المركز الوطني للأمن السيبراني
National Cyber Security Center

# الاستراتيجية الوطنية للأمن السيبراني

# National Cyber Sceurity Strategy

## 2028 - 2025

المركز الوطني للأمن السيبراني
عمّان - الدوار السابع +(962) 6 900 500 +(962) 65 300 265 Info@ncsc.jo

# Contents

## المقدمة

تواجه المملكة الأردنية الهاشمية شأنها شأن باقي الدول تهديدات سيبرانية وبشكل متزايد الامر الذي يجعل مواجهتها والحد من تأثيرها هدفا وطنيا تتكاثف كافة جهود المؤسسات الوطنية لتحقيقه. وقد أظهرت الأرقام الصادرة عن المركز الوطني للأمن السيبراني أن الهجمات السيبرانية المكتشفة في عام 2024 كانت أعلى من عام 2023 وذلك نتيجة للتوسع في خدمات المركز وربط عدد من الشبكات الحكومية على أنظمة المركز. وكانت هذه التهديدات اما من جماعات الجريمة السيبرانية المنظمة (Organized Cybercrime)

أو من جماعات التهديد المتطورة (Advance Persistent Threat) لأغراض مادية أحياناً وأحياناً أخرى بهدف سرقة المعلومات والإضرار بالخدمات الأساسية

لقد أصبحت الجرائم السيبرانية عملاً مربحًا لأولئك الذين يريدون سرقة البيانات أو إتلاف الأنظمة وممارسة الابتزاز مقابل المال، حيث تواصل جماعات التهديد استخدام الأدوات السيبرانية للتجسس والأضرار بالاقتصاد الاردني، لا سيما أنهم يستهدفون البنية التحتية الحرجة والانظمة الحكومية لقد أدت الجهود التي بذلتها الدولة لتبني التكنولوجيا إلى تشكيل مجتمع أكثر ترابطًا و تقدمًا .و كان للتحول الرقمي في الأردن خلال السنوات الماضية اثراً إيجابياً في مختلف القطاعات ، 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

خلال السنوات القليلة الماضية طرأ تحول كبير على مجتمعنا الأردني الذي أصبح يعتمد بشكل أكبر على الخدمات الرقمية ويستخدم الإنترنت بشكل أوسع ويعتمد بتزايد على قنوات الدفع الرقمية، حيث أن نسبة انتشار الإنترنت في الأردن هي من أعلى النسب في المنطقة، حيث يتمتع 91% من الأردنيين بحرية الوصول إلى الإنترنت[2]، وبشكل أو بآخر يعمل التحول الرقمي على تغيير مجتمعنا واقتصادنا بشكل أسرع من أي وقت مضى، حيث يتم ربط المزيد من الأشخاص والمؤسسات والأجهزة والبيانات بالإنترنت، وهنالك ربط أكبر للأجهزة المحمولة وإنترنت 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، مما يستدعي الحفاظ على أمان هذه البيانات من خلال جعل البيئة الرقمية الأردنية آمنة

لقد نجحت الاستراتيجية الوطنية للأمن السيبراني السابقة (2018 – 2023) في حوكمة الأمن السيبراني على المستوى الوطني وبناء النظام الإيكولوجي السيبراني الوطني، حيث تم خلال هذه الفترة إعداد 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 الأمن السيبراني على المستوى الوطني

وقد حقق الأردن قفزة نوعية في مؤشر الأمن السيبراني العالمي(GCI) لعام 2024 والصادر عن الاتحاد الدولي للاتصالات، حيث تم تصنيف الأردن ضمن أعلى فئات المؤشر والتي شملت فقط (47) دولة من أصل 194[3]

ونسعى من خلال هذه الاستراتيجية إلى تامين الفضاء السيبراني الأردني ، وإلى خلق بيئة رقمية آمنة تشجع على الإبداع والريادة، جاذبة للشركات العالمية وداعمة لرؤية التحديث الاقتصادي، كما ونسعى من خلال هذه الاستراتيجية إلى جعل الأردن مركزاً إقليمياً متميزاً في مجال الأمن السيبراني.

ان مسؤولية مراقبة وتنسيق والاشراف على تنفيذ الاستراتيجية الوطنية للأمن السيبراني وبرنامجها التنفيذي تقع على عاتق المركز الوطني للأمن السيبراني وستتم مراجعتها وتعديلها بشكل دوري عند الضرورة

## واقع التهديدات السيبرانية في الأردن

إن الموقع الجغرافي والجيوسياسي الفريد للمملكة يجذب عدداً من التهديدات السيبرانية التي تنشأ من جهات تهديد إقليمية وعالمية متعددة. وقد تستهدف هذه الجهات الأردن لتعزيز أجنداتها ونفوذها في المنطقة. واستنادًا إلى التطورات الأخيرة والحوادث التي تعرضت لها المملكة، مؤخراً من المرجح أن تواجه المملكة تهديدًا متزايدًا للأنظمة الحكومية والبنى التحتية الحرجة، ومن المرجح أن تركز هذه التهديدات على تعطيل الخدمة وسرقة البيانات والتجسس، وهجمات الفدية. وان التحديات الأكثر شيوعاً التي تؤدي إلى مخاطر وثغرات أمنية سيبرانية تتمثل في عدم الوعي بين موظفي الحكومة والشركات والمستخدمين بمخاطر هذه التهديدات والية مواجهتها. و بالرجوع الى التقارير الأمنية الصادرة عن المركز الوطني للأمن السيبراني، والتي تركز في العادة على شبكات المعلومات الحكومية، يتضح وجود نوعين من المخاطر والتهديدات التي تواجهها المؤسسات الوطنية، وهذه التهديدات هي

