في الأمن السيبراني للمؤسسات والافراد	TBD
C	**تطوير إطار عمل وضوابط خاصة بقطاعات البُنية التحتية الحرجة**	تطوير إطار عمل وضوابط سيبرانية لمشغلي البنية التحتية الحرجة	TBD
		تطوير وتنفيذ برنامج لتقييم البُنى التحتية الحرجة ووضع "خطة حماية" لكل قطاع من هذه القطاعات	TBD
D	**تطوير قدرات المراقبة وفرق الاستجابة القطاعية**	تشجيع ودعم إنشاء فرق استجابة قطاعية ترتبط أفقياً مع بعضها البعض وعامودياً مع فريق الاستجابة الوطني	TBD
		تشجيع ودعن بناء مراكز عمليات أمنية (Security Operation Centers) قطاعية ترتبط جميعها بمركز عمليات وطني بشكل هرمي يهدف الى تسهيل وتعزيز إجراءات الاستجابة وتبادل المعلومات بشكل انسيابي وسريع	TBD
7. تعزيز صمود ومناعة الشبكات الرقمية الحكومية			
A	**وجود رؤية وفهم وسيطرة على الأصول الرقمية الحكومية**	التأكد أن لدى جميع المؤسسات الحكومية طريقة نشطة ومؤتمتة لاكتشاف الأصول وإدارتها لتحديد الأنظمة والأجهزة والبرامج التي يمتلكونها ويعملون عليها بشكل مستمر	TBD

أولوية-2: المرونة والصمود			
	المبادرات	البرامج	الجهة المسؤولة
B	**وجود رؤية شاملة للبيانات التي تتعامل معها الحكومة وتشاركها مع الآخرين**	تحديد رؤية شاملة لأصول البيانات الخاصة بالحكومة، من البيانات الشخصية إلى المعلومات السرية، وحمايتها بما يتناسب مع المخاطر وبما يتوافق مع تشريعات حماية البيانات	TBD
C	**إدارة المخاطر الناجمة عن الموردين التجاريين على الحكومة**	اتخاذ خطوات لدراسة وفهم درجة اعتماد المؤسسات الحكومية على الموردين وعلى سلاسل التوريد بشكل أفضل والتأكد من دمج منتجاتهم وخدماتهم في الأنظمة الحكومية بطريقة تأخذ في الاعتبار تأثيراتها على الأمن الوطني والقدرة على الصمود	TBD
D	**التأكد أن التقنيات الحكومية مهيئة بشكل صحيح**	تطوير تكوينات الأمان الأساسية (Baseline Security Configuration) لجميع الأنظمة والأصول الرقمية الحكومية حتى تتمكن المؤسسات من اعتمادها وتطبيقها لديها بشكل متجانس على مستوى الحكومة	TBD
E	**تصنيف البيانات الحكومية والتعامل معها بشكل مناسب**	تحديث سياسة تصنيف البيانات المعمول بها حالياً، لتحسين التعامل مع المعلومات في المستوى الرسمي والتأكد من أن المعلومات الأكثر حساسية الموجودة في هذا المستوى محمية بشكل مناسب ومستمر	TBD
F	**مراقبة الشبكات والأنظمة والتطبيقات والأجهزة الطرفية الحكومية لكشف التهديدات**	تطوير مركز المراقبة الحكومة (GovSOC) وتطوير عمليات الحكومة السيبرانية وتحديثها وكذلك تطوير العاملين فيها وتطبيق أفضل الممارسات العالمية لضمان الكشف المبكر عن التهديدات	TBD
G	**تطوير قدرات الاستجابة لدى الحكومة**	تطوير قدرات فرق الاستجابة الحكومية والتأكد من امتلاكها الأدوات والخبرات اللازمة للتعامل مع الحوادث المعقدة والتحقيق فيها وكشف الجهات المهاجمة ومعرفة تبعيتها	TBD
H	**الاستثمار في تعزيز قدرات الامن السيبراني في الوزارات والدوائر الحكومية**	تنفيذ برنامج "تعزيز قدرات الامن السيبراني في الوزارات والدوائر الحكومية" بهدف تعزيز مناعة كل من الشبكة الحكومية الآمنة وشبكات الوزارات والدوائر الحكومية	TBD
I	**رفع المهارات السيبرانية للعاملين في دوائر تكنولوجيا المعلومات**	تنفيذ برنامج تدريبي لكافة العاملين في أمن المعلومات والامن السيبراني في الوزارات والدوائر الحكومية	TBD
J	**إنشاء شبكة اتصالات معلوماتية حكومية مشفرة وآمنة**	ضمان سرية شبكات المعلومات الحكومية من خلال اعتماد منظومة تشفير تعتمد على تقنيات متطورة قادرة على مواجهة تحديات عصر ما بعد الحوسبة الكمية (Quantum Computing)	TBD

