الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

مشروع إرشادات الأمن السيبراني للمدن الذكية

Cybersecurity Guidelines for Smart Cities

(CGSC – 1: 2024)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP)

يستخدم هذا البروتوكول على نطاق واسع في العالم. وهناك أربعة ألوان (إشارات ضوئية)

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

قائمة الأشكال

قائمة الجداول

الملخص التنفيذي

الهيئة الوطنية للأمن السيبراني هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية؛ وذلك وفقًا لتنظيمها الصادر بموجب الأمر الملكي الكريم ذي الرقم (٦٨٠١) والتاريخ ١٤٣٩/٢/١١ هـ.

وقامت الهيئة الوطنية للأمن السيبراني بإعداد إرشادات الأمن السيبراني للمدن الذكية (CGSC – 1: 2024)، مستهدفة بذلك صناع القرار، وشركاء منظومة المدن الذكية في جميع أنحاء المملكة. وتهدف هذه الإرشادات إلى تقليل مخاطر الأمن السيبراني التي تواجهها المدن الذكية ومن ثم توفير أفضل الممارسات للتخفيف من هذه المخاطر السيبرانية.

تعتمد المدن الذكية على بنية معقدة ومترابطة تضم مكونات مختلفة، مثل أجهزة إنترنت الأشياء، والمنصات السحابية، وأدوات تحليل البيانات؛ لتعزيز الإدارة الحديثة، وجودة الحياة. ويمر تطوير المدن الذكية في دورة حياة كاملة؛ تتضمن التخطيط، والتصميم، والتنفيذ، والتشغيل، والتحسين المستمر؛ مما يضمن مواكبة التقدم التقني، ومعالجة مخاطر الأمن السيبراني. كما يؤدي أصحاب المصلحة في كامل المنظومة أدواراً محورية في حوكمة المدن الذكية وتطويرها وتشغيلها الآمن.

وتغطي هذه الإرشادات؛ أربع مكونات رئيسية، هي: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني المتعلق بالأطراف الخارجية، والحوسبة السحابية.

يُعنى مكون حوكمة الأمن السيبراني بضمان كون الإستراتيجية، والرؤية، وخارطة الطريق، والأهداف للمدينة الذكية؛ تضع في حسبانها الأمن السيبراني لسكان المدن الذكية وشركاء منظومتها. ويشمل ذلك الالتزام بالتنظيمات والتشريعات ذات العلاقة بالمدن الذكية. ويعنى هذا المكون كذلك؛ بتوثيق سياسات الأمن السيبراني وإجراءاته ذات العلاقة بالمدن الذكية وتطبيقها بالإضافة إلى ضمان تحديد أدوار الأمن السيبراني للمدن الذكية، لجميع الأطراف المعنية داخل الجهة؛ ضمن هيكلية الحوكمة. ويبين هذا المكون أيضاً الإرشادات التي يوصى بتطبيقها، فيما يخص إدارة مخاطر الأمن السيبراني للمدن الذكية، كما يضمن إدراج متطلبات الأمن السيبراني للمدن الذكية في دورة حياة إدارة المشاريع المعلوماتية والتقنية.

فيما يخص مكون تعزيز الأمن السيبراني؛ فإنه يُعنى بضمان تطبيق آليات الأمن السيبراني الملائمة لمنظومة المدن الذكية، من أجل حماية المعلومات وأصولها ضد الهجمات السيبرانية. في حين يُعنى مكون صمود الأمن السيبراني بتعزيز قدرة المدنية الذكية على الصمود أمام الآثار، التي قد تطرأ بسبب الحوادث المتعلقة بالأمن السيبراني للمدن الذكية.

ويُعنى مكون الأمن السيبراني المتعلق بالأطراف الخارجية، والحوسبة السحابية، بتلبية الاحتياج للإدارة الفعالة لمخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية التي تعمل على دعم عمليات المدن الذكية؛ بما في ذلك المخاطر المرتبطة بخدمات الحوسبة السحابية.

المقدمة

تعتمد المدن الذكية على التقنيات الرقمية، وأدوات التحليل، وإنترنت الأشياء؛ لتوفير الخدمات التي تعمل على تحسين جودة الحياة في المدينة، والازدهار الاقتصادي، والاستدامة البيئية، وتعزيز فعالية الإدارة الحكومية. ويتسق هذا التعريف مع تعاريف الجهات العالمية الأخرى، التي أبرزت أن المدن الذكية، تمثل تقاطع بين تقنية المعلومات والاتصالات والتقنية التشغيلية، مع البنية التحتية المادية.

حرصت رؤية المملكة العربية السعودية ٢٠٣٠ وبرامج تحقيق الرؤية بشكل كبير على المدن الذكية، وحددت أهدافًا متعلقة باستخدام التقنية لإنشاء مناطق حضرية، وصالحة للعيش بكفاءة واستدامة أعلى. وقد أدى ذلك إلى زيادة في النمو، وفي أعمال التطوير في مشاريع المدن الذكية ومبادراتها بأشكالها المختلفة.

يعنى الهدف الإستراتيجي للمدن الذكية باستخدام أجهزة الاستشعار، وأجهزة إنترنت الأشياء وغيرها من تقنيات جمع البيانات؛ بهدف جمع البيانات في الوقت الفعلي، وتحليلها أيضًا. وبعد ذلك، يجري الاعتماد على هذه البيانات؛ لتحسين أداء الخدمات والبنية التحتية في المدينة، بالإضافة إلى تحديد مجالات التحسين اللازمة، ورفع مستوى العيش في المدينة.

أمّا الهدف الرئيسي من المدن الذكية، فيتمثّل في خلق بيئة حضرية مستدامة وفعّالة، تضمن حياةً عالية الجودة وتعزز مشاركة المستفيدين، مع تقليل استهلاك الموارد، والحدّ من الأثر البيئي السلبي المنعكس من هذه الموارد. وعلى هذا فإن الاعتماد المتزايد على تقنية المعلومات والاتصالات يجعل المدن الذكية أكثر عرضة لمخاطر الأمن السيبراني.

وبناءً على ذلك؛ قامت الهيئة الوطنية للأمن السيبراني بتطوير إرشادات الأمن السيبراني للمدن الذكية (CGSC – 1: 2024). وذلك بعد إجراء دراسة شاملة لعدة إرشادات، ومعايير، وأطر، وضوابط عالمية؛ تتعلق بالأمن السيبراني للمدن الذكية، وكذلك تحليل الوضع الراهن للمبادرات الوطنية والإحصاءات؛ والمتطلبات التشريعية، والتنظيمية ذات العلاقة، ومراجعة أفضل الممارسات في مجال الأمن السيبراني؛ للاستفادة منها، وتحليل حوادث وهجمات الأمن السيبراني السابقة. وجرى تطوير هذه الوثيقة، لتقديم التوجيه الأساسي لأصحاب القرار في المدن الذكية وشركاء المنظومة. والغرض من ذلك هو تحديد الإستراتيجيات، والممارسات الفعالة؛ للتخفيف من مخاطر الأمن السيبراني، وضمان النمو الصامد والتشغيل الآمن للمدن الذكية.

تتكون إرشادات الأمن السيبراني للمدن الذكية من:

- (٤) مكونات رئيسية (Main Domains).
- (١٤) مكونًا فرعياً (Subdomains).
- (٧١) إرشادًا (Guidelines).