### 1 تهديدات خارجية

**أ. جماعات الجريمة السيبرانية المنظمة** والتي تشكل الجزء الأكبر من التهديدات ، والدافع الأساسي لهذه الجماعات هي دوافع مالية

**ب. جماعات التهديد المتطورة** المرتبطة بحكومات ، ودوافع هذه الجماعات هي دوافع سياسية واستخبارية وتهدف الى سرقة المعلومات والتجسس

**ج. جماعات القرصنة الدولية** وهذه الجهات مدفوعة سياسياً وقد لا تكون مرتبطة بأية حكومات أو حركات سياسية

### 2 تهديدات داخلية

من خلال متابعة تقارير المركز،وخاصة الجزء المتعلق بواجهة التهديدات الوطنية نلاحظ ارتفاع في المخاطر المتأتية من الممارسات الخاطئة وعدم التقيد بالمعايير والضوابط،حيث لوحظ ارتفاع في عدد المؤسسات التي تقدم خدمات رقمية تحتوي على ثغرات.وبالمجمل فإن المخاطر الداخلية والتي تم رصدها من قبل المركز خلال السنوات الماضية يمكن تلخيصها كما يلي

[1] الاستراتيجية الوطنية للتحول الرقمي والخطة التنفيذية 2021 – 2025، وزارة الاقتصاد الرقمي والريادة

[2] https://datareportal.com/reports/digital-2024-jordan

[3] Global Cybersecurity Index 2024, ITU, https://www.itu.int/en/ITU-D/-Cybersecurity/Pages/global-cybersecurity-index.aspx

أ. ثغرات في البرمجيات ومنصات الخدمات الرقمية، وتشمل البرمجيات غير المُرخصة والغير محدثة، وتمثل هذه الفئة النسبة الأكبر من المخاطر وهذا يتطلب من المؤسسات بذل مجهود أكبر من ناحية تحديث برمجياتها وإدارة المخاطر المتأتية من الثغرات البرمجية

ب. إعدادات غير آمنة، حيث يُلاحظ أن العديد من أجهزة وأنظمة الحماية في المؤسسات لا يتم تهيئتها وإعدادها بشكل صحيح لمنع وكشف التهديدات، وأحياناً يتم تركها حسب الإعدادات المصنعية. ومن الممارسات الخاطئة أيضاً .استخدام شهادة توثيق منتهية الصلاحية

ج. بروتوكولات مفتوحة، تستخدم تلك البروتوكولات في العديد من الأنظمة شائعة الاستخدام مثل المواقع الإلكترونية والبريد الإلكتروني وبرمجيات نقل الملفات. ومن الأمثلة عليها استخدام بعض المواقع لبروتوكول(http) الإلكترونية

د. قلة وعي المستخدمين بمخاطر التهديدات السيبرانية كأساليب الهندسة الاجتماعية التي تعد من ابرز الأسباب التي ادت الى زيادة الحوادث السيبرانية من خلال استغلال ثقة المستخدم للحصول على معلومات او الوصل الى الأنظمة والأجهزة

## الفئات المستهدفة

الأمن السيبراني مسؤولية جماعية تتشارك فيها الجهود الحكومية مع أصحاب المصلحة و هذه الاستراتيجية تركز على أربع فئات، هي

**الأفراد**

الافراد 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

تقدم الحكومة الدعم والإرشاد للأفراد من خلال المنصات الحكومية حتى يكونوا أكثر مناعة ضد الهجمات وأعمال التحايل

**قطاع الأعمال**

تعاني معظم الشركات الأردنية من عدم القدرة على الاستثمار في الأمن السيبراني بسبب التكاليف المرتفعة وعدم إمكانية توظيف أشخاص لهذه الغاية فقط، لذلك فإن الحوادث التي تتعرض لها هذه الشركات تكون كارثية أحياناً بسبب عدم وجود ضوابط الازمه لحمايتها

