الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للأنظمة الحساسة

Critical Systems Cybersecurity Controls
(CSCC -1 :2018)

مسودة

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم 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 من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

الملخص التنفيذي ٦
المقدمة ٧
الأهداف ٨
تعريف ومعايير قياس الأنظمة الحساسة ٨
تعريف الأنظمة الحساسة ٨
معايير قياس الأنظمة الحساسة ٨
مكونات الأنظمة الحساسة ٩
نطاق العمل وقابلية التطبيق ٩
نطاق عمل الضوابط ٩
قابلية التطبيق داخل الجهة (Statement of Applicability) ١٠
التنفيذ والالتزام ١٠
التحديث والمراجعة ١٠
مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة الحساسة ١١
العلاقة بين الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة الحساسة ١١
المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة ١٣
الهيكلية ١٤
ضوابط الأمن السيبراني للأنظمة الحساسة ١٥
١- حوكمة الأمن السيبراني (Cybersecurity Governance) ١٥
٢- تعزيز الأمن السيبراني (Cybersecurity Defense) ١٧
٣- صمود الأمن السيبراني (Cybersecurity Resilience) ٢٢
٤- الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity) ٢٣

ملاحق
ملحق (أ): مصطلحات وتعريفات ٢٤
ملحق (ب): قائمة الاختصارات ٣١

قائمة الجداول
جدول ١: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة ١٣
جدول ٢: مصطلحات وتعريفات ٢٣
جدول ٣: قائمة الاختصارات ٣١

قائمة الأشكال والرسوم التوضيحية
شكل ١: دليل ألوان المكونات الفرعية في الشكل ٢ ١١
شكل ٢: مكونات الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة الحساسة ١٢
شكل ٣: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة ١٣
شكل ٤: معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة ١٣
شكل ٥: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة ١٤

الملخص التنفيذي

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية؛ لذلك أتى تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

لقد جاءت مهمات هذه الهيئة واختصاصاتها ملبيةً للجوانب الاستراتيجية، ولجوانب وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعميمها على الجهات.

كما جاءت ملبيةً لجوانب التحديث ومتابعة الالتزام من قبل الجهات الحكومية وغير الحكومية بما يعزز دور الأمن السيبراني وأهميته والحاجة الملحة التي ازدادت مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

وقد نص التنظيم المشار إليه أن مسؤولية هذه الهيئة لا يُخلي أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني، وهو ما أكده الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠هـ بأن «على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن»، وكذلك أكده الأمر السامي الكريم رقم ٧٧٣٢ وتاريخ ١٤٤٠/٢/١٢ هـ.

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني بتطوير ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2018) لوضع الحد الأدنى من متطلبات الأمن السيبراني للأنظمة الحساسة في الجهات الوطنية بالإضافة إلى الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018).

وتوضح هذه الوثيقة تفاصيل ضوابط الأمن السيبراني للأنظمة الحساسة وأهدافها ونطاق العمل وآلية الإلتزام ومتابعته.

وعلى مختلف الجهات الوطنية التي تملك أو تستخدم أنظمة حساسة تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط على الأنظمة الحساسة، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ وما ورد في الأمر السامي الكريم رقم ٧٧٣٢ وتاريخ ١٤٤٠/٢/١٢ هـ.

المقدمة

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ «الهيئة») بتطوير وإصدار الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) التي وضعت الحد الأدنى من متطلبات الأمن السيبراني الواجب الالتزام المستمر بها من قبل الجهات الوطنية. ومن ثم أتى تطوير هذه الوثيقة المتضمنة لضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2018) والتي تأتي إمتداداً للضوابط الأساسية، ومكملة لها نحو تحقيق مستويات أعلى من أهداف الأمن السيبراني الوطنية الأكثر ملاءمة لما هو حساس من الأنظمة الوطنية.

وقد شمل تطوير هذه الضوابط دراسة عدد من المعايير والأطر والضوابط ذات الأهداف المماثلة لدى جهات ومنظمات دولية، وكذلك دراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، والاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، إضافة إلى تحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الوطنية.

وقد حرصت الهيئة في إعدادها لهذه الضوابط على مواءمة مكوناتها مع مكونات الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) حيث تعتبر الضوابط الأساسية للأمن السيبراني متطلب أساسي لضوابط الأمن السيبراني للأنظمة الحساسة ولا يمكن تحقيق الالتزام بها إلا من خلال تحقيق الالتزام المستمر بالضوابط الأساسية أولاً. وبناء على ذلك فقد جاءت مكونات ضوابط الأمن السيبراني للأنظمة الحساسة على النحو التالي:

- ٤ مكونات أساسية (Main Domains)
- ٢١ مكوناً فرعياً (Subdomains)
- ٢٨ ضابطاً أساسياً (Controls)

كما أن هذه الضوابط مرتبطة مع المتطلبات التشريعية والتنظيمية الوطنية والدولية ذات العلاقة.

الأهداف

تهدف هذه الضوابط إلى دعم الضوابط الأساسية للأمن السيبراني في توفير الحد الأدنى من متطلبات الأمن السيبراني للأنظمة الحساسة المبنية على أفضل الممارسات والمعايير؛ لتلبية الاحتياجات الحالية الأمنية ورفع جاهزية الجهات ضمن نطاق عمل هذه الضوابط حتى تتمكن من حماية أنظمتها الحساسة ومنع الدخول غير المصرح به لها الذي ينجم عنه مخاطر وخسائر مكلفة على المستوى الوطني.