الأهداف

تهدف هذه الوثيقة إلى تقديم إرشادات يكون الغرض منها، تضمين أفضل ممارسات الأمن السيبراني في تطوير المدن الذكية وإدارتها.

ومع تزايد الاعتماد على التقنيات المترابطة؛ قد تظهر مخاطر الأمن السيبراني المحتملة، داخل منظومة المدينة الذكية. ولذلك، يوصى بتضمين متطلبات الأمن السيبراني باستمرار، في حوكمة المدن الذكية، وتطويرها وصيانتها وإدارتها وتشغيلها؛ لضمان حماية مصالح الجهات المعنية في منظومة المدينة الذكية.

تهدف الإرشادات الواردة في هذه الوثيقة، إلى تحقيق العديد من الأهداف الرئيسية، الضرورية للتشغيل الآمن والصامد للمدن الذكية:

- تضمين الأمن السيبراني، خلال مراحل تطوير المدن الذكية؛ لمواجهة التهديدات السيبرانية.
- توجيه وإرشاد أصحاب المصلحة في المدن الذكية، لإدارة مخاطر الأمن السيبراني.
- تعزيز الوعي بالأمن السيبراني، بين جميع أصحاب المصلحة في المدن الذكية؛ بما في ذلك التشريعات الوطنية للأمن السيبراني ذات العلاقة.
- تعزيز تبني أفضل ممارسات الأمن السيبراني، في تصميم وتشغيل المدن الذكية.
- تعزيز التكيف المستمر، مع التهديدات الناشئة والتغيرات التقنية.

نطاق العمل وقابلية التطبيق

تستهدف الإرشادات في المقام الأول صناع القرار في المدن الذكية، في كل من القطاعين العام والخاص، في المملكة العربية السعودية. ويشمل مصطلح صناع القرار في المدن الذكية؛ جميع الأفراد والجهات، المكلفين بالإشراف على المدن الذكية وإدارتها. وتستهدف هذه الإرشادات أيضاً شركاء المنظومة؛ بما في ذلك رؤساء إدارة الأمن السيبراني، وخبراء الأمن السيبراني ومهندسيه وغيرهم من الأشخاص الذين يشاركون في تخطيط المدن الذكية، وتصميمها، وتنفيذها، وتشغيلها.

هذه الإرشادات مخصصة للتوعية؛ وتهدف إلى المساعدة في تعزيز الأمن السيبراني للمدن الذكية، بهدف ضمان تطبيق أفضل الممارسات؛ للحد من مخاطر الأمن السيبراني، وزيادة الصمود في مواجهة الهجمات السيبرانية.

ونظراً للطبيعة المتغيرة للتهديدات السيبرانية؛ تحث الهيئة الوطنية للأمن السيبراني، صناع القرار في المدن الذكية، وشركاء المنظومة على مراجعة المخاطر السيبرانية وتقييمها بشكل دوري؛ لتحديد الحاجة إلى اتخاذ تدابير إضافية فيما يتعلق بالأمن السيبراني للمدن الذكية.

أسس المدن الذكية

أصحاب المصلحة

تعد المدن الذكية؛ هي نتيجة للجهود التعاونية بين مجموعات مختلفة من أصحاب المصلحة؛ حيث يسهم كل منهم بخبرات وموارد فريدة. تشمل المجموعات الأساسية ما يلي:

- **الجهات التنظيمية:** هي الجهات المسؤولة عن إنشاء، السياسات والتنظيمات وتطويرها ونشرها وتنفيذها. وهي السياسات التي تؤثر على تطوير المدن الذكية وتشغيلها. وتتمثل مهماتها دورها في ضمان عمل المدن الذكية ضمن إطار قانوني وتنظيمي؛ يعزز الأمن، والسلامة، والخصوصية، والكفاءة.

- **أصحاب القرار في المدن الذكية:** تشمل هذه الفئة جميع الأفراد والجهات، ممن لديهم الصلاحيات اللازمة لاتخاذ القرار، والمكلفين بالإشراف على المدن الذكية وإدارتها. تتولى هذه الفئة تحديد التوجه الإستراتيجي، والأهداف والسياسات، التي تقود النمو والتطور في التقنية، والبنية التحتية للمدن الذكية.

- **شركاء المنظومة:** تندرج تحت هذه المظلة الواسعة، جميع الجهات المشاركة بشكل مباشر في تخطيط المدن الذكية، وتصميمها، وتنفيذها، وتشغيلها. وقد يشمل ذلك جهات حكومية، وجهات قطاع خاص، وجهات غير ربحية، ومؤسسات أكاديمية. تعد أدوار شركاء المنظومة، مهمة وبارزة في تحقيق رؤية المدن الذكية، بدءاً من تطوير البنية التحتية، ووصولاً إلى تقديم الخدمات.

- **شركاء المنظومة من الأطراف الخارجية:** تضم هذه الفئة الجهات المختصة، أو الموردين المتخصصين بتقديم الخدمات والتقنيات الأساسية؛ لدعم إطار عمل المدن الذكية. تقدم هذه الفئة حلولاً في مجالات محددة؛ مثل تحليل البيانات، والحوسبة السحابية، والأمن السيبراني، وأجهزة إنترنت الأشياء. ويعد التعاون مع الشركاء من الأطراف الخارجية أمراً مهماً للوصول إلى التقنيات والخبرات التي تعزز عمليات المدن الذكية ووضعها الأمني.

- **السكان:** الأفراد الذين يتفاعلون مع البنية التحتية للمدن الذكية، والخدمات المقدمة من قبلها. وتضم هذه الفئة المستفيدين من الخدمات الرقمية والمادية للمدن الذكية. ويشمل ذلك دون حصر، خدمات النقل، والمرافق، والسلامة العامة. تستفيد هذه الفئة بشكل مباشر من التطورات التي تشهدها المدن الذكية ويسهمون أيضًا في تلبية احتياجاتها الناشئة وتطورها المستمر.

البنية التقنية

تُبنى المدن الذكية على أساس من التقنيات المترابطة، التي تشكل منظومة حديثة، وفعالة، وسريعة الاستجابة. إذ تعمل أجهزة إنترنت الأشياء، وأجهزة الاستشعار المنتشرة في جميع أنحاء المناطق الحضرية، لجمع بيانات لحظية بطريقة مباشرة، ثم يجري نقلها إلى شبكة مركزية من المنصات السحابية، ومراكز البيانات. وتتولى هذه الشبكة معالجة البيانات وتخزينها، ليجري استخدامها بعد ذلك بواسطة تطبيقات، وبرمجيات مختلفة، لإدارة عمليات المدن الذكية؛ بدءاً من تدفق حركة

المرور، ووصولًا إلى الخدمات العامة. وتشكل أدوات التحليل المتقدمة، والذكاء الاصطناعي أهمية بارزة في هذا النظام، إذ تساعد هذه الأدوات في تحليل البيانات؛ لتوجيه عملية صنع القرار، وتحسين وظائف المدن الذكية.