أولوية-2:
المرونة والصمود

	المبادرات	البرامج	الجهة المسؤولة
8. التوعية وتسهيل الوصول للمعلومات والمصادر			
A	**التوعية بالمخاطر المتأتية من الفضاء السيبراني**	تنفيذ حملات وطنية تشاركية بين مختلف المؤسسات الحكومية والخاصة للتوعية بمخاطر الانترنت والفضاء السيبراني	TBD
		دعم وإثراء منصة (Safeonline.jo) وتوسيع الشرائح التي تغطيها وتنويع محتواها والترويج لها للوصول الى عدد أكبر من المتلقين	TBD
B	**تسهيل الوصول للمعلومات والتحذيرات**	تزويد الجهات الوطنية بالتحذيرات الأمنية حول التهديدات وكذلك المعلومات المتعلقة بالثغرات الأمنية التي يتم نشرها من قبل الجهات والشركات الصانعة والمنصات الدولية المتخصصة	TBD
		انشاء نظام انذار مبكر (Early Warning System) لإخطار القطاعات الحيوية ومؤسسات البنى التحتية الحرجة بشكل سريع وفوري	TBD
9. الاستجابة لحوادث الامن السيبراني التي تهدد الأمن الوطني			
A	**خطة الطوارئ للاستجابة لحوادث الأمن السيبراني**	تطوير خطة طوارئ وطنية للاستجابة لحوادث الامن السيبراني الخطرة وشديدة الخطورة التي يكون لها بُعد أمني او اقتصادي او تؤثر على قدرة المواطنين على الوصول للخدمات الأساسية في الدولة	TBD
B	**تمارين سيبرانية لفحص صمود البنية التحتية الحرجة**	تنفيذ برنامج للتمارين السيبرانية يغطي كافة القطاعات ويكون بشكل دوري	TBD
10. حماية وتامين المعلومات الاكثر حساسية للدولة والمجتمع			
A	**حفظ البيانات الوطنية الحساسة**	انشاء مركز حفظ البيانات الوطني (National Data Vault)	TBD
		مراجعة سياسات حفظ المعلومات الحكومية	TBD
B	**ضوابط أمنية لخدمات الاستضافة**	تحديث وتطوير الضوابط والمعايير الأمنية التي تنظم عملية استضافة المعلومات الحكومية	TBD
		إصدار تعليمات ترخيص لخدمات الامن السيبراني السحابية	TBD
11. إدارة استخباراتية فعالة ومنظومة وطنية لمشاركة المعلومات			
A		توسيع المشاركة في منصة "شارك" لتبادل المعلومات بين الجهات الوطنية	TBD