تحتل الشركات الصغيرة والمتوسطة مكاناً مهماً في الاقتصاد الأردني

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

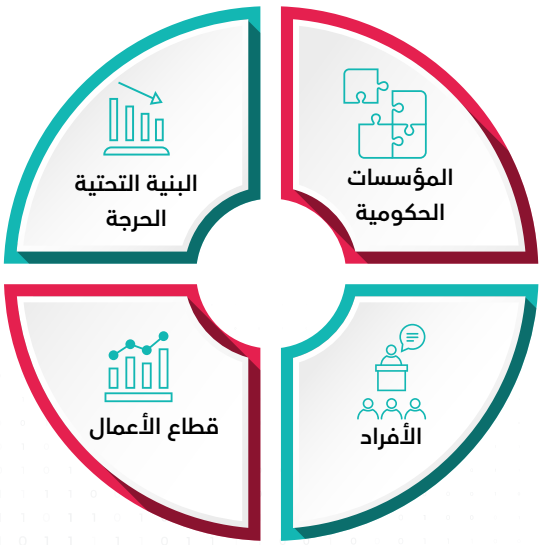
**البنية التحتية الحرجة**

تركز هذه الاستراتيجية على ضمان صمود البنى 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 على تقديم الدعم والمساندة لمشغلي البُنى التحتية الحرجة وبناء علاقات تشاركية داخل كل قطاع وما بين القطاعات المختلفة، بهدف تبادل المعلومات والتعاون في بناء القدرات

**المؤسسات الحكومية**

تُعتبر المؤسسات الحكومية من الجهات المستهدفة 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 من خلال رفع كفاءة مواردها البشرية ورفع كفاءة وتحسين الإجراءات




## الرؤية

سوف نعمل بجهود تكاملية وطنية لضمان استدامة أمن واستقرار الفضاء السيبراني الأردني، وحماية كافة مستخدميه من الأفراد والمؤسسات، وجعل المملكة درعاً منيعاً أمام التهديدات والهجمات السيبرانية من خلال تعزيز المرونة السيبرانية والقدرة على الصمود أمام النشاطات السيبرانية الهادفة للعبث بأمن الاردن الرقمي واستقرار بيئته السيبرانية، **وصولاً إلى:**

فضاء سيبراني أردني، آمن وموثوق، قادر على الصمود
معتمد على القدرات الوطنية، معزز للاقتصاد والرفاه

**فضاء سيبراني أردني:** شاملاً لكافة مكونات الفضاء السيبراني الأردني من الأصول الرقمية والمادية

**آمن:** قادر على توفير متطلبات الأمن والحماية السيبرانية، لكافة مستخدميه من المؤسسات والأفراد

**موثوق:** حائز على ثقة المستخدمين من الأفراد والشركات والمستثمرين في ممارسة نشاطاتهم وأعمالهم في بيئة آمنة وموثوقة

**قادر على الصمود:** حصين بتشريعاته الناظمة وبرامج إدارة مخاطره، صامد وقادر على الاستمرار في تقديم خدماته أمام الهجمات والتهديدات السيبرانية

**معتمد على القدرات الوطنية:** قادر على خلق واستدامة وتحفيز الموارد البشرية الموهوبة، ومصدرًا لها

**معزز للاقتصاد والرفاه:** مسانداً لمحركات النمو في الاقتصاد الوطني، ومعززاً للرفاه المجتمعي

## الأهداف الاستراتيجية

**الأمن والثقة**
تطوير بيئة رقمية أردنية آمنة وموثوق بها

**المرونة والصمود**
حوكمة شمولية للأمن السيبراني وضمان صمود الخدمات الأساسية

**بناء القدرات**
الأردن بيت خبرة ومصدر للمواهب السيبرانية

**التعاون والشراكات**
فضاء سيبراني متين بعلاقاته التشاركية، منافس إقليميًا وعالميًا

**اشتملت هذه الاستراتيجية على: (4) أهداف رئيسية (14) هدف فرعي**

# 1 الأمـــن والثـقـة

بهدف بناء الثقة بالفضاء السيبراني الأردني لكافة مستخدميه من الأفراد والمؤسسات المحلية والإقليمية والدولية، من خلال بنية تحتية رقمية آمنة وموثوق بها تعزز كافة الجهود الوطنية الرامية للتحول الرقمي ، وترمي كذلك لحماية الأصول الرقمية المُشغلة والداعمة لهذه الخدمات، من خلال اتباع منهجية ترتكز على الإدارة الاستباقية للمعلومات السيبرانية ، وتكوين فهم اكثر شمولية لأثرها وتهديداتها على الفضاء السيبراني الأردني، وبما يضمن أمن هذا الفضاء واستقراره

## أولوية-1: تطوير بيئة رقمية أردنية آمنة وموثوق بها

الأهداف الفرعية (عددها 4 أهداف)


### 1 تعزيز الثقة بالبيئة الرقمية الأردنية وتقديم خدمات رقمية آمنة

إن 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 عبر الإنترنت، وتضمن حماية المعلومات الحساسة وتعزز الثقة في التفاعل عبر الإنترنت، كما تتيح البيئة الرقمية الآمنة للأطفال الاستكشاف والتعلم عبر الإنترنت دون التعرض للمحتوى الضار وتمكن الجميع من المشاركة في الاقتصاد الرقمي بثقة
ان البيئة الرقمية الآمنة تحمي بيانات الشركات كحقوق الملكية الفكرية ومعلومات العملاء و تقلل من مخاطر الهجمات السيبرانية التي يمكن أن تعطل العمليات وتضر بالسمعة وتلحق بالشركات 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
ان تنفيذ هذا الهدف من خلال البرامج التالية