وتشمل البنية التقنية الأساسية للمدن الذكية العديد من الوظائف التقنية، والمكونات التابعة لها. يقدم الشكل (1) مثالاً توضيحياً للبنية التقنية، التي تتضمن الأساسيات التقنية اللازمة؛ لتحقيق الإمكانات الكاملة للمنظومة الذكية والحديثة. ويعد هذا بمثابة مثال توضيحي؛ وتظل الإرشادات قابلة للتطبيق، حتى في حال استخدام تقسيم مختلف للبنية التقنية.

شكل ١: البنية التقنية المرجعية للمدن الذكية

مراحل دورة حياة التقنية

توجد المدن الذكية في مراحل مختلفة، من دورة حياة تطويرها. تتسق مراحل التطوير في هذه الدورة بشكل وثيق مع مراحل دورة حياة التقنية الخاصة بها. وتحدد دورة الحياة، المراحل الرئيسية المطلوبة لتطوير التقنية في المدن الذكية، لتكون متقدمة ومدارة بفعالية وكفاءة.

تمتد دورة الحياة الموضحة في الشكل (٢) إلى خمس مراحل رئيسية؛ ولكل مرحلة منها أهمية بالغة للتطوير الناجح للمدن الذكية. بالإضافة إلى ضمان التوزيع الإستراتيجي للتقنية، تعنى دورة الحياة هذه أيضًا بالقدرة على التكيف والتحسين المستمر؛ لمواجهة المخاطر المستقبلية، بما في ذلك مخاطر الأمن السيبراني.

شكل ٢: مراحل دورة حياة التقنية للمدن الذكية

مراحل دورة حياة التقنية للمدن الذكية:

١- **التخطيط**: تعد هذه المرحلة الأولية حاسمة في إنشاء أساسات المدينة الذكية. وتتضمن هذه المرحلة تقييم منظومة المدينة الذكية، وتحديد احتياجات أصحاب المصلحة. وتشمل المهمات الرئيسية؛ إعداد أهداف واضحة لتنفيذها، وتشكيل إستراتيجيات لتحقيقها، وتحديد الأدوار والمسؤوليات لضمان التعاون والحوكمة الفعالة.

٢- **التصميم**: يجري التركيز في مرحلة التصميم على تطوير حلول تقنية آمنة ومرنة. ويتضمن ذلك تخطيط البنية التحتية، والأنظمة اللازمة؛ لتحقيق أهداف المدينة الذكية، والتأكد من أنها قابلة للتطوير، وآمنة ومتوافقة مع التقنيات الحالية.

٣- **التنفيذ**: خلال مرحلة التنفيذ، يجرى وضع التقنيات والعمليات المخطط لها في مواضعها. وتتضمن هذه الخطوة الإعداد والتركيب الفعلي لأنظمة التقنية، وفقاً للخطط والتصميمات الموضحة في المراحل السابقة.

٤- **التشغيل**: في مرحلة التشغيل، تجري إدارة تقنيات المدن الذكية بشكل فعال. ويشمل ذلك المراقبة والصيانة المنتظمة، وجمع الآراء والملحوظات؛ لضمان توفر التقنيات باستمرار، بغية تلبية احتياجات المدينة الذكية وعملها بشكل صحيح.

٥- **التحسين المستمر**: تتضمن المرحلة النهائية، تحديث البنية التحتية والوثائق والعمليات الخاصة بالتقنية وتحسينها. ويعني ذلك استبدال الأنظمة القديمة، أو التخلص منها تدريجياً، وإدارة النقل الآمن للبيانات، وتحسين الخطط والوثائق؛ لتحقيق أهداف التطوير الحالية والمستقبلية.

نظرة عامة على مخاطر الأمن السيبراني

تؤدي الأدوات المستخدمة في المدن الذكية، مثل: إنترنت الأشياء، والحوسبة السحابية، والأدوات الأخرى؛ إلى توسيع نطاق تهديدات الأمن السيبراني.

ويمكن أن تؤدي الثغرات في هذه الأنظمة إلى مشكلات تتعلق بالسلامة، وأعطال واسعة النطاق؛ مما يعرّض البنية التحتية الرقمية والمادية للخطر. كما يمكن أن تؤدي الهجمات السيبرانية على مراكز البيانات، والمنصات السحابية، والتطبيقات الحديثة إلى إضعاف ثقة العامة، وتعطيل عمليات المدينة الذكية. بالإضافة إلى ذلك؛ قد تشكل التهديدات، مثل انتحال الهوية في مراكز العمليات والانتهاكات في الواجهات العامة، مخاطر كبيرة على سلامة البيانات وسريتها، والأمن العام في المدينة. وتؤكد الأهمية البارزة لشبكات الاتصالات، وضرورة تأمين البوابات، وواجهات برمجة التطبيقات، على ضرورة اتخاذ تدابير إضافية؛ لضمان الأمن السيبراني للمدينة الذكية.

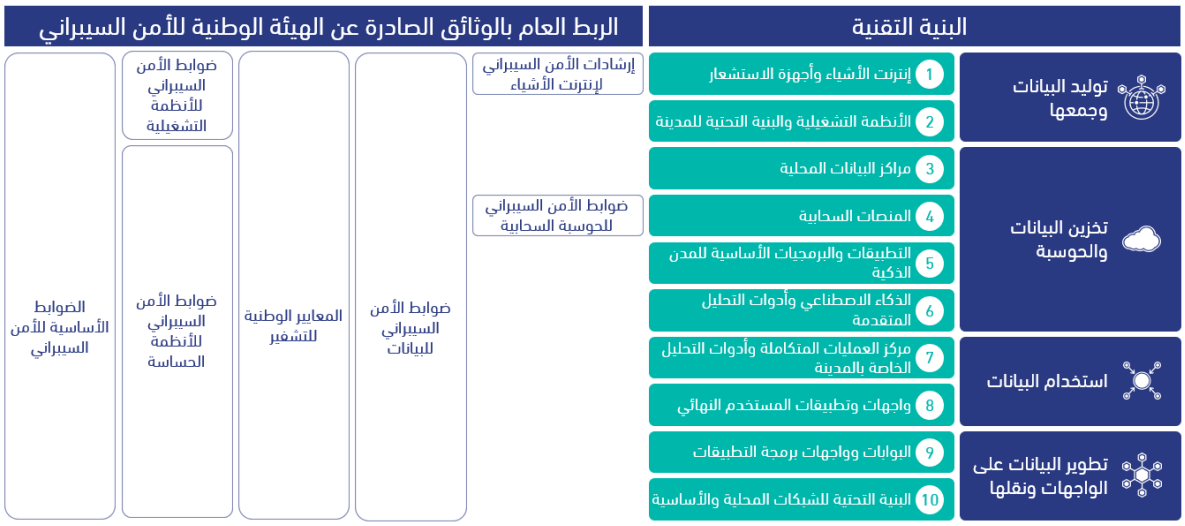
لمعالجة هذه التحديات وتخفيف مخاطرها؛ يجب وجود منظومة شاملة ومتماسكة تعزز أفضل ممارسات الأمن السيبراني في جميع مراحل دورة حياة المدينة الذكية. ويعد هذا النهج في غاية الأهمية، لحماية المدن الذكية، من التهديدات السيبرانية الناشئة، وضمان تطويرها، لتكون أكثر أماناً وصموداً. ويتطلب ذلك التفاني من جميع أصحاب المصلحة داخل منظومة المدينة الذكية. ومع هذا كله فإن، تقع المسؤولية العظمى تقع على صانعي القرار في المدينة الذكية، بحكم أدوارهم الأساسية في الإشراف على تضمين هذه التدابير، وتوجيه المدينة نحو مستقبل أكثر أمانًا وصموداً.