تعريف ومعايير قياس الأنظمة الحساسة

تعريف الأنظمة الحساسة

هي أي أنظمة يؤدي تعطلها أو التغيير غير المشروع لطريقة عملها أو الدخول غير المصرح به لها أو للبيانات والمعلومات التي تحفظها أو تعالجها إلى التأثير بشكل كبير على توافر الخدمات أو أعمال الجهة أو إلى آثار اقتصادية أو مالية أو اجتماعية كبيرة على المستوى الوطني.

معايير قياس الأنظمة الحساسة

يعد النظام حساسًا إذا كان فشله أو تعطله أو الدخول غير المصرح به إليه يؤدي بشكل مباشر أو غير مباشر إلى واحد أو أكثر من الآتي:

- أضرار أو خسائر في الأرواح .
- التأثير على السمعة الوطنية.
- خسائر مالية كبيرة.
- التأثير على خدمات مقدمة لعدد كبير من المستخدمين (أكثر من 0٪ من التعداد السكاني).
- الافشاء غير المصرح به لبيانات تصنيفها سري او سري جدا.

مكونات الأنظمة الحساسة

المكونات المعتمدة للأنظمة الحساسة هي (المكونات من ١-٦ هي المكونات التقنية):

١. الشبكة:
- الأجهزة المرتبطة بالشبكة (connecting devices) وهي:
  - الموجه (Router)
  - المبدلات (Switches)
  - البوابات (Gateways)
- جدار الحماية (Firewall)

٢. قواعد البيانات

٣. وحدات الحفظ والتخزين

٤. برمجيات التكامل الوسيطة (Middleware)

٥. خوادم وأنظمة التشغيل الخاصة بها

٦. التطبيقات

٧. الأشخاص العاملون في وظائف دعم الأنظمة الحساسة (مثل: المستخدمون، مسؤولو النظام، المشغلون، المبرمجون، مقدمي الخدمات)

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تُطبَّق هذه الضوابط على الجهات الحكومية التي تملك أو تستخدم أنظمة حساسة (وتشمل الوزارات والهيئات والمؤسسات والسفارات وغيرها) سواء كانت داخل المملكة العربية السعودية أو خارجها، وكذلك الجهات والشركات التابعة للجهات الحكومية، أو جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة (Critical National Infrastructures "CNIs") أو تقوم بتشغيلها أو استضافتها، (ويشار لها جميعاً في هذا الوثيقة بـ «الجهة»). كما تُشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق داخل الجهة (Statement of Applicability)

تم إعداد هذه الضوابط بحيث تكون ملائمة لاحتياجات الأمن السيبراني لجميع الجهات والقطاعات التي تملك أو تستخدم أنظمة حساسة في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على كل جهة الالتزام بجميع الضوابط القابلة للتطبيق عليها بعد إجراء الفحوصات اللازمة قبل التطبيق.

من الأمثلة على الضوابط التي تتفاوت فيها قابلية التطبيق من جهة إلى أخرى حسب طبيعة أعمال الجهة واستخدامها للتقنيات المذكورة:

- الضوابط ضمن المكون الفرعي رقم (٤-٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity) تكون قابلة التطبيق وملزمة على الجهة التي تستخدم حالياً خدمات الحوسبة السحابية والاستضافة أو تخطط لاستخدامها.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ وما ورد في الأمر السامي الكريم رقم ٧٧٣٢ وتاريخ ١٤٤٠/٢/١٢ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط. كما يجب على الجهات تصنيف أنظمتها وتزويد الهيئة سنويًا بمعلومات الأنظمة المصنفة لديها (اسم النظام، وصف النظام، الفئة المستهدفة لخدمات النظام، وتوضيح ارتباط النظام بالانترنت أو لا).

تقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات و/أو الزيارات الميدانية للتدقيق، وفق الآلية التي تراها الهيئة مناسبة لذلك.

التحديث والمراجعة

تتولى الهيئة التحديث والمراجعة الدورية لضوابط الأمن السيبراني للأنظمة الحساسة حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى الهيئة إعلان الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

مكونات وهيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

•

العلاقة بين الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة الحساسة

تعتبر ضوابط الأمن السيبراني للأنظمة الحساسة امتداداً للضوابط الأساسية للأمن السيبراني (ECC٢٠١٨:١-). حيث تم إضافة مكون فرعي خاص بضوابط الأمن السيبراني للأنظمة الحساسة و تسع مكونات فرعية لم يضاف لها ضوابط خاصة بالأنظمة الحساسة وليست جزء من ضوابط الأمن السيبراني للأنظمة الحساسة (كما هو موضح في الشكلان ١ و٢).