أولوية-2: المرونة والصمود			
	المبادرات	البرامج	الجهة المسؤولة
	تعزيز وتأطير الجهود الوطنية لتبادل المعلومات	وضع سياسات لتأطير تبادل المعلومات بين المؤسسات في القطاعين العام والخاص وتشجيع تبادل المعلومات على المستوى القطاعي	TBD
12. تعزيز القدرات السيبرانية لمؤسسات الدفاع الوطنية			
A	**تطوير استراتيجية القوات المسلحة للأمن السيبراني**	وضع استراتيجية دفاعية للأمن السيبراني، تحدد من خلالها الأولويات الدفاعية السيبرانية ضمن المتغيرات والمعادلات الإقليمية الجيوسياسية والتهديدات الإقليمية والعالمية	TBD
		تطوير القدرات السيبرانية الدفاعية للقوات المسلحة الاردنية	TBD

أولوية-3:
بناء القدرات

	المبادرات	البرامج	الجهة المسؤولة
13. تطوير وبناء القدرات والمعارف والمهارات السيبرانية على المستوى الوطني			
A	**تعزيز وتطوير منظومة المهارات والمهن السيبرانية**	تطوير "الإطار الأردني للمهارات السيبرانية" لتحديد وتصنيف وظائف الامن السيبراني ووضع المعايير التي تحدد المهارات والقدرات اللازمة لأداء المهام الوظيفية	TBD
B	**الاستثمار في التدريب وتطوير رأس المال البشري**	تطوير وتنفيذ برامج تنمية القدرات والمهارات في مجال الأمن السيبراني للمهنيين وموظفي الحكومة والمسؤولين رفيعي المستوى في المؤسسات العامة، وللمهنيين الذين يقومون بحماية البنى التحتية الحيوية الوطنية وكذلك للعاملين في مجال إنفاذ القانون	TBD
		تنفيذ برامج تدريبية لخريجي الجامعات (Upskilling) وطلاب الجامعات والمدارس	TBD
		إنشاء "الاكاديمية الوطنية لأمن السيبراني"	TBD
14. مبادرات لجعل الأردن بيت خبرة ومصدر للمواهب السيبرانية			
A	**تشجيع وتحفيز المواهب الوطنية**	تنفيذ ودعم مسابقات الامن السيبراني مثل مسابقة "محاربو السايبر" التي أطلقها المركز الوطني للأمن السيبراني، ومنصة صائدو الجوائز (bugbounty.jo)	TBD
		دعم وتشجيع المواهب الوطنية من خلال توفير منصات تدريب رقمية مجانية تستهدف أصحاب والمواهب والمهارات	TBD
B	**تجويد مخرجات التعليم الأكاديمي في مجال الامن السيبراني**	مراجعة أسس اعتماد برامج الامن السيبراني في الجامعات الأردنية بشكل يضمن تجويد هذه البرامج وتحقيقها لمعايير عالية تضاهي أفضل الجامعات في العالم	TBD
		تطوير إطار شهادات وطني يستهدف برامج الامن السيبراني في الجامعات الأردنية، بالإضافة الى إطار شهادات للمحترفين في مختلف مهن ووظائف الامن السيبراني	TBD
C	**التركيز على المدارس**	إدماج مواد تتعلق بالأمن السيبراني بالمناهج الدراسية للصفوف الابتدائية والثانوية	TBD
15. تعزيز النظام البيئي للأعمال في قطاع الأمن السيبراني			
A	**دعم وتشجيع صناعة الامن السيبراني الأردنية**	دعم المبادرات والمشاريع الريادية من خلال إنشاء حاضنة أعمال الامن السيبراني كمبادرة مشتركة مع القطاع الخاص والقطاع الأكاديمي	TBD

أولوية-3: بناء القدرات			
	المبادرات	البرامج	الجهة المسؤولة
		إنشاء صندوق لدعم الأفكار الريادية والشركات الناشئة من وإطلاق مسابقة للأمن السيبراني لاختيار الأفكار التي سيتم دعمها وذلك بهدف تحفيز الشركات الناشئة وتشجيعها وخلق بيئة تنافسية داعمة	TBD
		تشجيع استقطاب الشركات الكبرى العاملة في مجال الأمن السيبراني وتأسيس وجود لها في الأردن	TBD
16. دعم وتشجيع البحث التطوير			
A	**تشجيع الفرق البحثية وتمكين الأردن من تطوير قدراته في البحث والتطوير والانتاج**	تشجيع الفرق البحثية والمشاريع البحثية في مجال الأمن السيبراني وتمكين الأردن استراتيجيًا من امتلاك قدرات البحث والتطوير والإنتاج والتحقق والتقييم وتقييم الخبراء في مجال الامن السيبراني	TBD

أولوية-4:

التعاون والشراكات

	المبادرات	البرامج	الجهة المسؤولة
17. تعزيز الدور الأردني والمشاركة في المبادرات الاقليمية والدولية			
A	**المشاركة الإيجابية الفاعلة في المحافل الدولية**	ستشارك الحكومة في المنتديات والتجمعات الدولية الداعمة للأمن والسلم السيبراني وستطرح وجهة نظرها في مختلف القضايا المطروحة	TBD
		استضافة **قمة الأردن السنوية للأمن السيبراني** (DotCyber Summit)، واستضافة النشاطات والتمارين السيبرانية والاجتماعات الدولية والإقليمية	TBD
B	**تعزيز مشاركة فرق الاستجابة الأردنية في النشاطات الإقليمية والدولية**	توسيع دائرة مشاركة فرق الاستجابة الاردنية في النشاطات الإقليمية والدولية واستضافة اجتماعات كل من المركز العربي الإقليمي للأمن السيبراني واجتماعات الفرق التي تتبع لمنظمة دول العالم الإسلامي واية اجتماعات دولية ذات علاقة	TBD
C	**التعاون في مجال مكافحة الجريمة السيبرانية**	تطوير التعاون مع مؤسسات انفاذ القانون الدولية، مثل المنظمة الدولية للشرطة الجنائية (الانتربول) والمكتب العربي للشرطة الجنائية، في مجالات التحقيق والملاحقة القضائية للجرائم السيبرانية، والانخراط في عمليات مشتركة وتعاونية لتفكيك شبكات الجرائم السيبرانية الإقليمية والدولية وحماية ضحاياها	TBD
D	**تعزيز وتطوير العلاقات التعاونية والتشاركية على المستوى الثنائي والمتعدد الأطراف**	الاستمرار في تعزيز العلاقات والشراكات الثنائية والمتعددة الأطراف مع الدول التي تشاركنا نفس المبادئ والقيم ونلتقي معها في ضرورة المحافظة على أمن وسلامة الفضاء السيبراني العالمي	TBD
E	**دعم المبادرات الدولية الداعية للعمل من أجل السلوك المسؤول للدول في الفضاء السيبراني**	تعزيز مشاركتنا في النقاشات الدولية الهادفة الى سلوك الدولة المسؤول في الفضاء السيبراني، والبقاء على اطلاع دائم بالمناقشات الدولية بهذا الخصوص	TBD
18. تعزيز الالتزام والتعاون والتنسيق محلياً ما بين أصحاب المصلحة			
A	**تشجيع الشراكات والمبادرات القطاعية**	تشجيع التعاون والشراكة ما بين القطاعات المختلفة ودعم بناء وتنفيذ مبادرات مشتركة والتشاور بشكل مستمر مع القطاع الخاص	TBD

	المبادرات	البرامج	الجهة المسؤولة
أولوية-4: التعاون والشراكات			
		والقطاعات المتأثرة عند أي إقرار أو أي تشريعات تتعلق بالأمن السيبراني	
B	**مبادرة الشراكة ما بين القطاعين العام والخاص لتعزيز الامن السيبراني الأردني**	تصميم وتنفيذ شراكة بين القطاعين العام والخاص لتكون شاملة تجمع نقاط القوة في كلا القطاعين، من خلال الجمع بين سرعة الحركة والابتكار والبراعة التكنولوجية للقطاع الخاص والرقابة الاستراتيجية والسلطة التنظيمية للقطاع العام	TBD