العلاقة مع إصدارات الهيئة الوطنية للأمن السيبراني الأخرى

بالإضافة إلى إرشادات الأمن السيبراني للمدن الذكية؛ فقد أصدرت الهيئة الوطنية للأمن السيبراني، سياسات أخرى للأمن السيبراني، وآليات للحوكمة، وأطر، ومعايير، وضوابط وإرشادات (على سبيل المثال إرشادات الأمن السيبراني لإنترنت الأشياء) يجب على صناع القرار في المدن الذكية، وشركاء المنظومة، الرجوع إليها للاسترشاد والتوجيه؛ وفي بعض الحالات يجب الالتزام بها.

وجرى ربط الإرشادات بإصدارات الهيئة الوطنية للأمن السيبراني، التي يمكن أن توفر تفاصيل إضافية بشأن طريقة التنفيذ وقابلية التطبيق.

يعرض الشكل (٣) الربط العام بين مكونات البنية التقنية للمدينة الذكية، والإصدارات الصادرة عن الهيئة الوطنية للأمن السيبراني.



شكل ٣: الربط العام بين البنية التقنية والإصدارات الصادرة عن الهيئة الوطنية للأمن السيبراني

مكونات وهيكلية إرشادات الأمن السيبراني للمدن الذكية

المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني للمدن الذكية

يوضح الشكل (٤) الآتي، المكونات الأساسية والفرعية، لإرشادات الأمن السيبراني للمدن الذكية.

١. حوكمة الأمن السيبراني Cybersecurity Governance	١-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١-٢	إدارة الأمن السيبراني Cybersecurity Management
	١-٣	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١-٥	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٦	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information and Technology Project Management
	١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	١-٨	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit
	١-٩	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-١٠	برنامج التوعية والتدريب في مجال الأمن السيبراني Cybersecurity Awareness and Training Program
٢. تعزيز الأمن السيبرانى Cybersecurity Defense	١-٢	تعزيز الأمن السيبراني Cybersecurity Defense		
٣. صمود الأمن السيبرانى Cybersecurity Resilience	١-٣	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
٤. الأمن السيبرانى المتعلق بالأطراف الخارجية والحوسبة السحابية Third Party and Cloud Computing Cybersecurity	١-٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٢-٤	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity

شكل ٤: المكونات الأساسية والفرعية لإرشادات الأمن السيبراني للمدن الذكية

الهيكلية

يوضح الشكلان (٥) و(٦) الآتيان معنى رموز إرشادات الأمن السيبراني للمدن الذكية:

شكل 0: معنى رموز إرشادات الأمن السيبراني للمدن الذكية

شكل ٦: هيكلية إرشادات الأمن السيبراني للمدن الذكية

يبين الجدول (١) أدناه طريقة هيكلة ارشادات الأمن السيبراني للمدن الذكية.

١	اسم المكون الأساسي		
رقم مرجعي للمكون الأساسي			
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي		
الهدف			
الإرشادات		مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
رقم مرجعي للإرشاد	بنود الإرشاد	مرحلة دورة حياة المدينة الذكية، أو مراحلها؛ حيث يكون هذا الإرشاد أكثر إمكانية للتطبيق	وثيقة أو وثائق الهيئة الوطنية للأمن السيبراني، التي توفر تفاصيل وضوابط وأطر وإرشادات إضافية؛ تنطبق على هذا الإرشاد

جدول ١: هيكلية إرشادات الأمن السيبراني للمدن الذكية

إرشادات الأمن السيبراني للمدن الذكية

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إستراتيجية الأمن السيبراني	
الهدف	ضمان احتواء إستراتيجية المدينة الذكية ورؤيتها، وخطط عملها، وأهدافها، ومبادراتها على جوانب الأمن السيبراني، الخاصة بالمدن الذكية، وإسهامها في تحقيق الالتزام بالمتطلبات التشريعية، والتنظيمية ذات العلاقة.	
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-١-١	تضمين أهداف الأمن السيبراني ضمن الوثائق الإستراتيجية التأسيسية للمدينة الذكية؛ مما يضمن أن جميع مبادرات التخطيط والتطوير، تأخذ في الحسبان الأمن السيبراني منذ البداية.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة
١-١-٢	تطوير إستراتيجية شاملة للأمن السيبراني للمدينة الذكية، بحيث تتوافق مع أهداف العمل العامة للمدينة، وتحديد أهداف ومبادرات خاصة للأمن السيبراني.	التخطيط	
١-١-٣	إنشاء خارطة طريق ديناميكية للأمن السيبراني، للمدينة الذكية؛ لتحديد الإجراءات المرحلية، للتخفيف من المخاطر التي جرى تحديدها، بحيث تكون مصممة لتناسب تطورات المشهد الرقمي للمدينة ومستجداتها.	التخطيط	
١-١-٤	تحديد مؤشرات الأداء الرئيسية للأمن السيبراني للمدينة الذكية، ومتابعتها؛ لضمان تلبية متطلبات الأمن السيبراني طوال دورة حياة المدينة الذكية.	التخطيط والتشغيل والتحسين المستمر	
١-١-٥	إجراء تقييمات لاحتياجات الأمن السيبراني بشكل سنوي، أو عند الحاجة لتحديث إستراتيجية الأمن السيبراني وخارطة الطريق في المدينة الذكية، لضمان المواءمة المستمرة مع إستراتيجية المدينة الذكية، والتقنيات الناشئة، والتهديدات، والتغييرات التنظيمية.	التخطيط والتحسين المستمر	

١-٢	إدارة الأمن السيبراني	
الهدف	ضمان امتلاك منظمة المدينة الذكية، الهيكليات اللازمة؛ لضمان إدارة الأمن السيبراني وتنفيذها، ضمن منظومة المدينة الذكية، وفقًا للتنظيمات والتشريعات ذات العلاقة.	
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٢-١	إنشاء إدارة معنية بالأمن السيبراني، داخل إدارة المدينة الذكية؛ تكون مسؤولة عن حوكمة الأمن السيبراني وتنفيذ إجراءاته داخل المنظمة الإدارية، والمنظومة الأوسع. ويجب أن تكون هذه الإدارة مستقلة عن إدارة تقنية المعلومات في المدينة الذكية.	التخطيط	الضوابط الأساسية للأمن السيبراني
١-٢-٢	إنشاء لجنة إشرافية للأمن السيبراني؛ لضمان تنفيذ برامج ومبادرات الأمن السيبراني ودعمها، ضمن منظومة المدينة الذكية. كما يُنصح بتحديد ميثاقها وأدوارها ومسؤولياتها وإطار الحوكمة الخاص بها، بالإضافة إلى تحديد أعضاء اللجنة وتوثيق أسماءهم، مع الأخذ بالحسبان عدم تعارض المصالح.	التخطيط	

١-٣	سياسات وإجراءات الأمن السيبراني	
الهدف	ضمان التوثيق والنشر لسياسات الأمن السيبراني للمدن الذكية وإجراءاته، والالتزام بها من قبل شركاء المنظومة، للمدينة الذكية؛ بما في ذلك مشغلو عناصر البنية التحتية الرئيسية، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.	
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٣-١	تحديد سياسات الأمن السيبراني وإجراءاته للمدن الذكية وتوثيقها، واعتمادها، ونشرها. ويجب أن تفرض هذه السياسات، ممارسات الأمن السيبراني وإستراتيجيات إدارة المخاطر اللازمة؛ لحماية البنية التحتية والخدمات الحساسة.	التصميم	الضوابط الأساسية للأمن السيبراني

١-٣-٢	ضمان تطبيق سياسات الأمن السيبراني وإجراءاته للمدن الذكية وما تشمله من ضوابط ومتطلبات.	التشغيل	ضوابط الأمن السيبراني للأنظمة التشغيلية
١-٣-٣	تنفيذ آليات عمليات التدقيق والمراجعة المنتظمة، المتعلقة بالالتزام وتطبيقها؛ لضمان الامتثال لسياسات الأمن السيبراني للمدينة الذكية وإجراءاته.	التشغيل	
١-٣-٤	مراجعة سياسات الأمن السيبراني وإجراءاته وتحديثها؛ إذا لزم الأمر على سبيل المثال، عند حدوث تطورات تقنية، أو تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة.	التحسين المستمر	
١-٤	أدوار ومسؤوليات الأمن السيبراني		
الهدف	ضمان تحديد الأدوار والمسؤوليات لجميع شركاء المنظومة، للمدينة الذكية، لإدارة متطلبات الأمن السيبراني في المدينة الذكية وتنفيذها ومراقبتها.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٤-١	توثيق منظومة الأمن السيبراني للمدينة الذكية، وتحديد جميع أصحاب المصلحة ومهماتهم ومسؤولياتهم في الحفاظ على الأمن السيبراني الخاصة بهم.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة التشغيلية
١-٤-٢	إجراء تحليل لأصحاب المصلحة؛ لتحديد مسؤوليات الأمن السيبراني بوضوح، وضمان التوافق مع أهداف المدينة الذكية والمتطلبات التنظيمية.	التخطيط	
١-٤-٣	ضمان عدم وجود تعارض في المصالح، والفصل بين المهمات الموكلة، عند تحديد الأدوار والمسؤوليات بين أصحاب المصلحة، داخل منظومة المدينة الذكية.	التخطيط	
١-٤-٤	تطوير برنامج تدريب واعتماد، لجميع أصحاب المصلحة؛ ممن يتحملون مسؤوليات الأمن السيبراني، والتأكد بأنهم يتمتعون بالمهارات والمعرفة اللازمة.	التخطيط	
١-٤-٥	تحديد إطار للمراجعة الدورية، وإعادة تقييم أدوار ومسؤوليات الأمن السيبراني، والتكيف مع التغيرات في البيئات التشغيلية، والتهديدات في المدينة الذكية.	التحسين المستمر	

١-٥	إدارة مخاطر الأمن السيبراني		
الهدف	ضمان اتباع طريقة منهجية، لإدارة مخاطر الأمن السيبراني، داخل منظومة المدينة الذكية؛ بما في ذلك تحديد مخاطر الأمن السيبراني وتقييمه وإدارته داخل منظومة المدينة الذكية، وضمان حماية أصول المعلومات والتقنية، بما يتسق مع متطلبات المدينة للمخاطر والالتزام.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٥-١	إنشاء وتوثيق إجراءات شاملة لإدارة مخاطر الأمن السيبراني وتوثيقها؛ بما في ذلك تحديد المخاطر، وتقييمها، ومعالجتها، والإشراف عليها؛ مما أقرها صناع القرار في المدن الذكية عبر المنظومة.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية
٢-٥-١	إجراء تقييمات شاملة لمخاطر الأمن السيبراني مع الأخذ في الحسبان الأصول الرقمية والمادية للمدينة الذكية، وتحديد التهديدات، والثغرات، والتأثيرات المحتملة.	التخطيط والتشغيل	
٣-٥-١	الاحتفاظ بسجل مخاطر الأمن السيبراني، وتحديثه بانتظام بالمخاطر المحددة، وإستراتيجيات التخفيف، ومراقبة مدى فعاليتها؛ مقارنةً مع مستوى تحمل المخاطر المحدد للمدينة الذكية.	التخطيط والتشغيل	
٤-٥-١	تنفيذ إجراءات تقييم مخاطر الأمن السيبراني، في جميع مراحل دورة حياة المدينة الذكية.	جميع المراحل	
٥-٥-١	إجراء تقييمات الاعتمادية، لتقييم مستوى الحساسية والصمود، لشركاء المنظومة، ومقدمي الخدمات. وذلك لضمان وجود خطط للطوارئ.	التصميم	
٦-٥-١	تطبيق التقييم الذاتي للأمن السيبراني لشركاء المنظومة، وخاصة، ممن يتولون إدارة البنية التحتية الحساسة، لتقييم الثغرات في الأمن السيبراني، ومعالجتها بانتظام.	التخطيط والتنفيذ والتشغيل	
٧-٥-١	مراجعة إطار إدارة مخاطر الأمن السيبراني وتحديثه بشكل دوري؛ ليعكس التغييرات في مشهد التهديدات والمتطلبات التقنية والتنظيمية.	التحسين المستمر	

٦-١	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية		
الهدف	ضمان شمول متطلبات الأمن السيبراني في دورة حياة إدارة مشروع تقنية المعلومات، لمبادرات المدينة الذكية؛ مما يضمن صمود البيانات، والبنية التحتية وتوافرها وسلامتها.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٦-١	التأكد من أن الأمن السيبراني جزء لا يتجزأ من دورة حياة إدارة المشروع، لجميع مبادرات المدينة الذكية، بدءاً من التصميم الأولي، وحتى التشغيل.	التخطيط والتصميم	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية
٢-٦-١	تطوير بنية للأمن السيبراني؛ لتحديد الضوابط الأمنية وتكاملها، ضمن بنية تقنية المعلومات لكل مشروع في مجال التقنية، مصحوبة بخطة لإدارة المخاطر؛ خاصة بالمشروع.	التصميم	
٣-٦-١	تضمين معايير التشفير الآمن، ومبدأ الأمن من خلال التصميم، وآليات الأمان الفعالة (بما في ذلك التشفير والتحكم في الوصول/الدخول) في جميع المشاريع الخاصة بالتقنية.	التصميم	
٤-٦-١	تضمين التدريب في مجال الأمن السيبراني، وصيانة التقنية وإجراءات إدارة الحوادث وإدراجها ضمن اتفاقيات مستوى الخدمة لجميع مشاريع التقنية.	التصميم	
٥-٦-١	تخطيط آليات التدقيق وتطبيقها لمكونات الحلول في مراحل التصميم والتنفيذ.	التصميم والتنفيذ	
٦-٦-١	تقييم التأثير على الأمن السيبراني وإدارته، عند تضمين الحلول، أو التقنيات الجديدة في الأنظمة القائمة، مع ضمان اتباع نهج الدفاع متعدد المراحل.	التصميم والتنفيذ	
٧-٦-١	طلب اختبار و/أو شهادة اعتماد بطريقة مستقلة؛ لضمان الأمن السيبراني، لجميع الحلول التقنية المنفذة، داخل منظومة المدينة الذكية.	التصميم والتنفيذ	

١-٦-٨	تأمين الترابط والتفاعل بين الأنظمة؛ خاصة تلك التي تعالج بيانات المدينة الحساسة أو تخزنها، باستخدام إستراتيجية الدفاع المتعدد المراحل.	التصميم والتنفيذ	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للبيانات
١-٦-٩	وضع خطة لإدارة مخاطر الأمن السيبراني للمشاريع التقنية.	التصميم والتحسين المستمر	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة
١-٦-١٠	التأكد من تضمين ضوابط حماية البيانات، أثناء مراحل تصميم وتنفيذ المشاريع؛ مما يضمن حماية البيانات طوال دورة حياة المشروع.	التخطيط والتنفيذ	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للبيانات
١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني		
الهدف	التأكد من أن برنامج الأمن السيبراني للجهات، داخل منظومة المدينة الذكية، يتوافق مع المتطلبات التنظيمية والتشريعية ذات العلاقة.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٧-١	ضمان الالتزام الكامل بتشريعات الأمن السيبراني الوطنية، وتنظيماته المعمول بها، من خلال تضمين المتطلبات القانونية في عملية التخطيط، وعمليات المدينة الذكية.	التخطيط والتشغيل	الضوابط الأساسية للأمن السيبراني
١-٧-٢	تسهيل تبني معايير الأمن السيبراني الوطنية، داخل المدينة الذكية.	التخطيط	

١-٧-٣	تنفيذ آليات؛ لفرض الالتزام بالتشريعات، والتنظيمات، والمعايير الإلزامية الحالية، المعمول بها في منظومة المدينة الذكية.	التخطيط والتشغيل	
١-٨	المراجعة والتدقيق الدوري للأمن السيبراني		
الهدف	التأكد من تنفيذ ضوابط الأمن السيبراني؛ لتكون ملتزمة ومتوافقة مع متطلبات الأمن السيبراني للمدن الذكية.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٨-١	إعداد برنامج مراجعة وتدقيق للأمن السيبراني وتنفيذه بطريقة منظمة، وإجراء تقييمات منتظمة؛ لتقييم فعالية ضوابط الأمن السيبراني.	التخطيط والتشغيل	الضوابط الأساسية للأمن السيبراني
١-٨-٢	التأكد من أن شركاء منظومة المدينة الذكية؛ يعتمدون آليات للتدقيق، والمراجعة الدورية؛ بهدف تسهيل عمليات التدقيق المستقلة، وإتاحة النتائج لأصحاب المصلحة المعنيين.	التخطيط والتشغيل	ضوابط الأمن السيبراني للأنظمة الحساسة
١-٨-٣	تطوير عمليات خاصة لإدارة، المشكلات المتعلقة بعدم الالتزام بسياسات وإجراءات الأمن السيبراني وتصحيحها؛ مع العناية بالإجراءات التصحيحية للمتطلبات الإلزامية.	التشغيل	ضوابط الأمن السيبراني للأنظمة التشغيلية ضوابط الأمن السيبراني للبيانات
١-٩	الأمن السيبراني المتعلق بالموارد البشرية		
الهدف	ضمان إدارة مخاطر الأمن السيبراني ومتطلباته، المتعلقة بالعاملين (الموظفين والمتعاقدين) لشركاء منظومة المدينة الذكية، بشكل فعال، خلال دورة حياة التوظيف، وفقاً للسياسات والإجراءات التنظيمية، والمتطلبات التشريعية ذات العلاقة.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-٩-١	إعداد متطلبات شاملة للأمن السيبراني لجميع العاملين، المشاركين في منظومة المدينة الذكية، بما في ذلك الشروط التعاقدية، وإجراء عمليات المسح الأمني للأدوار الحساسة، والتدريب الإلزامي على الأمن السيبراني.	التخطيط	الضوابط الأساسية للأمن السيبراني

١-٩-٢	المراجعة بانتظام، والتعديل على إمكانية العاملين للوصول إلى أصول المعلومات والتقنية؛ بما يتسق مع أدوارهم، مما يضمن الرفض، والإلغاء الفوري للوصول إلى أصول المعلومات والتقنية، عند تغيير أدوارهم أو إنهائها.	التشغيل	ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية ضوابط الأمن السيبراني للبيانات
١-١٠	برنامج التوعية والتدريب في مجال الأمن السيبراني		
الهدف	تعزيز ثقافة الوعي بالأمن السيبراني عند إدارة المدينة الذكية، وبين جميع أصحاب المصلحة؛ بما في ذلك السكان، لتعزيز الوضع الأمني، العام وتشجيع الممارسات الرقمية الآمنة.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-١٠-١	إعداد برامج شاملة للتوعية والتدريب، في مجال الأمن السيبراني، عند إدارة المدينة الذكية؛ لتعزيز ونشر ثقافة قوية للأمن السيبراني.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للبيانات
١-١٠-٢	تعزيز الوعي بالأمن السيبراني بين موظفي شركاء منظومة المدينة الذكية، وجميع السكان؛ بما في ذلك الممارسات الرقمية الآمنة ومسؤوليات التعامل مع البيانات.	التخطيط	
١-١٠-٣	تضمين التدريب على الأمن السيبراني، ضمن الإجراءات التشغيلية لشركاء المنظومة، ممن يتولون إدارة البنية التحتية الحساسة، وتصميم البرامج، لمعالجة مخاطر تشغيلية محددة.	التصميم	

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	تعزيز الأمن السيبراني		
الهدف	ضمان وجود آليات كافية؛ لتعزيز الأمن السيبراني عبر منظومة المدن الذكية؛ لحماية المعلومات، وأصول المعلومات، ضد الهجمات السيبرانية.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-١-٢	الاحتفاظ بقائمة جرد دقيقة وحديثة، لجميع أصول الأجهزة والبرامج، داخل منظومة المدينة الذكية، وتصنيفها حسب الحساسية، والجهة المسؤولة عنها.	التخطيط والتشغيل	الضوابط الأساسية للأمن السيبراني
٢-١-٢	تطبيق معايير عالية، لإدارة الهويات والوصول؛ ويتضمن ذلك على سبيل المثال، مبدأ الحد الأدنى من الصلاحيات، والمراقبة المستمرة، ومبدأ التحقق متعدد العناصر للهوية (MFA)، ومبدأ الثقة الصفرية (zero trust architecture)، وآليات التحكم في الوصول لجميع المستخدمين والأجهزة.	التصميم والتنفيذ	ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية
٣-١-٢	فرض مبادئ "الحد الأدنى من الصلاحيات والامتيازات" (Least Privilege) و "الحاجة إلى المعرفة" (Need-to-know) عند توفير الوصول إلى أصول المعلومات والتقنية في المنظومة.	التنفيذ	الضوابط الأساسية للأمن السيبراني المعايير الوطنية للتشفير
٤-١-٢	تطوير إجراءات آمنة لإدارة الهويات، وبيانات الاعتماد، والشهادات الرقمية، وسلوكيات المستخدم، والأجهزة والخدمات، والتحقق منها ومنحها صلاحية المستخدم.	التصميم	
٥-١-٢	تطبيق التشفير الشامل (end-to-end encryption) للبيانات الحساسة؛ أثناء الاستخدام، والنقل والتخزين؛ مع الالتزام بالمعايير الوطنية للتشفير، وأفضل الممارسات.	التصميم والتنفيذ	ضوابط الأمن السيبراني للأنظمة الحساسة المعايير الوطنية للتشفير