**1-1 توفير بيئة إنترنت آمنة**
**1-2 تقديم خدمات إلكترونية آمنة وموثوق بها**
**1-3 تمكين جهات انفاذ القانون في مكافحة الجريمة السيبرانية**

### 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 تشير عمليات التقييم المستمرة لنطاقات عناوين الإنترنت الأردنية التي يجريها المركز الوطني للأمن السيبراني والحوادث التي يتعامل معها بشكل شبه يومي، إلى وجود ثغرات وضعف في إجراءات الأمن السيبراني
ان تنفيذ هذا الهدف من خلال البرامج التالية

**2-1 توفير منصة لدعم الشركات الصغيرة والمتوسطة**
**2-2 إطلاق برنامج الدفاع السيبراني الفعّال**

### 3 إدارة المخاطر المتأتية من استخدام التقنيات الحديثة وسلاسل التوريد

يمكن أن تشكل التقنيات والخدمات التي لم تراعى فيها متطلبات الأمن في مراحل التطوير والإنتاج نقاط ضعف يمكن للجهات الخبيثة استغلالها بسهولة مما قد يؤدي إلى تقويض ثقة الجمهور في التكنولوجيا، كما أن العديد من التقنيات الرقمية لا تحتوي على معايير أمان مضمنة في التصميم أو يتم تشغيلها بناء على الإعدادات الافتراضية، ونتيجة لذلك من الممكن أن يُعرض على المستهلكين والشركات منتجات وخدمات أقل أماناً، مع عدم وجود خبرة كافية لإدارة المخاطر من الضروري وضع إطار عمل لتقييم المخاطر الأمنية المتأتية من التقنيات الرقمية الحديثة وسلاسل التوريد الداخلة إلى 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 التي من شأنها الحد من دخول المنتجات الرقمية غير الآمنة الى السوق المحلية

وكون الذكاء الاصطناعي هو أحد التقنيات الرئيسية في القرن الحادي والعشرين ويؤثر على العمليات والقرارات الأمنية في قضايا حرجة، مثل القياسات الحيوية والرعاية الصحية والتنقل والطيران وغيرها، فمن الضروري كذلك، تحقيق أعلى مستوى ممكن من الأمن السيبراني لأنظمة الذكاء الاصطناعي، ولتحقيق هذه الغاية، ستتأكد الحكومة من وجود الضوابط والمعايير الأمنية المناسبة للحماية من المخاطر الأمنية المتأتية من الذكاء الاصطناعي. في نفس الوقت ستتأكد .الحكومة من الاستفادة من الفرص التي يجلبها الذكاء الاصطناعي لتوفير مستوى عال من الأمن السيبراني

ان تنفيذ هذا الهدف من خلال البرامج التالية

**3-1 تطوير معايير أمن سيبراني للتقنيات الناشئة وسلاسل التوريد**

**3-2 تنفيذ برنامج للاعتماد وإصدار الشهادات في مجال الأمن السيبراني**

**3-3 تشجيع الشركات على تطوير حلول رقمية آمنة تراعي تقنيات الذكاء الاصطناعي**

### 4 تحقيق التنوع والشمول السيبراني لفئات 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، العمل، والاحتفاظ بالمواهب بشكل أكبر

ان مراعاة التنوع والشمول في مجال الأمن السيبراني، كجزء من التزام الحكومة بالشمول الرقمي الذي يمنح جميع فئات المجتمع فُرص متساوية سواء في الوصول للخدمات أو في فُرص العمل وسيتم دعم مبادرات تحقق هذا الغرض، مثل تمكين المرأة في السايبر، أو مشاريع تشمل كافة فئات المجتمع بما في ذلك الفئات الاجدر بالحماية والدعم في المجتمع، مثل كبار السن والأطفال والمرأة، يسهم في تشجيع الأشخاص من هذه الفئات السكانية لمتابعة التدريب أو العمل في مجال الأمن السيبراني

ان تنفيذ هذا الهدف من خلال المبادرات التالية

**4-1 تمكين المرأة في السايبر**

**4-2 حماية الطفل**

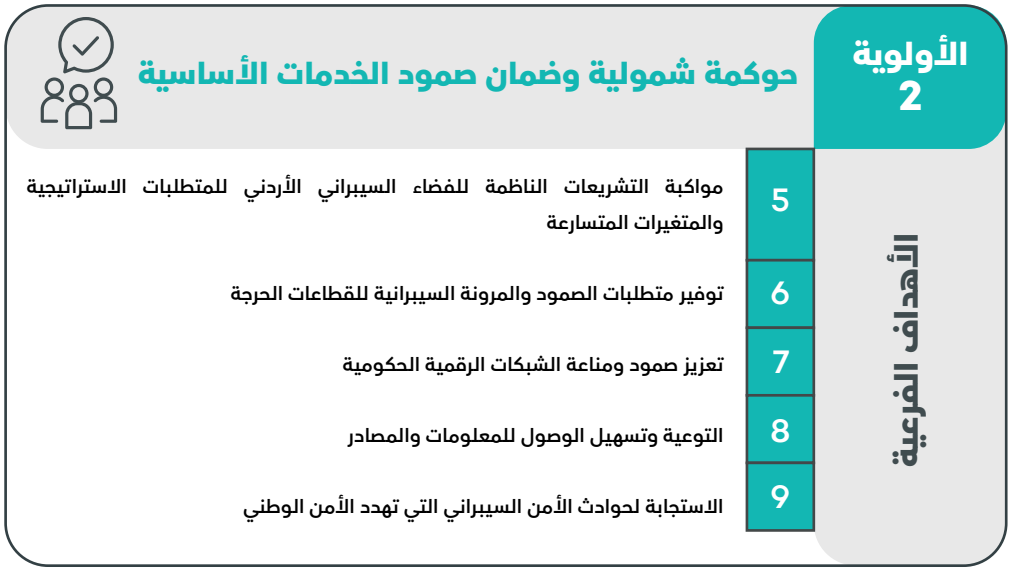
**4-3 دعم القدرة على الوصول لخدمات الأمن السيبراني للفئات الاجدر بالحماية والدعم في المجتمع**

## 2 المرونة والصمود

التكييف مع أية تهديدات أو هجمات سيبرانية قد تتعرض لها الأصول الرقمية والتقنية المشغلة للقطاعات الوطنية الحرجة والأساسية في المملكة، وتطوير القدرة على مواجهة التهديدات السيبرانية، 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

## أولوية-2: حوكمة شمولية وضمان صمود الخدمات الأساسية

الأهداف الفرعية (عددها 5 أهداف)




### 5 مواكبة التشريعات الناظمة للفضاء السيبراني الأردني للمتطلبات الاستراتيجية والمتغيرات المتسارعة

إن حوكمة الأمن السيبراني تتطلب مراجعة مستمرة للتشريعات الناظمة لضمان موائمتها للعصر وللتغيرات السريعة وخصوصاً في المجال التكنولوجي الذي هو في تغير ديناميكي مستمر وسريع، وخاصة تلك المرتبطة بقطاعات البنى التحتية الحرجة، حيث ستعمل الحكومة على تقييم مدى الحاجة إلى ضوابط وأطر قطاعية بناءً على حاجة كل قطاع ومتطلباته الخاصة

ان تنفيذ هذا الهدف من خلال البرامج التالية

**5-1 مراجعة القوانين والأنظمة والتعليمات ذات العلاقة بالأمن السيبراني**

### 6 توفير متطلبات المرونة والصمود السيبرانية للقطاعات الحرجة

يجب أن تكون البنى 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 الإلكترونية الأساسية

وتعرف البنية التحتية الحرجة انها مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة التي يعد تشغيلها المستمر ضرورة لضمان امن الدولة واقتصادها وسلامة المجتمع. وللحد من مخاطر الاضطرابات الكبيرة التي قد تتعرض لها مجتمعاتنا وقطاعاتنا، يجب أن تكون هذه الأنظمة قادرة على تحمل الهجمات السيبرانية واسعة النطاق، وان للاستجابة لهذه الحوادث يتطلب خطة وطنية شاملة وواضحة تضمن التعافي من هذه الهجمات بسرعة وكفاءة عالية وبما يضمن استمرارية الخدمات الأساسية وانسيابها بشكل معتاد

ان تنفيذ هذا الهدف من خلال البرامج التالية

**6-1 تطبيق الإطار الوطني الأردني للأمن السيبراني**
**6-2 تعزيز وتطوير المنظومة الوطنية للتدقيق ومراقبة الالتزام**
**6-3 تطوير إطار عمل وضوابط خاصة بقطاعات البُنية التحتية الحرجة**
**6-4 تطوير قدرات المراقبة وفرق الاستجابة القطاعية**
**6-5 حماية وتامين المعلومات الأكثر حساسية للدولة والمجتمع**
**6-6 إدارة فعالة ومنظومة وطنية لمشاركة المعلومات**

## 7 تعزيز صمود ومناعة الشبكات الرقمية الحكومية

استثمرت الحكومة الأردنية ممثلةً بوزارة الاقتصاد الرقمي والريادة بشكل كبير في بناء شبكة قوية في جميع أنحاء المملكة لخدمة المتمثل في ربط جميع الجهات الحكومية لتقديم خدمة أفضل للمواطنين الأردنيين، وتُعتبر الشبكة الحكومية الآمنة (SGN) والمحرك الداعم لعملية التحول الرقمي والذي تعتمد عليه أغلب الخدمات الرقمية في القطاعين العام والخاص، ولذلك فإن صمود الشبكة الحكومية الآمنة أمر حيوي وأساسي في صمود باقي الخدمات الأساسية الوطنية أن المعلومات والخدمات الحكومية أهدافًا عالية القيمة لجهات التهديد الفاعلة، ويمكن أن تهدد الحوادث السيبرانية سلامة المعلومات التي تحتفظ بها الحكومة، ويمكن أن تهز ثقة الجمهور في مؤسسات الدولة وفي الخدمات الرقمية المختلفة التي تقدمها الحكومة

ان 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 والأمن كجزء من وظائفها الأساسية، ولهذا فستقوم الحكومة بتعزيز المسائلة القانونية ومحاسبة الجهات المقصرة في الامتثال للأطر والضوابط والمعايير الوطنية

لقد كشفت التقييمات الأمنية التي نفذها المركز لعدد من المؤسسات الحكومية والوطنية، الى انخفاض مستويات النضوج السيبراني وإمكانية حدوث تعطل للخدمات الرقمية الأساسية، كما أشارت هذه التقييمات إلى وجود نقص كبير في المهارات السيبرانية .

ان تنفيذ هذا الهدف من خلال البرامج التالية

- **7-1 تصنيف البيانات الحكومية وادارتها**
- **7-2 التوسع في مراقبة الشبكات والأنظمة والتطبيقات والأجهزة الطرفية الحكومية**
- **7-3 تحسين وتعزيز قدرات الأمن السيبراني في الوزارات والدوائر الحكومية**
- **7-4 تطوير شبكة اتصالات معلوماتية حكومية مشفرة وآمنة**

## 8 التوعية وتسهيل الوصول للمعلومات والمصادر

تهدف هذه الاستراتيجية إلى رفع مستوى الوعي بين الأفراد 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 تلتزم الحكومة الأردنية من خلال مؤسساتها المختلفة بتنفيذ حملات توعوية على مدار السنة، كما يتولى المركز نشر التحذيرات المتعلقة بالتهديدات والثغرات الأمنية من خلال المنصات المختلفة المعتمدة لهذه الغاية بالمركز

ان تنفيذ هذا الهدف من خلال البرامج التالية

- **8-1 التوعية بالمخاطر المتأتية من الفضاء السيبراني**
- **8-2 التعريف بالمنصات المعتمدة للتوعية وتشجيع استخدامها**

## 9 الاستجابة لحوادث الأمن السيبراني التي تهدد الأمن الوطني

لقد حدد المركز الوطني للأمن السيبراني معايير لتصنيف حوادث الأمن السيبراني تم بموجبها تصنيف الحوادث الى أربع فئات هي: "**المنخفض**" و "**المتوسط**" و "**الخطير**" و "**شديد الخطورة**". وتتطلب الحوادث التي تشكل خطراً على أمن المملكة وسلامتها"[4] استجابة وطنية موحدة يتم إدارتها كخلية ازمة باشراف "المركز الوطني للأمن وإدارة الأزمات" بصفته الجهة المعنية بإدارة الأزمات والكوارث التي تؤثر على الأمن الوطني، ويتم إدارة الحادث من الجانب الفني من قبل المركز الوطني للأمن السيبراني الذي يتولى اصدار التعليمات و التوجيهات لكافة الجهات لاحتواء الحادث الأمني والتخفيف من اثاره

ان تنفيذ هذا الهدف من خلال البرامج التالية

- **9-1 خطة الطوارئ للاستجابة لحوادث الأمن السيبراني**
- **9-2 تمارين سيبرانية لفحص صمود الشبكات**

[4] المادة 9/أ من قانون الأمن السيبراني

# 3 بناء القدرات

بهدف تعزيز وتقوية مفهوم الأمن السيبراني وعملياته التشغيلية لدى كافة القطاعات الوطنية ، وذلك من خلال تطوير البنية التكنولوجيا والفنية المشغلة للعمليات الرقمية والداعمة لمتطلبات الحماية السيبرانية، واستخدام التقنيات والأنظمة الحديثة التي توفر الحماية للأصول الرقمية. سنعمل من خلال هذا التوجه لخلق بيئة سيبرانية أردنية قادرة على التعلم المستمر مُحفزة لعمليات التطوير والتحسين والإبداع والابتكار في الأمن السيبراني، مُسلحة بكوادر بشرية على قدرٍ عالٍ من المعرفة والاحترافية في الأداء، قادرة على التعامل مع تحديات ومستجدات الفضاء السيبراني وتطويعها لحماية الفضاء السيبراني الأردني

## أولوية-3: تعزيز القدرات السيبرانية الوطنية

الأهداف الفرعية (عددها 3 أهداف)


**10 تطوير وبناء القدرات والمعارف والمهارات السيبرانية على المستوى الوطني**

يعاني الأردن نقصاً حاداً في الخبرات في مجال الأمن السيبراني ، وبالرغم من إطلاق الجامعات الأردنية عدد لا بأس به من البرامج الأكاديمية في تخصص الأمن السيبراني خلال السنوات القليلة الماضية، إلا أن القطاع لا يزال يعاني من نقص في الخبرات، بحيث لا يتم التركيز أكثر على التعليم العملي والتطبيقي الذي يكفل منح الخريجيين المهارات التي يحتاجها السوق

ولجعل الأردن مركز إقليمي للتميز السيبراني يتطلب الامر تنفيذ إصلاحات لدعم وتطوير نظام تعليم وتدريب أكثر فعالية يلبي احتياجات القوى العاملة في مجال الأمن والسيبراني

ان تنفيذ هذا الهدف من خلال البرامج التالية

- **10-1 انشاء اكاديمية وطنية للامن السيبراني**
- **10-2 رفع المهارات السيبرانية للموظفين العاملين في مديريات ووحدات تكنولوجيا المعلومات والاتصالات في الوزارات والمؤسسات والدوائر الحكومية**
- **10-3 الاستثمار في التدريب وبناء القدرات**
- **10-4 تشجيع وتحفيز المواهب الوطنية**
- **10-5 جائزة التمييز في الامن السيبراني**
- **10-6 مراجعة معايير برامج الامن السيبراني في الجامعات الحكومية**
- **10-7 تطوير المناهج المدرسية وبناء قدرات الطلبة**

**11 تعزيز النظام البيئي للأعمال في قطاع الأمن السيبراني**

ان الحاجة إلى المساهمة في تعزيز السيادة الوطنية فيما يتعلق بالاعتماد على منتجات وحلول الأمن السيبراني الوطنية مع الأخذ في الاعتبار تعزيز الفرص الاقتصادية وفرص العمل وتعزيز الشركات في قطاع الأمن السيبراني في الأردن كمحور رئيسي لها، لذلك فان الحكومة ستعمل على مواصلة تحفيز إنشاء الأعمال والشركات الناشئة من خلال تشجيع صناعة الأمن السيبراني وتعزيزها وتشجيع البحث والتطوير ودعم المواهب لتلبية الطلب الكبير على المهنيين في هذا القطاع، بالإضافة الى دعم إنشاء مسرعات الأعمال والحاضنات 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)

ان تنفيذ هذا الهدف من خلال البرامج التالية

**11-1 دعم وتشجيع صناعة الأمن السيبراني**

**12 تعزيز بيئة البحث والتطوير**

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

ان تنفيذ هذا الهدف من خلال البرامج التالية

**12-1 دعم وتشجيع البحث العلمي والتطوير**

## 4 التعاون والشراكات

ان تأطير العلاقات المحلية والإقليمية والدولية، يكفل للفضاء السيبراني الأردني ومكوناته التكنولوجيا والعملياتية والبشرية الانفتاح على الخبرات الإقليمية والعالمية، والاستفادة من قصص نجاح الآخرين. كما ان الأردن معني بدعم الجهود الدولية الرامية لتعزيز مبادئ الاستخدام المسؤول للفضاء السيبراني العالمي

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

الأهداف الفرعية (عددها 2 أهداف)

**الأولوية 4**

**تشجيع الشراكات الاستراتيجية المحلية وتعزيز دور الأردن على المستويين الإقليمي والدولي**

الأهداف الفرعية

13 تعزيز الدور الأردني والمشاركة في المبادرات الإقليمية والدولية

14 تعزيز الالتزام والتعاون والتنسيق محليًا، مابين أصحاب المصلحة

**13 تعزيز الدور الأردني والمشاركة في المبادرات الإقليمية 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 الأعمال العدائية والتزامها بالسلوك المسؤول في استخدام التكنولوجيا وعدم الأضرار بالآخرين. كما أن الثقة بأمن الفضاء السيبراني الأردني والمحافظة علية كبيئة تفاعلية رقمية آمنة، 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 والإقليميين والدوليين

يتم تنفيذ هذا الهدف من خلال المبادرات التالية

**13-1 المشاركة الإيجابية الفاعلة في المحافل الدولية**
**13-2 تعزيز مشاركة فرق الاستجابة الأردنية في النشاطات الإقليمية والدولية**
**13-3 التعاون في مجال مكافحة الجريمة السيبرانية**
**13-4 دعم المبادرات الدولية الهادفة الى تبني السلوك المسؤول للدول في الفضاء السيبراني**
**13-5 تعزيز وتطوير العلاقات التعاونية والتشاركية على المستوى الثنائي والمتعدد الأطراف**

**14 تعزيز التعاون والتنسيق محلياً ما بين أصحاب المصلحة**

تلعب كل جهة من أصحاب المصلحة دوراً مهماً وحيوياً في منظومة الأمن السيبراني الوطنية، وتتحمل كل جهة مسؤوليات واضحة حددتها القوانين والأنظمة والتعليمات والقرارات الصادرة بهذا الخصوص، وهذا لا يمنع من الناحية التنفيذية أن 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 يضم في عضويته ممثلين عن القطاعات 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 إقرار أي تشريعات تتعلق بالأمن السيبراني

تنفيذ هذا الهدف من خلال المبادرات التالية

**14-1 تشجيع الشراكات والمبادرات القطاعية**
**14-2 مبادرة الشراكة ما بين القطاعين العام والخاص لتعزيز الأمن السيبراني الأردني**

## برامج ورؤى التحديث الوطنية

نادى جلالة الملك عبد الله الثاني ابن الحسين (حفظه الله) بإصلاح شامل يهدف إلى إطلاق الطاقات الوطنية في مختلف المجالات، سعياً لتحقيق النمو الشامل المستدام لتوفير حياة أفضل للمواطنين. وقد شملت خطط ورؤى الإصلاح برامج التَّحديث الشَّامل بمساراته السِّياسيَّة والاقتصاديَّة والإداريَّة ولقد تم تطوير هذه الاستراتيجية لتكون متوائمة مع خطط الإصلاح والتي تشمل خارطة تحديث القطاع العام ورؤية التحديث الاقتصادي التي تهدف إلى تحقيق معدلات نمو مرتفعة وجذب الاستثمارات وتوفير فرص عمل للشباب الأردني

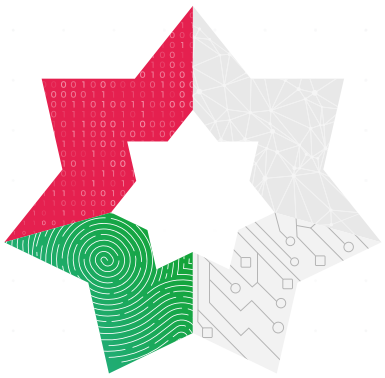
إن خلق بيئة رقمية آمنة، مرنة، وموثوق بها من شأنه أن يسهم بشكل كبير في تحفيز النشاطات التجارية وفي نمو وتطور الاقتصاد الرقمي الذي هو مستهدف أساسي في خطط وبرامج التحديث الوطنية. كما أن البيئة الرقمية الآمنة تسهم بشكل كبير في تحسين نوعية حياة المواطنين التي هي ركيزة أساسية في رؤية التحديث الاقتصادي[5]

لقد تم تطوير هذه الاستراتيجية بحيث تدعم وتعزز وتتماشى مع خطط التحديث الوطنية وتسهم في محركات النمو في رؤية التحديث الاقتصادي التالية

[5] رؤية التحديث الاقتصادي، https://www.jordanvision.jo/

| محركات نمو في رؤية الـتحديث الاقتـصادي | أولـويات الاستـراتيـجية الوطنية للأمن السيبراني |
|---|---|
| **الاستثمار**<br>تحفيز الاستثمارات المحلية والدولية من خلال بيئة جاذبة للاستثمار | **أولوية الأمن والثقة**<br>لخلق بيئة جاذبة للاستثمار لابد أن تكون هذه البيئة آمنة ومنظمة وتحمي سرية البيانات وخصوصيتها<br>الثقة في البيئة الرقمية شيء أساسي في تمكين الأعمال من ممارسة نشاطاتها التجارية |
| **الصناعات عالية القيمة**<br>تطوير الأردن ليكون مركزاً إقليميا للصناعة من خلال منتجات متميزة وذات قيمة عالية | **أولوية بناء القدرات**<br>نسعى من خلال أولوية التحول السيبراني الى خلق صناعة أمن سيبراني وطنية من خلال تشجيع ورعاية ودعم الأفكار الإبداعية وشركات الأمن السيبراني الناشئة |
| **الخدمات المستقبلية**<br>تحقيق التميّز في القطاعات الخدمّية وزيادة الصادرات الخدمّية الى الأسواق الخارجية | **أولوية الأمن والثقة**<br>نحرص من خلال تنظيم وترخيص خدمات الأمن السيبراني علي زيادة تنافسية مقدمي الخدمات الأردنيين<br>**أولوية بناء القدرات**<br>من خلال تعزيز بيئة الأعمال ودعم صناعات الأمن السيبراني الوطنية ودعم البحث والتطوير |
| **الريادة والإبداع**<br>إعداد المواهب المواكبة لمتطلبات ووظائف المستقبل | **أولوية بناء القدرات**<br>تركز هذه الأولوية بشكل كبير على تطوير وبناء القدرات والمعارف والمهارات السيبرانية التي هي من وظائف المستقبل |
| **نوعية الحياة**<br>تحسين نوعّية حياة الأردنّيين من خلال تطوير وتطبيق مفاهيم حياتية شاملة محورها المواطن والبيئة | **أولوية الأمن والثقة**<br>توفير بيئة رقمية آمنة، خصوصاً لفئات الأطفال وكبار السن مما يسهم في تحسين نوعية حياتهم ويمكنهم من ممارسة نشاطاتهم بحرية<br>**أولوية المرونة والصمود**<br>تركز الاستراتيجية على أهمية التوعية للأفراد وكذلك توفير المعلومات الإرشادية التي يحتاجونها للوقاية من مخاطر السايب |

وانطلاقاً من كتاب التكليف السامي لحكومة دولة الدكتور جعفر حسان سيعمل المركز على إعداد البرنامج التنفيذي لهذه الاستراتيجية ، لإرساء منظومة وطنية متطورة ومستدامة لإدارة العمليات السيبرانية تضمن الكشف المبكر والاستجابة الفاعلة للحوادث والتهديدات السيبرانية، التي قد تتعرض لها المملكة



المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

# الاستراتيجية الوطنية للأمن السيبراني
# National Cyber Sceurity Strategy

## 2028 - 2025