	مكونات فرعية خاصة بضوابط الأمن السيبراني للأنظمة الحساسة
	مكونات فرعية مضاف لها ضوابط خاصة بالأنظمة الحساسة
	مكونات فرعية لم يضاف لها ضوابط خاصة بالأنظمة الحساسة وليست جزء من ضوابط الأمن السيبراني للأنظمة الحساسة

شكل ١: دليل ألوان المكونات الفرعية في الشكل ٢

١ - حوكمة الأمن السيبراني Cybersecurity Governance	١-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	إدارة الأمن السيبراني Cybersecurity Management
		سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٣ الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
		الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	١-٤ المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	١ - ٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
2 - تعزيز الأمن السيبراني Cybersecurity Defense	٢ - ١	إدارة الأصول Asset Management	٢ - ٢ إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢ - ٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	حماية البريد الإلكتروني Email Protection
	٢ - ٤	إدارة أمن الشبكات Networks Security Management	٢ - ٥ أمن الأجهزة المحمولة Mobile Devices Security
	٢ - ٦	حماية البيانات والمعلومات Data and Information Protection	٢ - ٧ التشفير Cryptography
	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management	٢ - ٩ إدارة الثغرات Vulnerabilities Management
	٢ - ١٠	اختبار الاختراقات Penetration Testing	٢ - ١١ إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
		إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	الأمن المادي Physical Security
	٢ - ١٢	حماية تطبيقات الويب Web Application Security	٢ - ١٣ حماية التطبيقات Application Security
٣ - صمود الأمن السيبراني Cybersecurity Resilience	٣ - ١	صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)	
٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤ - ١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤ - ٢ الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
٥ - الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

شكل ٢: مكونات الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة الحساسة

المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة

يوضح الشكل ٣ أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة.

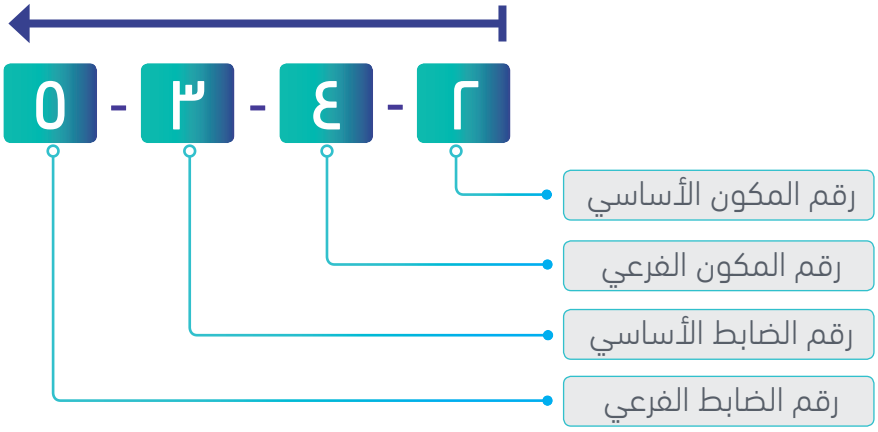
١ - حوكمة الأمن السيبراني Cybersecurity Governance	١ - ١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١ - ٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١ - ٣	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects	١ - ٤	المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	١ – ٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources		
٢ - تعزيز الأمن السيبراني Cybersecurity Defense	٢ - ١	إدارة الأصول Asset Management	٢ - ٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢ - ٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢ – ٤	إدارة أمن الشبكات Networks Security Management
	٢ - ٥	أمن الأجهزة المحمولة Mobile Devices Security	٢ - ٦	أمن الأجهزة المحمولة Mobile Devices Security
	٢ - ٧	التشفير Cryptography	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management
	٢ - ٩	إدارة الثغرات Vulnerabilities Management	٢ - ١٠	اختبار الاختراقات Penetration Testing
	٢ - ١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢ - ١٢	حماية تطبيقات الويب Web Application Security
	٢ - ١٣	حماية التطبيقات Application Security		
٣ - صمود الأمن السيبراني Cybersecurity Resilience	٣ - ١	صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)		
٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٤ - ١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	٤ - ٢	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity

شكل ٣: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة الحساسة

الهيكلية

يوضح الشكلان ٤ و٥ أدناه معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة.

شكل ٤: معنى رموز ضوابط الأمن السيبراني للأنظمة الحساسة



شكل 0: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

يوضح الجدول ١ أدناه طريقة هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة.

جدول ١: هيكلية ضوابط الأمن السيبراني للأنظمة الحساسة

١	اسم المكون الأساسي
رقم مرجعي للمكون الأساسي	
رقم مرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
رقم مرجعي للضابط	بنود الضابط

ضوابط الأمن السيبراني للأنظمة الحساسة

تفاصيل ضوابط الأمن السيبراني للأنظمة الحساسة

١ حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١	إستراتيجية الأمن السيبراني (Cybersecurity Strategy)
الهدف	ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	بالإضافة للضوابط ضمن المكون الفرعي ECC-1-1، يجب أن تضع إستراتيجية الأمن السيبراني للجهة أولوية لدعم حماية الأنظمة الحساسة الخاصة بالجهة.
١-٢	**إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)**
الهدف	ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	بالإضافة للضوابط ضمن المكون الفرعي ECC-1-5، يجب أن تشمل منهجية إدارة مخاطر الأمن السيبراني تنفيذ إجراء تقييم مخاطر الأمن السيبراني على الأنظمة الحساسة مرة واحدة سنوياً على الأقل.