٢-١-٦	تطوير ضوابط كافية لتعزيز الأمن السيبراني لحماية أنظمة المعلومات، ومرافق معالجة المعلومات في المدينة الذكية، من المخاطر السيبرانية؛ بما في ذلك خدمات البريد الإلكتروني، والشبكات، والتطبيقات، والأجهزة المحمولة.	التخطيط والتصميم	الضوابط الأساسية للأمن السيبراني
٢-١-٧	التعاون مع الموردين من الأطراف الخارجية، والشركات المصنعة للمعدات الأصلية؛ لضمان تطبيق التصحيحات، والتحديثات الأمنية، في الوقت المناسب، لجميع الأنظمة في المدينة الذكية.	التشغيل	الضوابط الأساسية للأمن السيبراني
٢-١-٨	تنفيذ التدابير اللازمة؛ لضمان سلامة البيانات وسريتها وتوافرها، طوال دورة حياتها، وذلك باستخدام التقنيات المتطورة، وحلول التخزين الاحتياطية.	التصميم والتنفيذ	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للبيانات
٢-١-٩	تطبيق ضوابط الأمن المادي، في المواقع التي تعالج البيانات الحساسة، أو تدعم عمليات المدينة الذكية الحساسة، للحماية من الوصول المادي غير المصرح به.	التصميم	
٢-١-١٠	تعزيز تدابير الأمن المادي، في مواقع معالجة البيانات الحساسة؛ لمنع الوصول غير المصرح به، وتضمين المراقبة، والتحكم بالوصول، والتدابير البيئية.	التصميم	
٢-١-١١	فحص ثغرات الأمن السيبراني واكتشافها، ومراقبتها باستمرار، ومعالجتها في أنظمة معلومات المدينة الذكية.	التشغيل والتحسين المستمر	
٢-١-١٢	تطوير القدرات لجمع أحداث الأمن السيبراني وحوادثه، وتحليلها والإبلاغ عنها، وإدارتها؛ مما يعزز قدرة المدينة الذكية على اكتشاف الهجمات السيبرانية المحتملة مبكرًا، وتقليل تأثيرها.	التشغيل والتحسين المستمر	الضوابط الأساسية للأمن السيبراني

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال		
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني، ضمن خطة إدارة استمرارية الأعمال للمدينة الذكية؛ وذلك من أجل تعزيز سلامة البنية التحتية الرقمية، والمادية؛ أثناء حوادث الأمن السيبراني وبعدها.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
١-١-٣	تضمين سيناريوهات تهديدات الأمن السيبراني في خطط استمرارية الأعمال، والتعافي من الكوارث؛ مما يضمن استمرار تشغيل الخدمات الأساسية، أثناء الحوادث السيبرانية.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية ضوابط الأمن السيبراني للبيانات
٢-١-٣	مواءمة عناصر الأمن السيبراني في خطط التعافي من الكوارث، مع الإستراتيجيات الوطنية والإستراتيجيات المدنية الأوسع، لإدارة الحوادث السيبرانية؛ بما يضمن تنسيق جهود الاستجابة.	التصميم	
٣-١-٣	تطوير خطط إدارة الحوادث المصممة خصيصاً لحوادث الأمن السيبراني المحتملة وتنفيذها؛ متضمنةً بذلك آليات الاحتواء، والتعافي، وآليات تقييم ما بعد الحادث.	التصميم	
٤-١-٣	إجراء تدريبات وتمرينات منتظمة؛ للاستجابة لحوادث الأمن السيبراني، مع جميع شركاء منظومة المدينة الذكية ذوي الصلة، بناءً على سيناريوهات تحاكي واقع الحوادث السيبرانية.	التشغيل والتحسين المستمر	
٥-١-٣	تحديث خطط إدارة الحوادث، والتعافي من الكوارث بانتظام لتعكس التهديدات السيبرانية الجديدة، والتقدم التقني، والدروس المستفادة من التدريبات، والتمرينات، والحوادث الحقيقية.	التحسين المستمر	

٤ الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية		
الهدف	ضمان الإدارة الفعالة، والتخفيف من مخاطر الأمن السيبراني، المرتبطة بالأطراف الخارجية، ومقدمي الخدمات؛ وضمان التزامهم بمعايير الأمن السيبراني وإجراءاته الخاصة بالمدن الذكية.		
	الإرشادات	مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
٤-١-١	وضع متطلبات صارمة، للأمن السيبراني، لشركاء المنظومة من الأطراف الخارجية؛ المشاركين في معالجة بيانات المدينة، أو تخزينها؛ ليتم عكس هذه المتطلبات في الاتفاقيات والعلاقات التعاقدية.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة الحساسة ضوابط الأمن السيبراني للأنظمة التشغيلية ضوابط الأمن السيبراني للبيانات
٤-١-٢	التأكد من أن الشركاء من الأطراف الخارجية، يعتمدون استخدام التدابير المناسبة، للحذف الآمن للبيانات؛ وإيقاف استخدام الأصول بعد انتهاء الخدمة، والحفاظ على خصوصية البيانات وسلامتها.	التشغيل والتحسين المستمر	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للبيانات
٤-١-٣	إجراء تقييمات شاملة لمخاطر الأمن السيبراني، قبل استكمال العقود، مع شركاء الأطراف الخارجية؛ وتحديث متطلبات الأمن السيبراني، بناءً على ملف التعريف الخاص بمخاطر الشريك.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للأنظمة التشغيلية ضوابط الأمن السيبراني للبيانات
٤-١-٤	تجميع عناصر ملف مخاطر شامل للمدينة الذكية وتحديثه بانتظام، بحيث يعكس تقييمات مخاطر الأمن السيبراني لجميع شركاء المنظومة من الأطراف الخارجية.	التحسين المستمر	

٤-٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة		
الهدف	ضمان الإدارة الفعالة لمخاطر الأمن السيبراني، المرتبطة بمنصات الحوسبة السحابية والاستضافة، وتطبيق متطلبات الأمن السيبراني؛ لتوفير الحماية الكافية، لأصول المعلومات، المستضافة على السحابة.		
الإرشادات		مراحل دورة الحياة	وثائق الهيئة الوطنية للأمن السيبراني
٤-٢-١	تنفيذ تنظيمات الأمن السيبراني، الشاملة للخدمات السحابية، التي تتضمن إدارة متمكنة للوصول للبيانات، ومعايير تشفير للبيانات، وإستراتيجيات مفصلة للاستجابة للحوادث.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للحوسبة السحابية المعايير الوطنية للتشفير
٤-٢-٢	تقييم وضع الأمن السيبراني لمقدمي الخدمات السحابية قبل التعاقد؛ وإجراء تقييمات مستمرة، لضمان الالتزام بمتطلبات الأمن السيبراني للمدينة الذكية.	التخطيط	الضوابط الأساسية للأمن السيبراني ضوابط الأمن السيبراني للحوسبة السحابية
٤-٢-٣	تضمين الأحكام التي تضمن استرجاع البيانات، بتنسيقات محايدة للموردين، في اتفاقيات الخدمة السحابية؛ مما يضمن إمكانية نقل البيانات وإمكانية الوصول إليها.	التصميم	
٤-٢-٤	إنشاء عمليات للمراقبة الأمنية المستمرة، والتدقيق، والمراجعة للبيئات المستضافة على الحوسبة السحابية؛ لاكتشاف الأنشطة غير المصرح بها، والاستجابة لها على الفور.	التخطيط والتشغيل	
٤-٢-٥	استخدام أدوات المراقبة المتقدمة؛ لتحقيق رؤية شاملة للبنى التحتية، المستضافة على الحوسبة السحابية؛ وتسهيل الإدارة الفعالة، والإشراف الأمني والالتزام.	التصميم	
٤-٢-٦	مراجعة سياسات الحوسبة السحابية وتحديث إجراءاتها بشكل منهجي؛ للتكيف مع تهديدات الأمن السيبراني الجديدة والتقدم التقني والمتطلبات التنظيمية.	التحسين المستمر	

ملاحق

ملحق (أ): مصطلحات وتعريفات

المصطلح	التعريف
واجهات برمجة التطبيقات Application Programming Interface (API)	مجموعة من القواعد (مثل: الأوامر والدوال والكائنات والبروتوكولات) التي طورت؛ ليتم استخدامها من قبل المبرمجين، لتطوير البرمجيات، أو التفاعل مع أنظمة و/أو برمجيات أخرى.
إمكانية نقل البيانات Data Portability	القدرة على نقل البيانات بين التطبيقات، أو البرامج، أو بيئات الحوسبة، أو الخدمات السحابية المختلفة.
إدارة الهوية وصلاحيات الدخول Identity and Access Management (IAM)	إطار من السياسات والتقنيات؛ لضمان حصول مستخدمين محددين، دون غيرهم، على إمكانية الوصول المناسب إلى الموارد التقنية.
حادثة Incident	انتهاك أمني بمخالفة سياسات الأمن السيبراني، أو سياسات الاستخدام المقبول، أو ممارسات، أو ضوابط، أو متطلبات الأمن السيبراني.
سلامة المعلومات Integrity	الحماية من التعديل، أو التدمير غير المصرح به للمعلومات، كما يتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
مؤشر الأداء الرئيسي Key Performance Indicator (KPI)	أحد أدوات قياس الأداء، وتستخدم لتقييم مدى نجاح نشاط أو جهة في تحقيق أهداف محددة.
الحد الأدنى من الصلاحيات والامتيازات Least Privilege	مبدأ في الأمن السيبراني، يتمثل في منح المستخدمين فحسب امتيازات الوصول، التي يحتاجونها، للقيام بمسؤولياتهم الرسمية.
التحقق من الهوية متعدد العناصر Multi-factor Authentication (MFA)	عنصر ضبط أمني؛ للتحقق من هوية المستخدم، وهو أمر يتطلب استخدام عناصر منفصلة، ومتعددة، لآليات التحقق من الهوية. وقد تتضمن آليات التحقق من الهوية العناصر الآتية: • شيء تعرفه (على سبيل المثال، كلمة المرور). • شيء تملكه (على سبيل المثال، جهاز يقوم بإنشاء شفرة رقم التعريف الشخصي، أو رسالة نصية قصيرة لسجلات تسجيل الدخول).

	• أو شيء يمثلك ويكون جزءاً منك (على سبيل المثال، بصمة الإصبع).
الحاجة إلى المعرفة Need-to-know	نهج لتقييد الوصول فحسب، لمن يحتاجون إلى معرفة ذلك، أو يحتاجون إلى استخدامه.
الشركات المصنعة للمعدات الأصلية Original Equipment Manufacturers (OEMs)	شركة تقوم بتصنيع منتجات أو بيعها، وتشمل كذلك أجزاء من منتج يمكن تسويقه بواسطة جهة مصنعة أخرى.
التحكم في الوصول بناءً على الأدوار Role-Based Access Control (RBAC)	وسيلة للتحكم في الوصول إلى الشبكة؛ بناءً على الصلاحيات والأدوار ومتطلبات المستخدمين داخل الجهة.
البيانات / المعلومات الحساسة Sensitive Data/Information	المعلومات (أو البيانات) ذات الأهمية البالغة، ومن المحتمل أن تكون سرية وفقًا لتصنيف المعلومات أو البيانات. فقدان هذه المعلومات أو سوء الاستخدام، أو الوصول غير المصرح به، أو تعديل هذه المعلومات أو البيانات؛ يمكن أن يؤثر سلبًا على المنظمة، أو الجهة المسؤولة عن هذه المعلومات أو البيانات.
أصحاب القرار في المدن الذكية Smart City Decision Makers	تشمل هذه الفئة جميع الأفراد، وأصحاب المصلحة، المكلفين بالإشراف على المدن الذكية وإدارتها؛ ممن لديهم الصلاحيات اللازمة لاتخاذ القرار.
شركاء منظومة المدن الذكية Smart City Ecosystem Partners	جميع الجهات، والجهات المسؤولة عن المخاطر، ذات العلاقة، بما في ذلك كبار رؤساء إدارة الأمن السيبراني، ومهندسي ومخططي الأمن السيبراني، وغيرهم من الموظفين، الذين يشاركون في تخطيط المدن الذكية، وتصميمها، وتنفيذها، وتشغيلها.
الجهات الخارجية Third-party	أي جهة تعمل على أنها ذات علاقة تعاقدية؛ لتقديم السلع أو الخدمات (وهذا يشمل الموردين ومقدمي الخدمات).
منظومة المدن الذكية Smart City Ecosystem	شبكة معقدة ومترابطة؛ تضم مختلف أصحاب المصلحة، والتقنيات، والخدمات التي تعمل معًا، لإنشاء بيئة حضرية فعالة، ومستدامة، وعالية الجودة.

جدول ٢: المصطلحات والتعريفات

ملحق (ب): قائمة الاختصارات

المصطلح	التعريف
API	واجهة برمجة التطبيق Application Programming Interface
CCC	ضوابط الأمن السيبراني للحوسبة السحابية Cloud Cybersecurity Controls
CISO	رئيس إدارة الأمن السيبراني Chief Information Security Officer
CGSC	إرشادات الأمن السيبراني للمدن الذكية Cybersecurity Guidelines for Smart Cities
CSCC	ضوابط الأمن السيبراني للأنظمة الحساسة Critical Systems Cybersecurity Controls
DCC	ضوابط الأمن السيبراني للبيانات Data Cybersecurity Controls
ECC	الضوابط الأساسية للأمن السيبراني Essential Cybersecurity Controls
IAM	إدارة الهوية وصلاحيات الدخول Identity and access management
ICT	تقنية المعلومات والاتصالات Information and communication technology
IoT	إنترنت الأشياء Internet-of-Things
NCA	الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority
NCS	المعايير الوطنية للتشفير National Cryptographic Standards
OEMs	شركات تصنيع المعدّات الأصلية Original Equipment Manufacturers

التقنية التشغيلية Operational Technology	**OT**
ضوابط الأمن السيبراني للأنظمة التشغيلية Operational Technology Cybersecurity Controls	**OTCC**
التحكم في الوصول بناءً على الأدوار Role-Based Access Control	**RBAC**

جدول ٣: قائمة الاختصارات


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority