المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

الاستراتيجية الوطنية للأمن السيبراني

2025 - 2028

مملكة البحرين

"النسخة العامة"

شكر وتقدير

تُجسد هذه الاستراتيجية روح التعاون الوطني وحصيلة عمل مشترك، بمساهمة واسعة من الأفراد والمؤسسات في مختلف مناطق مملكة البحرين وقطاعاتها، ملتزمين جميعاً بصياغة ملامح الاستراتيجية الوطنية للأمن السيبراني للفترة من 2025 إلى 2028.

بدأت عملية إعداد الاستراتيجية عبر مراحل متعددة، شملت وضع خطة العمل وتحليل الوضع الحالي، تلتها مرحلة تطوير المسودة الأولية ومشاركتها مع الشركاء لاستطلاع آرائهم وتحديثها بناءً على الملاحظات واختُتمت بإعداد النسخة النهائية، وتضمنت هذا المراحل عقد 11 ورشة عمل جمعت أصحاب المصلحة الرئيسيين، حيث بلغ عدد الحضور 319 مشاركًا، إلى جانب تنظيم نحو 25 اجتماعًا فرديًا مع مؤسسات من القطاعات الحيوية لتبادل الرؤى والتوصل إلى توافق حول الأولويات والتطلعات في مجال الأمن السيبراني، كما أُجري استبيان لتقييم مستوى الوضع الحالي للأمن السيبراني شاركت فيه 173 مؤسسة كما دعمت هذه الجهود مناقشات فردية وجلسات عمل لضمان تطوير استراتيجية متكاملة ومستندة على أفضل الممارسات العالمية.

ونتقدم بجزيل الشكر والتقدير لكل من ساهم وشارك وقدم رؤاه القيمة، إيمانًا منا بأن هذا الجهد المشترك سيسهم في تحقيق وتعزيز تطلعات ومكانة المملكة كدولة رائدة في مجال الاقتصاد الرقمي.

الاستراتيجية الوطنية للأمن السيبراني (2025 – 2028)
حقوق النشر @ 2025
المركز الوطني للأمن السيبراني – مملكة البحرين
جميع الحقوق محفوظة.

www.ncsc.gov.bh

المحتوى

1. **الملخص التنفيذي** 6

2. **المقدمة** 8

3. **التوسع الرقمي للمملكة** 10

4. **القطاعات الحيوية الوطنية** 12

5. **الرؤية والرسالة** 14

6. **ركائز الاستراتيجية وأهدافها** 16

6.1 **الركيزة الأولى: المرونة السيبرانية المتقدمة** 18

6.1.1 الهدف الأول: تقوية الحماية السيبرانية للبنية التحتية الرقمية في مملكة البحرين 19

6.1.2 الهدف الثاني: رفع القدرات الوطنية للتصدي للتهديدات السيبرانية 20

6.1.3 الهدف الثالث: تعزيز إدارة الأزمات والاستجابة للحوادث السيبرانية 21

6.2 **الركيزة الثانية: الحوكمة السيبرانية الفعالة** 22

6.2.1 الهدف الأول: دعم إصدار القوانين واللوائح التنظيمية السيبرانية 23

6.2.2 الهدف الثاني: إدارة المخاطر السيبرانية على المستوى الوطني 24

6.2.3 الهدف الثالث: التطوير بناءً على السياسات والمعايير الوطنية للأمن السيبراني 25

6.2.4 الهدف الرابع: ضمان الالتزام المستمر لمعايير الأمن السيبراني 26

6.3 **الركيزة الثالثة: التعاون وتوسيع الشراكات** 28

6.3.1 الهدف الأول: تعزيز التعاون الوطني للأمن السيبراني 29

6.3.2 الهدف الثاني: توسيع الشراكات الإقليمية والدولية 30

6.4 **الركيزة الرابعة: ثقافة وكوادر سيبرانية مستدامة** 32

6.4.1 الهدف الأول: توسيع نطاق الوعي الوطني بالأمن السيبراني 33

6.4.2 الهدف الثاني: تطوير كوادر وطنية متخصصة في الأمن السيبراني 34

6.5 **الركيزة الخامسة: البحث والتطوير والابتكار** 36

6.5.1 الهدف الأول: تعزيز الكفاءات الوطنية في مجال البحث والتطوير والابتكار 37

6.5.2 الهدف الثاني: الارتقاء بصناعة الأمن السيبراني 38

7. **الخاتمة** 40

الملخص التنفيذي

01

تحرص مملكة البحرين على تبنّي نهج استراتيجي متكامل ورؤية مستقبلية طموحة لدفع عجلة التطوّر التقني وتعزّز مسيرة التحوّل الرقمي لتحقيق النموّ الاقتصادي والتقدّم الوطني المستدام، وفي ظلّ ما يشهده العالم من تهديدات. أدركت المملكة أهمية توفير فضاء سيبراني آمن وموثوق يحقق الحماية اللازمة للبنية التحتية الرقمية الوطنية والحفاظ على المنجزات والمكتسبات في مجال تقنية المعلومات التي تحقّقت عبر مسيرتها التنموية، لذلك وضعت المملكة الأمن السيبراني ضمن أبرز أولوياتها الوطنية، ملتزمةً باتخاذ كافة الإجراءات والتدابير التي تضمن حماية فضائها الرقمي وتُرسي دعائم بيئة تقنية متقدمة ومستدامة تُعزّز من قدراتها التنافسية في عصر الاقتصاد الرقمي.

ولأهمية الأمن السيبراني في المملكة تم إطلاق الاستراتيجية الوطنية للأمن السيبراني 2021-2024، والتي أسهمت في تعزيز الأمن السيبراني على المستوى الوطني، حيث تم تأسيس المركز الوطني للأمن السيبراني كجهة مختصة في المملكة تهدف إلى تعزيز الحوكمة وتنفيذ وسائل فعّالة للحماية والاستجابة ونشر الوعي السيبراني، حيث تم تطوير إطار وطني لحماية البنية التحتية الحيوية، بالإضافة إلى تشكيل الفريق الوطني للاستجابة للحوادث السيبرانية لضمان استجابة سريعة وفعّالة للتهديدات السيبرانية، علاوةً على ذلك، أطلقت البحرين حملات وبرامج توعوية وتدريبية تستهدف الجهات والأفراد من مواطنين ومقيمين، ومن إنجازات الاستراتيجية حصول المملكة على تصنيف «الفئة الأولى - نموذجاً رائداً» في مؤشر الأمن السيبراني العالمي للعام 2024 الصادر عن الاتحاد الدولي للاتصالات التابع لمنظمة الأمم المتحدة المتخصصة بتكنولوجيا المعلومات والاتصالات والتي شاركت فيه 194 دولة.

واستكمالاً على هذه الإنجازات والنجاحات المحققة، أطلق المركز الوطني للأمن السيبراني الاستراتيجية الوطنية للأمن السيبراني 2025-2028، حيث تم إعدادها وفق منهجية تستند على المعايير الدولية وأفضل الممارسات العالمية من خلال أربع مراحل رئيسية وهي وضع الخطة وتحديد الشركاء وتحليل الوضع الحالي وتطوير مسودة الاستراتيجية واخيراً الاعتماد النهائي، وتضمن هذه المنهجية ملاءمة الاستراتيجية لمتطلبات المملكة من خلال إشراك منظمي القطاع والشركاء الرئيسين من جميع القطاعات الحيوية لقياس مستوى الأمن السيبراني ومناقشة التحديات والفرص ثم تحديد الأولويات الاستراتيجية.

سيتم تنفيذ هذه الاستراتيجية على مدى أربع سنوات والتي تمثل إطاراً متكاملاً لحماية البنية التحتية الرقمية الوطنية من التهديدات السيبرانية المتجددة، وتحقق الريادة في مجال الأمن السيبراني وتخلق بيئة تدعم الابتكار والازدهار مع تمكين المؤسسات والأفراد في مجال الأمن السيبراني بناءً على الرؤية المتمثلة في

الريادة في توفير فضاء إلكتروني آمن ومرن وموثوق، يقوده الابتكار ويعزّز النمو الرقمي

بينما تتمثل الرسالة في

تحقيق الريادة في مجال الأمن السيبراني لحماية البنية التحتية الرقمية من خلال دعم الابتكار وتوفير بيئة إلكترونية آمنة ومرنة وموثوقة تعزز النمو الوطني وترفع التنافسية العالمية لمملكة البحرين.

تستند الاستراتيجية الوطنية للأمن السيبراني إلى خمس ركائز أساسية تمثّل منظومة شاملة تحدد التوجهات المستقبلية وتشمل المرونة السيبرانية المتقدمة والحكومة السيبرانية الفعّالة والتعاون وتوسيع الشراكات وثقافة وكوادر سيبرانية مستدامة والبحث والتطوير والابتكار، مما يعزز جاهزية المملكة لمواجهة التهديدات السيبرانية ويضمن حماية واستدامة وموثوقية المنظومة الرقمية.

تمثل الاستراتيجية الوطنية للأمن السيبراني 2025-2028 نهجاً متكاملاً نحو تعزيز الأمن السيبراني في مملكة البحرين، وتهيئة بيئة رقمية آمنة ومرنة تدعم النمو الاقتصادي وتواكب التطور التقني من خلال ركائزها الأساسية، وتوفر الاستراتيجية رؤية شاملة لحماية البنية التحتية الحيوية وتعزيز الحوكمة الفعّالة وتوسيع التعاون الدولي ورفع مستوى الوعي في مجال الأمن السيبراني وتنمية الكفاءات الوطنية فضلاً عن الابتكار وصناعة الأمن السيبراني، ولتنفيذ الاستراتيجية بفعالية يتطلب تعاون وتكامل بين مختلف القطاعات والجهات المعنية وتنسيق الجهود على المستويين المحلي والدولي، بما يسهم في جعل مملكة البحرين رائدة في الأمن السيبراني.

المقدمة

انطلاقاً من حرص مملكة البحرين لتحقيق بيئة رقمية آمنة تدعم النمو والازدهار وتتبنى الابتكارات التقنية، أصبح الأمن السيبراني أولوية وطنية أساسية لحماية البنية التحتية الوطنية والأنظمة الحيوية والأصول المعلوماتية، وقد أدى التحول الرقمي إلى ظهور تحديات جديدة تتطلب التصدي للمخاطر وحماية الفضاء الإلكتروني للمملكة خاصة مع ازدياد التهديدات السيبرانية وتطويرها وتعقيدها، ولقد تجلى التزام المملكة بالأمن السيبراني بإطلاق الاستراتيجية الوطنية للأمن السيبراني الأولى 2021-2024، والتي أسهم تنفيذها في تصنيف البحرين كـ «نموذج عالمي من المستوى الأول» من بين 194 دولة وفقاً لمؤشر الأمن السيبراني العالمي الصادر عن الاتحاد الدولي للاتصالات لعام 2024.

وتواصل المملكة على ما تم إنجازه عبر تدشين الاستراتيجية الوطنية للأمن السيبراني 2025-2028، والتي تم تطويرها وفق أفضل الممارسات الدولية، مع الأخذ في الاعتبار المتطلبات الوطنية والتوجهات العالمية، وتقدم هذه الاستراتيجية نهجاً استباقياً شاملاً يعزز القدرات السيبرانية للمملكة، ويدعم مكانتها في الفضاء الرقمي العالمي، وقد شملت عملية إعداد الاستراتيجية أربع مراحل رئيسية، بدأت بوضع خطة إعداد الاستراتيجية وتحديد الشركاء الرئيسيين لضمان مشاركة فعّالة في تطويرها، تلتها مرحلة تحليل الوضع الحالي لإجراء دراسة شاملة لمستوى الأمن السيبراني وتحديد الإمكانيات المتاحة والتحديات القائمة مما وفر الأولويات لصياغة الاستراتيجية، ومن ثم تطوير المسودة الأولية ومشاركتها مع الشركاء بهدف تلقي الملاحظات والتعديلات بما يضمن توافقها مع المتطلبات الوطنية وأفضل الممارسات واختُتمت العملية باعتماد المسودة النهائية لبدء تنفيذ الاستراتيجية، وسيتم التركيز خلال تنفيذ الاستراتيجية على التعاون المستمر ومع منظمي ومؤسسات القطاعات الحيوية وخبراء الأمن السيبراني لجمع الملاحظات والمقترحات مع الحرص على تطوير الاستراتيجية من خلال إجراء تقييمات دورية، كما سيتم تعزيز التواصل مع الخبراء والمعنيين عبر عقد المؤتمرات الوطنية وورش العمل، وسيقوم المركز بمتابعة تنفيذ أهداف الاستراتيجية واتخاذ الإجراءات اللازمة والتصحيحية لضمان وضوح الأدوار وتعزيز المسؤولية.

وتعتمد الاستراتيجية الوطنية للأمن السيبراني على خمسة ركائز رئيسية تهدف إلى إنشاء فضاء إلكتروني آمن وموثوق في المملكة، تسعى الركيزة الاولى (المرونة السيبرانية المتقدمة) لحماية البنية التحتية الحيوية والمؤسسات الصغيرة والمتوسطة من خلال تعزيز الحماية والقدرات المتقدمة على اكتشاف التهديدات والاستجابة لها، وكما تدعم الركيزة الثانية (الحوكمة السيبرانية الفعّالة) مستوى الأمن السيبراني عبر سن التشريعات واللوائح التنظيمية وتنفيذ المعايير وأطر إدارة المخاطر وضمان الالتزام المستمر بها، أما الركيزة الثالثة (التعاون وتوسيع الشراكات) فتسهم في دعم التعاون المحلي والدولي لتبادل معلومات التهديدات والخبرات والمهارات وتعزيز الاستجابة المشتركة للتهديدات، وتساعد الركيزة الرابعة (ثقافة وكوادر سيبرانية مستدامة) على ترسيخ ثقافة الأمن السيبراني وبناء القدرات الوطنية من خلال برامج تدريبية موجهة، وتعمل الركيزة الخامسة (البحث والتطوير والابتكار) على خلق منظومة أمن سيبراني مستدامة من خلال الأبحاث والحلول المحلية بما يعزز تطوير الأنظمة ونمو الصناعة المحلية، وتم اعداد خطة عمل شاملة بما فيها من مبادرات استراتيجية لتنفيذ هذه الاستراتيجية لتحقيق الريادة وتمكين المملكة من الازدهار في بيئة رقمية موثوقة.

تدعم هذه الركائز الأمن السيبراني على مستوى المملكة من خلال المرونة والحوكمة الفعّالة والتعاون الاستراتيجي والكوادر المؤهلة الماهرة والابتكار.

03

التوسع الرقمي للمملكة

يشهد الفضاء الإلكتروني في المملكة توسعاً متسارعاً مدفوعاً بالتحول الرقمي المتنامي واعتماد التقنيات المتطورة مما يفتح آفاق للنمو والابتكار، وحرصت مملكة البحرين على تنفيذ العديد من الخطط والمبادرات الوطنية لدعم عملية التطور التقني مثل استراتيجية قطاع الاتصالات وتقنية المعلومات واستراتيجية الاقتصاد الرقمي والخطة الوطنية السادسة للاتصالات والاستراتيجية الوطنية للتجارة الإلكترونية وغيرها، والتي تهدف إلى تسريع وتيرة النمو للبنية الرقمية والاتصالات ودفع التنوع الاقتصادي لترسيخ مكانة المملكة كدولة رائدة في مجال التحول الرقمي.

كما أن لتحسين جودة خدمات الاتصالات والانترنت وضمان استدامة البنية التحتية الرقمية الوطنية دور محوري في هذا التطور التقني، حيث أسهم نشر شبكات الألياف البصرية عالية السرعة وتوسيع نطاق شبكات الجيل الخامس والتخطيط لتطبيق شبكات الجيل الخامس المتقدم والجيل السادس في بناء بيئة تقنية مترابطة تستفيد منها المؤسسات والأفراد، بالإضافة إلى جهود تعزيز الربط الدولي باستخدام الكابلات البحرية وانشاء وتطوير مراكز خدمات الحوسبة السحابية والتي دعمت موقع المملكة كمركز إقليمي للخدمات الرقمية.

وأسهمت المبادرات الوطنية بشكل فعّال في تعزيز تبني التقنيات المتقدمة، مما انعكس إيجاباً على رفع كفاءة وجودة الخدمات الرقمية، وعلى سبيل المثال، تطوير قطاع التجارة الإلكترونية من خلال تمكين المؤسسات الصغيرة والمتوسطة من الاستفادة المثلى من المنصات الرقمية، ومن جانب آخر، لعبت التقنيات المالية دوراً محورياً في إحداث نقلة نوعية في أساليب تقديم الخدمات المالية عبر تطوير حلول رقمية مبتكرة مكّنت الشركات والأفراد من الوصول إلى خدمات مالية تتسم بالكفاءة والموثوقية والأمان، وقد ساهم ذلك في إعادة تشكيل الفضاء الالكتروني وتعزيز التكامل الرقمي على المستوى الوطني.

القطاعات الحيوية الوطنية

04

تحديد القطاعات الحيوية الوطنية خطوة أساسية لتعزيز الحماية السيبرانية على هذه القطاعات وضمان استمرارية الخدمات الأساسية، حيث يشكل استهداف هذه القطاعات تهديداً مباشراً للأمن الوطني، وتعطّل هذه القطاعات قد يؤدي إلى خسائر فادحة في الأرواح واضطرابات في تقديم الخدمات الأساسية وانعكاسات اقتصادية واجتماعية سلبية واسعة النطاق.

الاستراتيجية الوطنية للأمن السيبراني (2021 – 2024) ضمت سبعة قطاعات ضمن القطاعات الحيوية، وهي: القطاع الحكومي، والقطاع المالي، قطاع الرعاية الصحية، قطاع المواصلات، قطاع تقنية المعلومات والاتصالات، وقطاع الغاز والكهرباء والنفط، وقطاع الصناعات المهمة.

وأثناء تطوير الاستراتيجية الوطنية للأمن السيبراني 2025–2028 تم دراسة القطاعات الحيوية لدى عدة دول وتحديد القطاعات الحيوية المحتملة، ومن ثم تقييم كل قطاع باستخدام أداة تحليل العوامل السياسية والاقتصادية والاجتماعية والتقنية والبشرية ، والذي نتج عنه تحديد ثمان قطاعات حيوية في مملكة البحرين وهي:

القطاعات الحيوية

القطاع الحكومي

القطاع الحكومي

يقدم القطاع الحكومي الخدمات العامة الحكومية في المملكة ويعزز الاستقرار الوطني من خلال إدارة المؤسسات الحكومية، وتقديم الخدمات الأساسية، وضمان استمرارية العمل الحكومي بكفاءة وأمان.

القطاع المالي

يُعتبر ركيزة للاقتصاد الوطني، حيث يشمل المؤسسات المصرفية والخدمات المالية الرقمية والنظام المصرفي والبنية التحتية للدفع الإلكتروني، ويمثل ضرورة لضمان استقرار الأسواق ويدعم الاقتصاد الرقمي.

قطاع تقنية المعلومات والاتصالات

المحرك الأساسي للتحول الرقمي، حيث يوفر البنية التحتية للاتصالات والخدمات الرقمية، ويربط مختلف القطاعات الحيوية عبر شبكات آمنة وموثوقة.

قطاع الطاقة والصناعات المهمة

يشمل حماية أنظمة شركات ومؤسسات الكهرباء والنفط والغاز والصناعات الأساسية، مما يضمن الاستقرار الاقتصادي والأمن الوطني، وقد يتسبب الهجمات السيبرانية على هذه الأنظمة إلى اضطرابات كبيرة تؤثر على إمدادات الطاقة وسلاسل التوريد.

قطاع الرعاية الصحية

يعتمد على الأنظمة الرقمية لإدارة المستشفيات وتقديم الرعاية الطبية والتعامل مع البيانات الصحية الحساسة، وأصبح تأمين هذا القطاع ضرورة لضمان استمرارية الخدمات الطبية وحماية خصوصية المرضى، وتعزيز قدرة المملكة على الاستجابة للأوبئة والطوارئ الصحية بفعّالية.

قطاع الإعلام

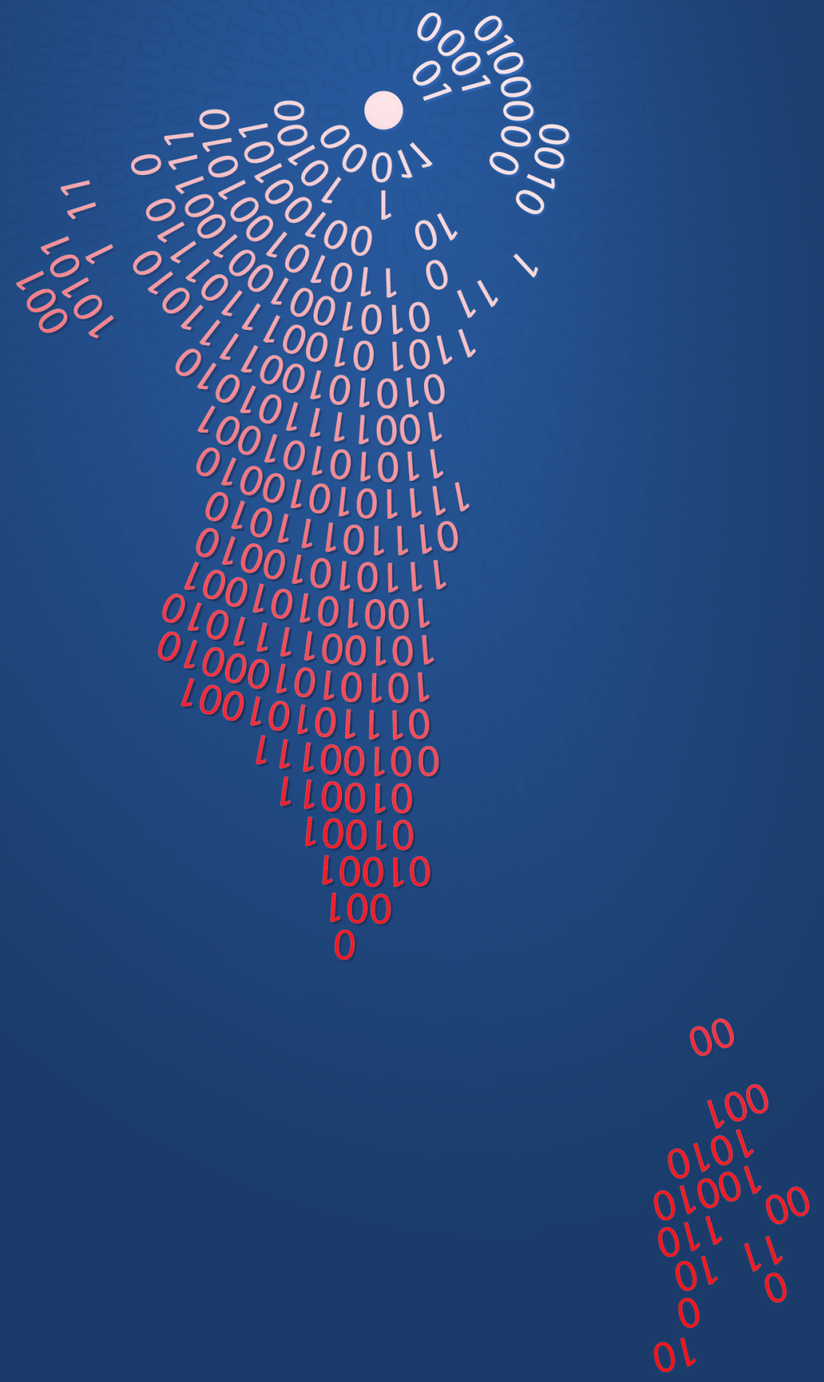
مسؤول عن نقل ونشر المعلومات بدقّة وتشكيل الرأي العام وتعزيز أمن منصات الإعلام الرقمي، والتركيز على تحسين جاهزية الأنظمة الإعلامية التي تؤثر على استقرار المجتمع وثقة الجمهور بالمصادر الرسمية.

قطاع المواصلات

يُسهل حركة الأفراد والسلع ويربط الأسواق المحلية والعالمية، ويدعم استدامة سلاسل التوريد، كما أن الاعتماد على الأنظمة والتقنيات في إدارة البنية التحتية الرقمية للموانئ والمطارات وشبكات النقل يوجب التأكد من استمرار الخدمات اللوجستية وعدم تعطلها.

قطاع التجارة والسياحة

يسهم في تحفيز ريادة الأعمال المحلية والأجنبية وجذب الاستثمارات وتعزيز التبادل التجاري على المستويين الإقليمي والدولي، كما يركز هذا القطاع على المرافق والفنادق والخدمات السياحة والتي لها دور في تنمية الاقتصاد الوطني.



الرؤية والرسالة

05

تعكس رؤية ورسالة الاستراتيجية الوطنية للأمن السيبراني إلتزام المملكة بتوفير فضاء رقمي آمن وموثوق ومرن يعزز الابتكار ويدعم النمو الرقمي، وتُجسّد الرؤية سعي المملكة في الريادة بمجال حماية الفضاء الإلكتروني، بما يتماشى مع أهدافها في مسيرتها التنموية.

الرؤية

الريادة في توفير فضاء إلكتروني آمن ومرن وموثوق، يقوده الابتكار ويعزز النمو الرقمي.

وتشمل الرسالة النهج الاستراتيجي لتحقيق الرؤية من خلال تعزيز المنظومة الرقمية باعتماد تدابير سيبرانية مبتكرة وتوفير حماية فعّالة، كما تُؤكد على أهمية حماية البنى التحتية الرقمية، وتمكين الصناعة ودعم نموها في مجال الأمن السيبراني، إلى جانب تعزيز الوعي المجتمعي بما يعزز الثقة العامة، وتشمل الرسالة أيضًا دعم الشراكات المحلية والدولية، والتصدي للتهديدات المستجدة، بما يسهم في رفع مستوى المرونة السيبرانية وتعزيز التنافسية العالمية.

الرسالة

تحقيق الريادة في مجال الأمن السيبراني لحماية البنية التحتية الرقمية من خلال دعم الابتكار وتوفير بيئة إلكترونية أمنة ومرنة وموثوقة تعزز النمو الوطني وترفع التنافسية العالمية لمملكة البحرين.

ركائز الاستراتيجية وأهدافها

06

ترتكز الاستراتيجية الوطنية للأمن السيبراني 2025 – 2028 على خمس ركائز استراتيجية أساسية، لكل منها أهداف ونتائج استراتيجية تدعم رؤية المملكة ورسالتها، وتشمل هذه الركائز المرونة السيبرانية المتقدمة، الحوكمة السيبرانية الفعّالة، التعاون وتوسيع الشراكات، ثقافة وكوادر سيبرانية مستدامة، والبحث والتطوير والابتكار.

ركائز الاستراتيجية الوطنية للأمن السيبراني

المرونة السيبرانية المتقدمة

الركيزة الأولى

الأهداف

01 تقوية الحماية السيبرانية للبنية التحتية الرقمية في مملكة البحرين
02 رفع القدرات الوطنية للتصدي للتهديدات السيبرانية
03 تعزيز إدارة الأزمات والاستجابة للحوادث السيبرانية

الحوكمة السيبرانية الفعّالة

الركيزة الثانية

الأهداف

01 دعم إصدار القوانين واللوائح التنظيمية السيبرانية
02 إدارة المخاطر السيبرانية على المستوى الوطني
03 التطوير بناءً على السياسات والمعايير الوطنية للأمن السيبراني
04 ضمان الالتزام المستمر لمعايير الأمن السيبراني

التعاون وتوسيع الشراكات

الركيزة الثالثة

الأهداف

01 تعزيز التعاون الوطني للأمن السيبراني
02 توسيع الشراكات الإقليمية والدولية

ثقافة وكوادر سيبرانية مستدامة

الركيزة الرابعة

الأهداف

01 توسيع نطاق الوعي الوطني بالأمن السيبراني
02 تطوير كوادر وطنية متخصصة في الأمن السيبراني

البحث والتطوير والابتكار

الركيزة الخامسة

الأهداف

01 تعزيز الكفاءات الوطنية في مجال البحث والتطوير والابتكار
02 الارتقاء بصناعة الأمن السيبراني

الركيزة
01

المرونة السيبرانية المتقدمة

الأهداف

01 تقوية الحماية السيبرانية للبنية التحتية الرقمية في مملكة البحرين

02 رفع القدرات الوطنية للتصدي للتهديدات السيبرانية

03 تعزيز إدارة الأزمات والاستجابة للحوادث السيبرانية

تعد المرونة السيبرانية عنصر أساسي لحماية النظام الرقمي في المملكة، حيث تضمن الاستدامة في استمرارية تقديم الخدمات والانظمة الحيوية مع الرصد والتصدي المستمر للتهديدات السيبرانية في ظل التطور والنمو السريع الذي تشهده المملكة، كما تُمكّن المملكة من الازدهار في بيئة رقمية مترابطة عن طريق تعزيز الحماية السيبرانية الرقمية وبناء الثقة ودعم الاستقرار الاقتصادي الوطني، ولتحقيق المرونة السيبرانية تسعى المملكة إلى توحيد الجهود الوطنية لحماية البنية التحتية الرقمية وتمكين قدرات التصدي للتهديدات وتعزيز إدارة الازمات وقدرات الاستجابة للحوادث السيبرانية.

الهدف الأول

تقوية الحماية السيبرانية للبنية التحتية الرقمية في مملكة البحرين

يؤكد تزايد الاعتماد على البنية التحتية الرقمية على أهمية تنفيذ تدابير أمن سيبراني قوية لحمايتها، لذلك ينبغي زيادة الجهود لحماية مؤسسات الحيوية وتوسيع النطاق ليشمل المؤسسات الصغيرة والمتوسطة نظراً لمحدودية الموارد لديها، مما يتطلب تدابير أمنية وخدمات مخصصة لتعزيز قدراتها السيبرانية، حيث يعد ضمان حماية الخدمات الحيوية والأنشطة الاقتصادية أساساً لزيادة قدرتها على التصدي للتهديدات السيبرانية.

وسيتم اعتماد نهجاً متعدد المستويات لتعزيز نطاق الحماية والذي يتضمن تنفيذ الأطر والمعايير وأفضل الممارسات الخاصة بالأمن السيبراني، والذي تم إعدادها وفقاً لمتطلبات القطاعات الحيوية والمؤسسات الصغيرة والمتوسطة، كما يتضمن تعزيز الحماية وتحسين الاستجابة للتهديدات السيبرانية ورفع كفاءتها في القطاعات الحيوية، وتعزيز التواصل بين القطاعات الحيوية لتطوير القدرات لمواجهة التهديدات السيبرانية على نطاق واسع.

الهدف الثاني

رفع القدرات الوطنية للتصدي للتهديدات السيبرانية

تشكل التطورات المستمرة للتهديدات السيبرانية مخاطر تؤثر على استمرارية الخدمات الحيوية واستقرار البنية التحتية الرقمية، والتي تعتمد على استخدام التقنيات المتقدمة من قبل المخترقين، لذلك تسعى المملكة إلى تعزيز القدرات التشغيلية والمعلوماتية والتقنية لرصد التهديدات والتصدي والاستجابة لها لتأمين البنية التحتية الوطنية، كما أن من الضروري التعاون بين الجهات المعنية وأصحاب المصلحة وجهات القطاعات الحيوي لاتّباع آلية لتبادل المعلومات المتعلقة بالتهديدات على المستويين الوطني والقطاعات الحيوية.

تعتمد هذه الآلية على تطوير منصة متخصصة لتبادل معلومات التهديدات بشكل مستمر، حيث توفر المنصة معلومات دقيقة ومحدثة حول التهديدات بين القطاعات الحيوية، بالإضافة إلى تبادل المعلومات بين الجهات التابعة لكل قطاع، مما يسهم في الكشف عن التهديدات والوقاية منها، كما أن دمج التقنيات المتقدمة مثل الذكاء الاصطناعي والتعلّم الآلي في عمليات كشف التهديدات والاستجابة لها، مما يساهم في تعزيز الحماية الاستباقية للبنية التحتية الرقمية الوطنية وترسيخ الثقة في جاهزيتها السيبرانية.

الهدف الثالث

تعزيز إدارة الأزمات والاستجابة للحوادث السيبرانية

تُعد إدارة الأزمات والاستجابة للحوادث السيبرانية أمراً أساسياً للحفاظ على مرونة البنية التحتية الرقمية نظراً للأضرار التي تسببها الهجمات السيبرانية بما في ذلك الحوادث الجيوسياسية، لذلك تسعى المملكة إلى وضع خطط واستراتيجيات وآليات شاملة لإدارة الأزمات والاستجابة للحوادث لضمان استمرارية الأعمال وقدرتها على التعافي بشكل فعّال من الكوارث السيبرانية، كما يجب التنسيق لهذه الخطط مع القطاعات الحيوية لاحتواء الهجمات السيبرانية والتخفيف من آثارها وضمان التحسين المستمر لقدرات الاستجابة.

وسيتم تطوير خطط الاستجابة للأزمات والحوادث السيبرانية على المستوى الوطني وللقطاعات الحيوية واختبارها بشكل منتظم لضمان جاهزيتها، بما في ذلك تحديد مستويات الهجمات السيبرانية والسيناريوهات المحتملة وإجراءات الإبلاغ عنها، كما تعتبر التمارين السيبرانية أداة لتعزيز التنسيق بين الجهات المعنية ورفع مستوى الجاهزية الجماعية، وسيتم توظيف التقنيات المتقدمة لاكتشاف الأزمات وتحليل التهديدات، مما يضمن تصنيفاً دقيقاً للحوادث واتخاذ التدابير اللازمة، بالإضافة إلى استخدام الدروس المستفادة من الحوادث السابقة لتحديث السياسات والإجراءات الأمنية، والأخذ في الاعتبار أفضل الممارسات الدولية لتسريع جهود التصدي للتهديدات السيبرانية وبناء بيئة رقمية أكثر أماناً واستدامة.

الركيزة
02

الحوكمة السيبرانية الفعّالة

الأهداف

01 دعم إصدار القوانين واللوائح التنظيمية السيبرانية

02 إدارة المخاطر السيبرانية على المستوى الوطني

03 التطوير بناء على السياسات والمعايير الوطنية للأمن السيبراني

04 ضمان الالتزام المستمر لمعايير الأمن السيبراني

تستند هذه الركيزة على إرساء نهج موحد واستباقي لحماية البنية التحتية الرقمية في مملكة البحرين، وتُعد الحوكمة الفعّالة عنصراً أساسياً في التقليل من المخاطر السيبرانية وضمان الحماية وتعزيز الثقة في الفضاء الإلكتروني، وتهدف هذه الركيزة إلى تطوير وتنفيذ إطار حوكمة متكامل للأمن السيبراني يستند إلى أفضل الممارسات الدولية وإصدار القوانين واللاوائح التنظيمية السيبرانية، كما يسعى إلى تمكين آليات لوضع السياسات والمتابعة المستمرة للالتزام وإدارة المخاطر بفعّالية.

الهدف الأول

دعم إصدار القوانين واللوائح التنظيمية السيبرانية

يُعد وجود إطار قانوني وتنظيمي أساساً لحوكمة الأمن السيبراني حيث يضع معايير واضحة للمساءلة ويحدد الأدوار والمسؤوليات ويوجه التنسيق بين القطاعات لحماية المصالح الوطنية، كما يسهم إنفاذ القوانين السيبرانية في توحيد الممارسات السيبرانية وتعزيز الالتزام للسياسات والضوابط.

إن بناء بيئة إلكترونية آمنة يتطلب سن لوائح تنظيمية مرنة قابلة للتكيف مع التهديدات، ويتطلب مراجعة دورية للتأكد من مواءمتها للمخاطر الناشئة والتطورات التقنية ومواكبتها أفضل الممارسات الدولية، مما يضمن جاهزية منظومة الأمن السيبراني ويُعزز قدرة المملكة للاستجابة بفعّالية للتحديات السيبرانية المتنامية.

الهدف الثاني

إدارة المخاطر السيبرانية على المستوى الوطني

تتطلب إدارة المخاطر السيبرانية على المستوى الوطني بناء ثقافة الوعي بالمخاطر لتمكين الجهات من تحديد التهديدات الناشئة وتقييمها والتخفيف من آثارها بطرق استباقية، مع الالتزام بأطر موحدة لإدارة المخاطر، وتسعى المملكة إلى تبني منهجية تعتمد على تحديد الأولويات استناداً إلى المخاطر السيبرانية، مما يوجه الموارد والجهود نحو المجالات الأكثر أهمية في حماية الأصول الرقمية.

وسيمثل الإطار الوطني لإدارة المخاطر السيبرانية المرجع الأساسي لإدارة المخاطر في الجهات، مستنداً إلى أفضل الممارسات والمنهجيات العالمية، مثل إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا وضوابط مركز أمن الإنترنت والمعايير الصادرة عن المنظمة الدولية للمعايير، ويوفر هذا الإطار آلية متكاملة لتمكين الجهات من تحديد الأصول الرقمية وتحليل التهديدات وتقييم المخاطر ووضع الآليات للحد منها.

الهدف الثالث

التطوير بناءً على السياسات والمعايير الوطنية للأمن السيبراني

وجود فضاء إلكتروني آمن يُحتم إنشاء سياسات ومعايير سيبرانية تحمي الأصول الرقمية لدى الجهات في القطاعات الحيوية، وينبغي أن تكون السياسات والمعايير شاملة تتناول المتطلبات الخاصة بكل قطاع بالإضافة إلى المتطلبات المتعلقة بالتقنيات الناشئة مثل أمن سلاسلة التوريد ومبدأ الأمن عبر مراحل التصميم والذكاء الاصطناعي وإنترنت الأشياء والحوسبة الكمية، علاوة على ذلك سيتم وضع آلية مراجعة مستمرة تضمن تحسين وتطوير السياسات والمعايير باستمرار لضمان التحسين الدائم.

وسيتم تشجيع الجهات على تبني المعايير والسياسات الأمنية بشكل تدريجي، مع الأخذ بعين الاعتبار التحديات المحتملة بما يضمن رفع مستوى الأمان السيبراني بطريقة منظمة، ويشمل أيضاً ضمان جودة خدمات الأمن السيبراني في المملكة لتعزيز الثقة في البنية التحتية الرقمية في المملكة، عن طريق تطوير آلية لترخيص مزودي خدمات الأمن السيبراني لضمان تنفيذ الضوابط الأمنية وضمان كفاءة الخدمات المقدمة.

الهدف الرابع

ضمان الالتزام المستمر لمعايير الأمن السيبراني

يُعد الالتزام بمعايير الأمن السيبراني عملية مستمرة تسهم في تعزيز وضع الأمن السيبراني للمملكة وتوفير الحماية للقطاعات الحيوية، مما يقلل من فرص استغلال الثغرات والبقاء على استعداد لمواجهة التهديدات المتغيرة، وتتطلب هذه العملية إجراء تقييمات دورية للالتزام تساهم في بناء ثقافة وعي متنامية لدى الجهات، وتعمل على رفع مستوى الجاهزية الأمنية وضمان استمرارية الأعمال في مواجهة المخاطر المحتملة.

وسيتم إنشاء إطار عمل لضمان الالتزام بالمعايير يهدف إلى تقييم الجهات من خلال إجراء عمليات تدقيق دورية وتطوير آليات للإبلاغ عن المخالفات، بالإضافة إلى تحديد جزاءات وإجراءات تصحيحية واضحة للتعامل مع حالات عدم الالتزام.

"
بالحوكمة
نحمي الحاضر
ونقود المستقبل

الركيزة
03

التعاون وتوسيع الشراكات

الأهداف

01 تعزيز التعاون الوطني للأمن السيبراني

02 توسيع الشراكات الإقليمية والدولية

إن توحيد الجهود الوطنية والإقليمية والدولية يُعد أساساً لتعزيز الأمن السيبراني في العالم الرقمي المترابط حيث تكون التهديدات السيبرانية جزءاً منه، ويُسهم التعاون وتوسيع الشراكات في تحقيق حماية سيبرانية مشتركة من خلال عملية تبادل المعلومات والمعارف والتجارب، كما تدعم الشراكات الدولية تنمية القدرات من خلال المشاركة في التمارين والمؤتمرات السيبرانية وتبادل المعارف، وبذلك تُسهم الجهود الموحّدة إلى تحسين الجاهزية السيبرانية واكتشاف التهديدات والاستجابة لها والتعافي منها مما يرسخ بيئة إلكترونية آمنة.

الهدف الأول

تعزيز التعاون الوطني للأمن السيبراني

يسهم تعزيز آليات التعاون الوطني بشكل مباشر في رفع كفاءة الحماية السيبرانية الوطنية، حيث يؤدي تطوير أطر للتعاون إلى تبادل المعلومات والاستفادة من الخبرات عبر القطاعات الحيوية، ويقوم الإطار إيضاً إلى تحسين الاستجابة للحوادث السيبرانية وتقوية الحماية المشتركة وترسيخ خطط موحدة لتعزيز الجاهزية والاستباقية.

وسيتم إعداد إطار عمل موحد لتعزيز التواصل بين الجهات المختلفة في المملكة، وسيحدد الإطار الأدوار والبروتوكولات والإجراءات اللازمة للتعاون الفعّال، وسيشمل نطاق الإطار تبادل الخبرات والمعرفة وتنفيذ برامج الأمن السيبراني، كما سيتم إعداد آلية تواصل لتسهيل إجراءات الإبلاغ عن الحوادث السيبرانية والتنبيه المستمر بشأن تحديثات التهديدات، بما يعزز سرعة الاستجابة وفعاليتها بين الجهات المعنية، وسيسهم هذا الإطار في تعزيز استراتيجيات الحماية المتقدمة وبناء منظومة أمن سيبراني قادرة على مواجهة التهديدات الحالية والمستقبلية بمرونة.

الهدف الثاني

توسيع الشراكات الإقليمية والدولية

في ظل تزايد وتعدد مصادر التهديدات السيبرانية على المستوى العالمي، يُعد تعزيز الشراكات الدولية والإقليمية في مجال الأمن السيبراني ضرورة لضمان الحماية والاستجابة للمخاطر المتطورة، ويسهم التعاون الإقليمي والدولي من خلال الاتفاقيات الثنائية ومتعددة الأطراف في تطوير نهج استباقي لمعرفة المستجدات الناشئة والتطورات التقنية والتهديدات السيبرانية.

وتُوفر هذه الشراكات فرصاً لتبادل المعرفة ومشاركة الخبرات وتنسيق الموارد مع الجهات والمنظمات الدولية، مما يرفع من كفاءة التصدي للتحديات السيبرانية وبناء القدرات الوطنية، وذلك من خلال البرامج التدريبية والمشاريع التعاونية التي تساعد في تطوير الكفاءات، وتسهم المشاركة في التمارين السيبرانية الإقليمية والدولية في رفع مستوى الجاهزية السيبرانية وتعزيز القدرة على الاستجابة للتهديدات، كما أن المشاركة في المؤتمرات العالمية للأمن السيبراني تضمن توافق الاستراتيجيات الوطنية مع أفضل الممارسات الدولية.

"
معاً نحقق
الحماية والأمان

الركيزة
04

ثقافة وكوادر سيبرانية مستدامة

الأهداف

01 توسيع نطاق الوعي الوطني بالأمن السيبراني

02 تطوير كوادر وطنية متخصصة في الأمن السيبراني

تحقيق الحماية للفضاء الإلكتروني لمملكة البحرين يتطلب مجتمع واعي وكوادر مزودة بالمهارات اللازمة لحماية البنية التحتية والأصول الرقمية، وتعزيز الوعي الوطني يتطلب تزويد الأفراد والمؤسسات بالمعرفة اللازمة مما يجعلهم خط الدفاع الأول ضد الهجمات، وذلك من خلال الحملات والبرامج التوعوية والتدريبية التي تشجع على تبني الممارسات الآمنة مما يعزز الثقة في الخدمات التقنيات الرقمية.

ومع تزايد الاعتماد على التقنيات الحديثة، أصبح من الضروري بناء كوادر متخصصة في الأمن السيبراني، مما يضمن الاستفادة من التحول الرقمي مع ضمان بيئة رقمية آمنة قادرة على مواجهة التحديات، وسيتم تطوير كوادر الأمن السيبراني بإدخال مفاهيم الأمن السيبراني إلى المناهج التعليمية وإطلاق مبادرات تهدف إلى تنمية المهارات من خلال البرامج التدريبية وتشجيع الحصول على شهادات الاحترافية الدولية.

الهدف الأول

توسيع نطاق الوعي الوطني بالأمن السيبراني

يُعد رفع وعي الأفراد والمؤسسات بالأمن السيبراني ضرورة لتعزيز الحماية والمرونة الرقمية في مملكة البحرين، كما يُعد هذا استثماراً يهدف إلى بناء مجتمع واعٍ وقادر على مواجهة التحديات الرقمية، وتسعى المملكة إلى تضمين مبادرات التوعية لجميع فئات المجتمع، بدءاً من الأفراد وصولاً إلى المؤسسات الصغيرة والمتوسطة والجهات التابعة للقطاعات الحيوية، وستتضمن هذه المبادرات برامج توعية مخصصة لكل قطاع يتم تنفيذها بالتعاون مع منظمي القطاعات والجهات والمجتمع المدني، مما يضمن انتشار ثقافة الأمن السيبراني في جميع أنحاء المملكة.

ولتحقيق ذلك، سيتم استخدام قنوات اتصال متنوعة لتعزيز التواصل الفعّال بين جميع الأطراف المستهدفة، كما ستوفر المنصات التعليمية معلومات قيمة حول المخاطر السيبرانية وأفضل الممارسات، مما يسهم في بناء فهم أعمق للأمن السيبراني.

الهدف الثاني

تطوير كوادر وطنية متخصصة في الأمن السيبراني

يُعد بناء كوادر وطنية قادرة على التطور أمراً ضرورياً لمواجهة المخاطر السيبرانية المتزايد وضمان تحول رقمي آمن، ويسهم تطوير الخبرات في تعزيز حماية البنية التحتية الرقمية ودعم النمو الاقتصادي، مما يرسخ مكانة المملكة في الريادة في هذا المجال.

وسيتم تطوير الكوادر والقدرات الوطنية من خلال عدة مبادرات، تشمل إدراج مفاهيم الأمن السيبراني في المناهج التعليمية على جميع المستويات بدءاً من الطفولة المبكرة وصولاً إلى التعليم العالي، وذلك بالتعاون مع المؤسسات التعليمية والأكاديمية لإعداد كوادر المستقبل، بالإضافة إلى ذلك سيتم رفع مهارات متخصصي الأمن السيبراني وتقنية المعلومات من خلال برامج تدريبية شاملة تتضمن مستويات متدرجة، مما يسهم في تطوير القدرات واكتساب الخبرة المطلوبة، كما ستحظى جهود تمكين المرأة من خلال برامج تدريبية تعزز مساهمتها في مجال الأمن السيبراني.

علاوة على ذلك، سيتم التعاون مع المؤسسات الأكاديمية والجهات المعنية بالأمن السيبراني لتنظيم ورش العمل والمؤتمرات وتوفير فرص للتواصل وتبادل المعرفة، إن تطوير الكوادر والمتخصصين يعزز من القدرات الوطنية في مجال الأمن السيبراني.

"

بالمعرفة تنمو المهارات
ويرتقي الأمن السيبراني

الركيزة
05

البحث والتطوير والابتكار

الأهداف

01 تعزيز الكفاءات الوطنية في مجال البحث والتطوير والابتكار

02 الارتقاء بصناعة الأمن السيبراني

تهدف هذه الركيزة إلى تشجيع البحث والتطوير والابتكار مما يعزز من تطوير الصناعة في مجال الأمن السيبراني بالمملكة، وذلك من خلال التعاون بين القطاعات الحيوية والتعليمية والأكاديمية والبحثية، حيث يتم التركيز على تحديد التحديات السيبرانية وتعزيز قدرات الحماية ودعم نمو الصناعة من خلال المبادرات الوطنية، وتسعى المملكة إلى تكوين منظومة مرنة ومبتكرة قادرة على المنافسة في مجال الأمن السيبراني، من خلال دعم الشركات الناشئة وتنمية مهارات الكوادر الوطنية وتشجيع المنتجات السيبرانية المحلية.

الهدف الأول

تعزيز الكفاءات الوطنية في مجال البحث والتطوير والابتكار

يعد تشجيع البحث والتطوير والابتكار في مجال الأمن السيبراني ضرورة لمواجهة التحديات الحالية في هذا المجال وتقليل الاعتماد على الجهات الخارجية لحماية البنية التحتية الوطنية، ويتطلب ذلك وضع خطط للبحث والتطوير والابتكار على المستوى الوطني بالتعاون مع الجهات المعنية، حيث سيتم تنفيذ هذه الخطط لتحديد التحديات السيبرانية الناشئة ووضع الأولويات السيبرانية.

وتشمل هذه الخطط الأنشطة والمسابقات والبرامج المتعلقة بالبحث والتطوير والابتكار مثل الجلسات الحوارية والمؤتمرات البحثية والهاكاثونات، كما ستشجع هذه الخطط على المشاركة الفعّالة من قبل المنظمات والشركات والهيئات الأكاديمية للعمل على تطوير حلول بحثية وعملية لمواجهة تحديات الأمن السيبراني.

الهدف الثاني

الارتقاء بصناعة الأمن السيبراني

تسعى المملكة إلى تنمية صناعة الأمن السيبراني من خلال دعم الشركات الناشئة وابتكار تقنيات جديدة وتعزيز تنوع الكفاءات، حيث يسهم تطوير الصناعة المحلية للأمن السيبراني في زيادة الثقة العامة في المنصات الرقمية وبناء منظومة آمنة وتحقيق بيئة جاذبة للاستثمارات الدولية تدعم الاقتصاد الوطني.

سيتم تشجيع الشركات الناشئة وأصحاب المصلحة المعنيين بما في ذلك الشركاء والمستثمرون والعملاء على التعاون والتواصل من خلال المؤتمرات والفعاليات، حيث يسهم هذا التعاون في تبادل المعرفة وأفضل الممارسات وبناء الثقة والسمعة للشركات الناشئة ورفع الوعي بمتطلبات صناعة الأمن السيبراني، بالإضافة إلى تشجيع اعتماد المنتجات والخدمات السيبرانية المحلية كأولوية لتعزيز السوق المحلي.

"

الابتكار يبني فضاءً إلكترونياً آمناً

الخاتمة

07

تضع الاستراتيجية الوطنية للأمن السيبراني لمملكة البحرين 2025-2028 نهجاً شاملاً ومتطلعاً نحو حماية النظام الرقمي في المملكة، حيث يُعد الأمن السيبراني أولوية وطنية خاصةً في ظل تنفيذ المبادرات المتعلقة بالتحول الرقمي وتبنّي التقنيات المتقدمة، وبذلك تضمن الاستراتيجية حماية القطاعات الحيوية الوطنية وتساهم في تأمين الاستقرار الاقتصادي وتعزيز الثقة العامة في الفضاء الالكتروني للمملكة، وتم إعداد هذه الاستراتيجية استكمالاً لما تم انجازه من مبادرات الاستراتيجية السابقة مع الاخذ بعين الاعتبار آليات التصدي للتهديدات السيبرانية المتقدمة والمستمرة وبالتوافق مع أفضل الممارسات العالمية.

وتعتمد الاستراتيجية على خمس ركائز أساسية لضمان تعزيز الريادة في توفير بيئة الكترونية آمنة ومرنة وموثوقة في مملكة البحرين، حيث تهدف الركيزة الأولى لتقوية حماية البنية التحتية الرقمية الوطنية والتصدي للتهديدات السيبرانية، مما يضمن جاهزية القطاعات الحيوية والمؤسسات الصغيرة والمتوسطة بإجراءات أمان قوية، وتسعى الركيزة الثانية لوضع أساساً قانونياً وتنظيمياً وتطوير وتنفيذ السياسات والمعايير ولضمان الالتزام بها وتنفيذ أطار إدارة المخاطر، وتهدف الركيزة الثالثة إلى توطيد التعاون والشراكات الوطنية والإقليمية والدولية لرفع مستوى الأمن السيبراني، كما أن الركيزة الرابعة تسعى إلى رفع مستوى الوعي في مجال الأمن السيبراني وتطوير الكوادر الوطنية، واهتمت الركيزة الخامسة بتشجيع التقدم في مجال الأمن السيبراني ونمو الصناعة عن طريق التركيز على البحث والتطوير والابتكار.

وتسعى الاستراتيجية إلى التصدى للتحديات السيبرانية الراهنة والمستقبلية، بما يضمن قدرة المملكة على مواكبة التطورات التقنية، كما تهدف إلى خلق بيئة إلكترونية آمنة ومبتكرة تدعم الأولويات الوطنية وتعزز التنافسية العالمية للمملكة.

ncscbh

ncsc_bh

www.ncsc.gov.bh