١-٣	**الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Projects)**
الهدف	التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-2-6-1، يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى ما يلي: ١-٣-١-١ إجراء اختبار التحمل للتأكد من سعة المكونات المختلفة.
١-٣-٢	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-6-1، يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي: ١-٣-٢-١ إجراء مراجعة أمنية للشفرة المصدرية قبل إطلاقها (Security Source Code Review). ١-٣-٢-٢ تأمين الوصول والتخزين والتوثيق للشفرة المصدرية (Source Code) وإصداراتها. ١-٣-٢-٣ تأمين واجهة برمجة التطبيقات (Authenticated API). ١-٣-٢-٤ النقل الآمن والموثوق للتطبيقات من بيئات الاختبار الى بيئات الإنتاج (Production Environment) مع حذف أي بيانات، أو هويات، أو كلمات مرور متعلقة ببيئات الاختبار قبل النقل.
١-٤	**المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)**
الهدف	ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرّة تنظيمياً على الجهة.
الضوابط	
١-٤-١	رجوعًا للضابط ECC-1-8-1، فإن مراجعة تطبيق ضوابط الأمن السيبراني على الأنظمة الحساسة يجب أن يتم مرة سنوياً على الأقل.
١-٥	**الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)**
الهدف	ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-9-1، يجب أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى ما يلي: ١-٥-١-١ إجراء المسح الأمني المتقدم للعاملين على الأنظمة الحساسة. ١-٥-١-٢ أن يشغل الوظائف المتعلقة بالأنظمة الحساسة مواطنون ذو كفاءة عالية.

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة الأصول (Asset Management)
الهدف	للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها.
الضوابط	
٢-١-١	بالإضافة للضوابط ضمن المكون الفرعي ECC-1-2، يجب أن تشمل متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية الاحتفاظ بقائمة محدثة لجميع الأصول التابعة للأنظمة الحساسة.
٢-٢	**إدارة هويات الدخول والصلاحيات (Identity and Access Management)**
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	
٢-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-2-2، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات في الجهة بحد أدنى ما يلي: ٢-٢-١-١ تقييد الدخول عن بعد على الأنظمة الحساسة وأن يتم التفعيل بعد تأكيد الدخول عن طريق مركز العمليات الخاص بالجهة. ٢-٢-١-٢ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لجميع مستخدمي الأنظمة الحساسة. ٢-٢-١-٣ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للمستخدمين ذوي الصلاحيات الهامة والحساسة على الأنظمة الحساسة، وعلى الأنظمة المستخدمة لإدارة ومتابعة الأنظمة الحساسة المذكورة في الضابط ٢-٣-١-٤. ٢-٢-١-٤ المراجعة الدورية للصلاحيات الخاصة بالأنظمة الحساسة مرة واحدة سنوياً على الأقل. ٢-٢-١-٥ وضع سياسة آمنة لكلمة المرور ذات معايير عالية. ٢-٢-١-٦ الإدارة الآمنة لحسابات الخدمات (Service Account) مابين التطبيقات والأنظمة وتعطيل الدخول البشري التفاعلي من خلالها (Interactive login). ٢-٢-١-٧ فيما عدا مشرفي قواعد البيانات، يمنع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات، ويتم ذلك من خلال التطبيقات فقط.
٢-٢-٢	رجوعًا للضابط ECC-2-2-3-5، يجب مراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ربع سنة على الأقل.
٢-٣	**حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)**
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.
الضوابط	

٢-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-3-2، يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة الحساسة وأجهزة معالجة المعلومات الخاصة بها بحد أدنى ما يلي: ٢-٣-١-١ السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. ٢-٣-١-٢ حماية الخوادم الخاصة بالأنظمة الحساسة بتقنيات حماية النهايات المعتمدة لدى الجهة (End-point Protection). ٢-٣-١-٣ تطبيق حزم التحديثات والإصلاحات الأمنية مرة واحدة شهرياً على الأقل للأنظمة الحساسة الخارجية والمتصلة بالإنترنت وكل ثلاثة أشهر على الأقل للأنظمة الحساسة الداخلية مع اتباع آليات التغيير المعتمدة لدى الجهة. ٢-٣-١-٤ تخصيص محطات عمل (Workstations) للفريق التقني ذوي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شبكة أو خدمة أخرى (مثل: خدمة البريد الإلكتروني، الإنترنت). ٢-٣-١-٥ تشفير أي وصول إشرافي عبر الشبكة (Non-console Administartive Access) لأي من المكونات التقنية للأنظمة الحساسة باستخدام خوارزميات، وبروتوكولات التشفير ذات العلاقة. ٢-٣-١-٦ مراجعة إعدادات وتحصين الأنظمة الحساسة (Secure configuration and hardening) كل ستة أشهر على الأقل.
٢-٤	**إدارة أمن الشبكات (Networks Security Management)**
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-5-2، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي: ٢-٤-١-١ العزل المنطقي لشبكات الأنظمة الحساسة. ٢-٤-١-٢ مراجعة إعدادات وقوائم جدار الحماية (Firewall rules) كل ستة أشهر على الأقل. ٢-٤-١-٣ منع التوصيل المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة إلا بعد الفحص، والتأكد من توافر عناصر الحماية المحققة للمستويات المقبولة للأنظمة الحساسة. ٢-٤-١-٤ منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية. ٢-٤-١-٥ الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT). ٢-٤-١-٦ منع الأنظمة الحساسة من الاتصال بالإنترنت في حال كانت تقدم خدمة داخلية للجهة ولا حاجة للوصول لها بعد. ٢-٤-١-٧ الحماية من هجمات تعطيل الشبكات ("DDoS" Distrbuted Denial of Service Attack).
٢-٥	**أمن الأجهزة المحمولة (Mobile Devices Security)**
الهدف	ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة (مبدأ «BYOD»).
الضوابط	
٢-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط Ecc-3-6-2، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي: ٢-٥-١-١ منع الوصول للأنظمة الحساسة إلا لفترة مؤقتة فقط. ٢-٥-١-٢ تشفير أقراص الأجهزة المحمولة (Full Disk Encryption).

٢-٦	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٦-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-7-2، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي: ٢-٦-١-١ منع استخدام بيانات الأنظمة الحساسة في بيئة الاختبار. ٢-٦-١-٢ تصنيف جميع بيانات الأنظمة الحساسة. ٢-٦-١-٣ حماية البيانات المصنفة من خلال تقنيات منع تسريب البيانات (Data Leakage Prevention). ٢-٦-١-٤ تحديد مدة الاحتفاظ المطلوبة (Retention Period) لبيانات الأعمال المتعلقة بالأنظمة الحساسة حسب التشريعات ذات العلاقة، ويتم الاحتفاظ فقط بالبيانات المطلوبة في بيئات الإنتاج للأنظمة الحساسة. ٢-٦-١-٥ منع نقل أي من بيانات بيئة الإنتاج إلى أي بيئة أخرى.
٢-٧	التشفير (Cryptography)
الهدف	ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٧-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-8-2، يجب أن تغطي متطلبات الأمن السيبراني للتشفير بحد أدنى ما يلي: ٢-٧-١-١ تشفير جميع بيانات الأنظمة الحساسة أثناء النقل (Data-In-Transit). ٢-٧-١-٢ تشفير جميع بيانات الأنظمة الحساسة أثناء التخزين (Data-At-Rest). ٢-٧-١-٣ استخدام طرق وخوارزميات محدثة وآمنة. ٢-٧-١-٤ استخدام مفاتيح تشفير لا تقل عن ٢٥٦ بت لخوارزميات التشفير التماثلية (Symmetric). ٢-٧-١-٥ استخدام مفاتيح تشفير لا تقل عن ٢٠٤٨ بت لخوارزميات التشفير الغير تماثلية (Asymmetric).
٢-٨	إدارة النسخ الاحتياطية (Backup and Recovery Management)
الهدف	ضمان حماية بيانات ومعلومات الجهة والإعـدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-٨-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-9-2، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية بحد أدنى ما يلي: ٢-٨-١-١ نطاق عمل النسخ الاحتياطي المتصل وغير المتصل (Online and Offline backup) ليشمل جميع الأنظمة الحساسة. ٢-٨-١-٢ يجب عمل النسخ الإحتياطي على فترات زمنية مخطط لها بناءً على تقييم المخاطر للجهة، وتوصي الهيئة بأن يتم عمل النسخ الإحتياطي للأنظمة الحساسة بشكل يومي.

٢-٨-٢	رجوعًا للضابط الفرعي ECC-3-3-9-2، يجب إجراء فحص دوري كل ربع سنة على الأقل لمدى فعالية استعادة النسخ الاحتياطية الخاصة بالأنظمة الحساسة.
٢-٩	**إدارة الثغرات (Vulnerabilities Management)**
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-٩-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-10-2، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات بحد أدنى ما يلي: ٢-٩-١-١ تنصيب حزم التحديثات والإصلاحات لمعالجة الثغرات على المكونات التقنية للأنظمة الحساسة مرة واحدة شهرياً على الأقل للأنظمة الحساسة الخارجية والمتصلة بالإنترنت وكل ثلاثة أشهر على الأقل للأنظمة الحساسة الداخلية.
٢-٩-٢	رجوعًا للضابط الفرعي ECC-1-3-10-2، يجب فحص واكتشاف الثغرات على المكونات التقنية للأنظمة الحساسة مرة واحدة شهرياً على الأقل.
٢-١٠	**اختبار الاختراق (Penetration Testing)**
الهدف	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة. وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٢-١٠-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-11-2، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق بحد أدنى ما يلي: ٢-١٠-١-١ نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية للأنظمة الحساسة.
٢-١٠-٢	رجوعًا للضابط الفرعي ECC-2-3-11-2، فيجب عمل اختبار الاختراق على الأنظمة الحساسة كل ثلاثة أشهر على الأقل.
٢-١١	**إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)**
الهدف	ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة.
الضوابط	
٢-١١-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-2-12-3، يجب أن تغطي متطلبات إدارة سجلات الأحداث ومراقبة الأمن السيبراني بحد أدنى ما يلي: ٢-١١-١-١ تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة الحساسة (أنظمة التشغيل، قواعد البيانات، التطبيقات، التخزين، الشبكات). ٢-١١-١-٢ حماية السجلات، والملفات الحساسة للأنظمة من العبث أو التغيير الغير مشروع بتفعيل تقنيات إدارة تغييرات الملفات (File Integrity Management). ٢-١١-١-٣ مراقبة وتحليل سلوك المستخدم ("UBA" User Behavior Analytics).

٢-١١-٢	رجوعًا للضابط الفرعي ECC-5-3-11-2، فيجب أن لا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني على الأنظمة الحساسة عن ١٨ شهرًا.
١٢-٢	**حماية تطبيقات الويب (Web Application Security)**
الهدف	ضمان حماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٢-١	بالإضافة للضوابط الفرعية ضمن ECC-3-15-2، يجب أن تغطي متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة بحد أدنى ما يلي: ٢-١٢-١-١ الإدارة الآمنة للجلسات (Secure Session Management)، و يشمل موثوقية الجلسات (Authenticity)، و إقفال الجلسات (Lockout)، و إنهاء مهلة الجلسات (Timeout).
٢-١٢-٢	رجوعًا للضابط ECC-2-3-15-2، استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture) على أن لا يقل عدد المستويات عن ٣ (3-Tier Architecture).
١٣-٢	**حماية التطبيقات (Application Security)**
الهدف	ضمان حماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة من المخاطر السيبرانية.
الضوابط	
٢-١٣-١	يجب أن تغطي متطلبات الأمن السيبراني لحماية التطبيقات الداخلية الخاصة بالأنظمة الحساسة للجهة بحد أدنى ما يلي: ٢-١٣-١-١ استخدام مبدأ المعمارية متعددة المستويات (Multi-tier Architecture) على أن لا يقل عدد المستويات عن ٣ (3-Tier Architecture). ٢-١٣-١-٢ استخدام بروتوكولات آمنة (مثل بروتوكول HTTPS). ٢-١٣-١-٣ توضيح سياسة الاستخدام الآمن للمستخدمين. ٢-١٣-١-٤ التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين ذوي الصلاحيات الهامة والحساسة. ٢-١٣-١-٥ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، إقفال الجلسات (Lockout)، إنهاء مهلة الجلسات (Timeout).

٣ صمود الأمن السيبراني (Cybersecurity Resilience)

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience aspects of Business Continuity Management "BCM")
الهدف	ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.
الضوابط	
٣-١-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-1-3، يجب أن تغطي إدارة استمرارية الأعمال في الجهة بحد أدنى ما يلي: ٣-١-١-١ وضع مركز تعافي من الكوارث للأنظمة الحساسة. ٣-١-١-٢ إدراج الأنظمة الحساسة ضمن خطط التعافي من الكوارث. ٣-١-١-٣ إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة مرة واحدة سنوياً على الأقل.

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

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات «Outsourcing» والخدمات المدارة «Managed Services»). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٤-١-١	يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية المذكورة ضمن المكون الفرعي ECC-1-4 بحد أدنى ما يلي: ٤-١-١-١ إجراء المسح الأمني المتقدم لموظفي خدمات الإسناد العاملين على الأنظمة الحساسة. ٤-١-١-٢ خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٤-٢	**الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)**
الهدف	ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية.
الضوابط	
٤-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ECC-3-2-4، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي: ٤-٢-١-١ موقع استضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية يجب أن يكون داخل الجهة أو في خدمات الحوسبة السحابية المقدمة من قبل جهات حكومية.

ملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول ٢ أدناه بعض المصطلحات وتعريفاتها التي ورد ذكرها في هذه الضوابط.

جدول ٢ :مصطلحات وتعريفات

المصطلح	التعريف
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفها.
الأصل Asset	أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم Attack	أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.
تدقيق Audit	المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
التحقق Authentication	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
توافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
النسخ الإحتياطية Backup	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.
أحضر الجهاز الخاص بك Bring Your Own Device (BYOD)	يشير هذا المصطلح إلى سياسة جهة تسمح (سواءً بشكل جزئي أو كلي) للعاملين فيها بجلب الأجهزة الشخصية الخاصة بهم (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) إلى أماكن العمل في الجهة، واستخدام هذه الأجهزة للوصول إلى الشبكات والمعلومات والتطبيقات والأنظمة التابعة للجهة المقيدة بصلاحيات دخول.

المصطلح	التعريف
إدارة التغيير Change Management	وهو نظام لإدارة الخدمة حيث يضمن منهجاً نظامياً واستباقياً باستخدام أساليب وإجـراءات معيارية فعالة (على سبيل المثال: التغيير في البنية التحتية للجهة، وشبكاتها، إلخ). تساعد إدارة التغيير جميع الأطراف المعنيين، بما في ذلك الأفراد والفرق على حد سواء، على الانتقال من حالتهم الحالية إلى الحالة المرغوبة التالية، كما تساعد إدارة التغيير أيضاً على تقليل تأثير الحوادث ذات العلاقة على الخدمة.
الحوسبة السحابية Cloud Computing	نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي والتدخل/ التفاعل لإعداد الخدمة من مزود الخدمة. تسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. يتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة "Software-as-Service"Saas ، والنظام أو المنصة السحابية كخدمة "Platform-as-Service "PaaS ، والبنية التحتية السحابية كخدمة"Infrastructure-as-Service "IaaS. كما أن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السحابية الهجين.
انتهاك أمني Compromise	الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواءً بقصد أو بغير قصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).
السرية Confidentiality	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.
المعلومات (أو البيانات) الحساسة Confidential Data/ Information	هي المعلومات (أو البيانات) التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الجهة، والمُعدة للاستخدام من قبل جهة أو جهات محددة. وأحد الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات هو قياس مدى الضرر عند الإفصاح عنها أو الاطلاع عليها بشكل غير مصرح به أو فقدها أو تخريبها، حيث قد يؤدي ذلك إلى أضرار مادية أو معنوية على الجهة أو المتعاملين معها، أو التأثير على حياة الأشخاص ذو العلاقة بتلك المعلومات، أو التأثير والضرر بأمن الدولة أو اقتصادها الوطني أو مقدراتها الوطنية. وتشمل المعلومات الحساسة كل المعلومات التي يترتب على الإفصاح عنها بشكل غير مصرح به أو فقدها أو تخريبها مساءلة أو عقوبات نظامية.

المصطلح	التعريف
البنية التحتية الوطنية الحساسة Critical National Infrastructure	تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: • أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها -بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/أو الاجتماعية الكبيرة. • تأثير كبير على الأمن القومي و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.
التشفير Cryptography	(ويسمى أيضاً علم التشفير) وهي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
الهجوم السيبراني Cyber-Attack	الاستغلال المتعمّد لأنظمة الحاسب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار.
المخاطر السيبرانية Cyber Risks	المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات.
الصمود الأمني السيبراني Cybersecurity Resilience	القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومسببات الضرر، والتعافي منها.
الأمن السيبراني Cybersecurity	حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١١/ ٢ /١٤٣٩هـ)، فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
الفضاء السيبراني Cyberspace	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد.
تصنيف البيانات والمعلومات Data and Information Classification	تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.

المصطلح	التعريف
التعافي من الكوارث Disaster Recovery	الأنشطة والبرامج والخطط المصممة لإرجاع وظائف وخدمات الأعمال الحيوية للجهة إلى حالة مقبولة، بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.
فعالية Effectiveness	تشير الفعالية إلى الدرجة التي يتم بها تحقيق تأثير مخطط له. وتعتبر الأنشطة المخططة فعالة إذا تم تنفيذ هذه الأنشطة بالفعل، وتعتبر النتائج المخطط لها فعالة إذا تم تحقيق هذه النتائج بالفعل. يمكن استخدام مؤشرات قياس الأداء "Key Performance Indicators "KPIs لقياس وتقييم مستوى الفعالية.
كفاءة Efficiency	العلاقة بين النتائج المحققة (المخرجات) والموارد المستخدمة (المدخلات). يمكن تعزيز كفاءة العملية أو النظام من خلال تحقيق نتائج أكثر باستخدام نفس الموارد (المدخلات) أو أقل.
حدث Event	شيء يحدث في مكان محدد (مثل الشبكة والأنظمة والتطبيقات وغيرها) وفي وقت محدد.
بروتوكول نقل النص التشعبي الآمن Hyper Text Transfer Protocol Secure (HTTPS)	بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من نظام بروتوكول نقل النص التشعبي (HTTP).
هوية Identification	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة Incident	انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.
سلامة المعلومة Integrity	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
التحقق من الهوية متعدد العناصر Multi-Factor Authentication (MFA)	نظام أمني يتحقق من هوية المستخدم، يتطلب استخدام عدة عناصر مستقلة من آليات التحقق من الهوية. تتضمن آليات التحقق عدة عناصر: • المعرفة (شيء يعرفه المستخدم فقط "مثل كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").
المعمارية متعددة المستويات Multi-tier Architecture	معمارية أو بنية تُطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وتخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.
العاملون في الجهة Organization Staff	الأشخاص الذين يعملون في الجهة (بما في ذلك الموظفون الرسميون والموظفون المؤقتون والمتعاقدون).

المصطلح	التعريف
الاسناد الخارجي Outsourcing	الحصول على (السلع أو الخدمات) عن طريق التعاقد مع مورد أو مزود خدمة.
حزم التحديثات والإصلاحات Patch	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.
اختبار الاختراق Penetration Testing	ممارسة اختبار على نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.
رسائل التصيّد الإلكتروني Phishing Emails	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
الأمن المادي Physical Security	يصف الأمن المادي التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للجهة، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس أو السرقة، أو الهجمات الإرهابية). ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمن، وحدود أمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.
سياسة Policy	وثيقة تحدد بنودها التزاماً عاماً أو توجيهاً أو نية ما كما تم التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة. سياسة الأمن السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة بتنفيذ وتحسين برنامج الأمن السيبراني في الجهة، وتشتمل السياسة على أهداف الجهة فيما يتعلق ببرنامج الأمن السيبراني وضوابطه ومتطلباته وآلية تحسينه وتطويره.
الخصوصية Privacy	الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد.
إدارة الصلاحيات الهامة والحساسة Privileged Access Management	عملية إدارة الصلاحيات ذات الخطورة العالية على أنظمة الجهة والتي تحتاج في الغالب إلى تعامل خاص لتقليل المخاطر التي قد تنشأ من سوء استخدامها.
إجراء Procedure	وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة في التوافق مع المعايير والسياسات ذات العلاقة. وتعرّف الإجراءات على أنها جزء من العمليات.
عملية Process	مجموعة من الأنشطة المترابطة أو التفاعلية تحول المدخلات إلى مخرجات. وهذه الأنشطة متأثرة بسياسات الجهة.
الاستعادة Recovery	إجراء أو عملية لاستعادة أو التحكم في شيء منقطع أو تالف أو مسروق أو ضائع.

المصطلح	التعريف
مدة الاحتفاظ Retention	هي المدة الزمنية التي يجب فيها الاحتفاظ بالمعلومات أو البيانات أو سجلات الأحداث أو النسخ الاحتياطية، بغض النظر عن الشكل (ورقي أو إلكتروني أو غير ذلك).
مراجعة الإعدادات والتحصين Secure Configuration and Hardening	حماية وتحصين وضبط إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.
طرف خارجي Third-Party	أي جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موردي ومزودي الخدمات).
تهديد Threat	أي ظرف أو حدث من المحتمل أن يؤثر سلباً على أعمال الجهة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلاً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. وهذا التعريف يشمل التهديدات السيبرانية.
الثغرة Vulnerability	أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.
جدار الحماية لتطبيقات الويب Web Application Firewall	نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة من محاولات الهجوم الموجهة على تطبيقات الويب.
البرمجيات الضارة غير المعروفة مسبقاً Zero-Day Malware	عبارة عن برمجيات ضارة (Malware) غير معروفة مسبقاً، تم إنتاجها أو نشرها حديثاً. ويصعب في العادة اكتشافها بواسطة وسائل الحماية التي تعتمد على المعرفة المسبقة للبرمجيات الضارة (Signature-based Protection).
واجهة برمجة التطبيقات Application Program Interface (API)	مجموعة من الأوامر (Commands)، والدوال (Functions) ، و الكائنات (Objects)، والبروتوكولات (Protocols) التي طوّرت ليتم استخدامها من قِبل المطورين لتطوير البرمجيات أو التفاعل مع أنظمة و/أو برمجيات أخرى.
اختبار التحمل Stress Testing	اختبار يتم إجراؤه للبرمجيات (Software) والعتاد (Hardware) للتأكد من توافرها وقياس مستوى فعاليتها في الظروف الغير متوقعة.
البيانات أثناء النقل Data-In-Transit	البيانات التي تنتقل من موقع إلى آخر عن طريق أي نوع من الشبكات (مثل: الانترنت، شبكة خاصة... إلخ).
البيانات أثناء التخزين Data-At-Rest	هي البيانات المخزنة في وسائط التخزين الدائمة (مثل: الأشرطة (Tapes) و الأقراص (Disk)
خوارزميات التشفير التماثلية Symmetric Encryption Algorithms	نوع من أنواع التشفير، تستخدم مفتاح واحد للتشفير وفك التشفير.

المصطلح	التعريف
خوارزميات التشفير الغير تماثلية Asymmetric Encryption Algorithms	نوع من أنواع التشفير، تستخدم مفتاح للتشفير ومفتاح آخر لفك التشفير. ويعتبر مستوى الحماية في هذا النوع أعلى من التشفير التماثلي.
تحليل سلوك المستخدم User Behavior Analytics (UBA)	هي عملية تتبع وجمع بيانات المستخدم والقيام بتحليلها وتحديد أنماط أنشطة المستخدم للكشف عن السلوكيات الضارة.
تقنيات منع تسريب البيانات Data Leakage Prevention	هي استراتيجية للحفاظ على البيانات المهمة من الأشخاص الغير مصرح لهم بالاطلاع عليها ومنع تداولها خارج نطاق المنظمة باختلاف حالة ومكان هذه البيانات سواء كانت مخزنة على وحدات التخزين (At-Rest) أو أجهزة المستخدمين والخوادم (In-Use) أو متنقلة من خلال الشبكة (In-Transit)
هجمات تعطيل الخدمات الموزعة Distributed Denial of Service Attack	هي محاولة لتعطيل النظام وجعل خدماته غير متوافرة عن طريق إرسال طلبات كثيرة من أكثر من مصدر في نفس الوقت.
الشفرة المصدرية Source Code	مجموعة من الأوامر والتعليمات المكتوبة بلغة من لغات البرمجة.
حسابات الخدمات Service Accounts	حساب يستخدم لتشغيل خدمات أو برامج، ولديه صلاحية الوصول للبيانات والموارد.
تقنية حماية النهايات End-point Protection	تقنية تستخدم لحماية الشبكات عند الوصول لها عند بعد.

ملحق (ب): قائمة الاختصارات

يوضح الجدول ٣ أدناه معنى الاختصارات التي ورد ذكرها في هذه الضوابط.

جدول ٣ : قائمة الاختصارات

الاختصار	معناه
APT	Advanced Persistent Threat التهديدات المتقدمة المستمرة
API	Application Program Interface واجهة برمجة التطبيقات
BCM	Business Continuity Management إدارة استمرارية الأعمال
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
CNI	Critical National Infrastructure البنية التحتية الحساسة
DDoS	Distributed Denial of Service Attack هجمات تعطيل الخدمات الموزعة
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
HTTPS	Hyper Text Transfer Protocol Secure بروتوكول نقل النص التشعبي الآمن
ICS	Industrial Control System نظام التحكم الصناعي
MFA	Multi-Factor Authentication التحقق من الهوية متعدد العناصر
UBA	User Behavior Analytics تحليل سلوك المستخدم

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority