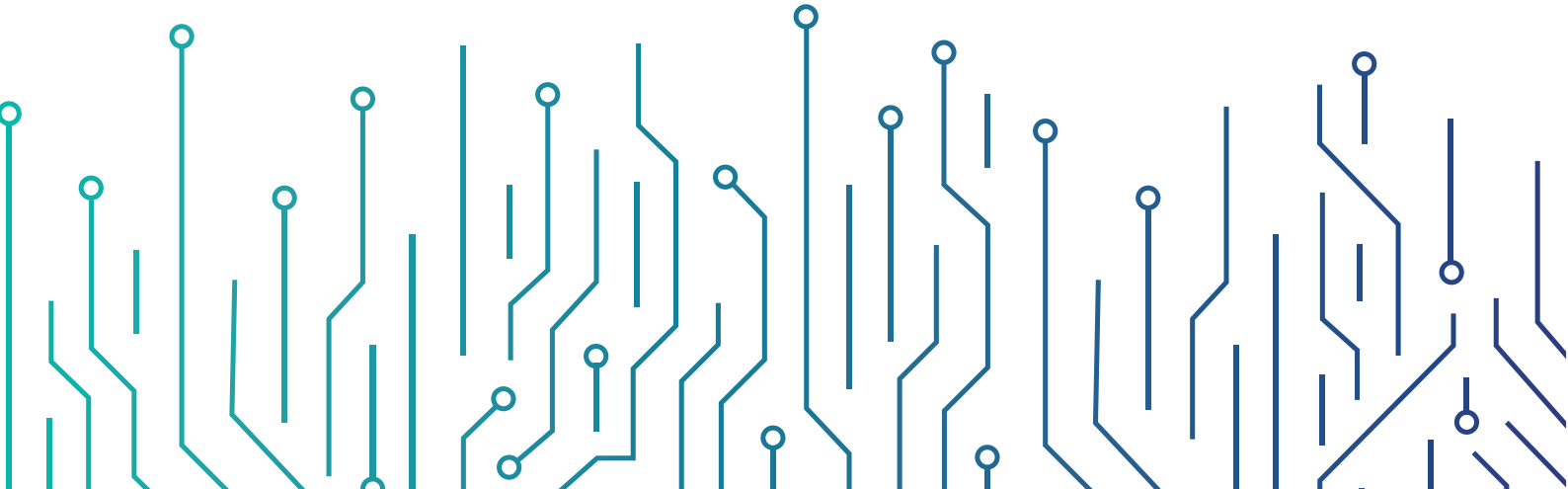
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
للعمل عن بعد

Telework Cybersecurity Controls
(TCC -1:2020)

مسودة

إشـــارة المـــشـــاركـــة: أبـيـض
تـصـنـيـف الـوثـيـقـة: مـتـــاح



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

المســتلم لا يحق له مشــاركة 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

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

الملخص التنفيذي

مع التطور التقني المستمر والمتزامن مع تطورات سوق العمل، توفرت خيارات تقنية مرنة لخلق بيئة عمل رقمية ممكنة لأداء بعض الوظائف والمهام دون الحاجة إلى الحضور إلى مقر العمل. مما يسهم في تعزيز التنمية الاقتصادية وتوفير فرص وظيفية جديدة، وزيادة الإنتاجية والأداء. ومما لا شك فيه أن تزايد اعتماد بعض الجهات على وسائل تقنية العمل عن بعد عبر الفضاء السيبراني، يزيد من التهديدات والمخاطر السيبرانية على أنظمة العمل عن بعد، مما يستوجب وضع متطلبات الأمن السيبراني للحد من هذه التهديدات والمخاطر.

جاءت مهمات الهيئة واختصاصاتها بموجب الأمر الملكي الكريم رقم (٦٨٠١) وتاريخ ١٤٣٩/٢/١١هـ وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. ومنها وضع السياسات، وآليات الحوكمة، والأطر والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني وتحديثها، وتعميمها على الجهات، ومتابعة الالتزام بها؛ بما يعزز دور الأمن السيبراني، وأهميته؛ والحاجة الملحة له التي ازدادت مع ازدياد التهديدات، والمخاطر السيبرانية، أكثر من أي وقت مضى. كما أن دور الهيئة التنظيمي لا يُخلي أي جهة عامة أو خاصة، أو غيرها من مسؤوليتها تجاه أمنها السيبراني؛ وهو ما تظمنه 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 ما أكده الأمر السامي الكريم رقم (٧٧٣٢) وتاريخ ١٤٤٠/٢/١٢ هـ.

وتماشياً مع هذا التوجه الوطني نحو العمل عن بعد؛ وبهدف الوصول إلى فضاء سيبراني سعودي آمن وموثوق يُمكن النمو والازدهار؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني للعمل عن بعد (TCC – 1: 2020) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهة من تنفيذ أعمالها عن بعد بطريقة آمنة، بالإضافة إلى الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018). وتوضح هذه الوثيقة تفاصيل ضوابط الأمن السيبراني للعمل عن بعد، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة. ويستوجب على الجهة الأخذ في الاعتبار متطلبات ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1:2019) في حال وجود أنظمة حساسة لديها تتطلب العمل عن بعد.

وعلى الجهة تنفيذ ما يحقق الالتزام الدائم، والمستمر بهذه الضوابط؛ تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني؛ وكذلك ما ورد في الأمر السامي الكريم ذي الرقم ٥٧٢٣١ والتاريخ ١٤٣٩/١١/١٠ هـ .

مقدمة

في عالم اليوم تشهد بيئة العمل متغيرات كثيرة بفعل تأثير التقنيات الحديثة ومتطلبات العمل، ومع تسارع التقنيات الناشئة كالذكاء الاصطناعي والواقع الافتراضي، زادت الشراكة بين الإنسان والتقنية مما أدى إلى تطور مفاهيم العمل عن بعد، وتقليل الروابط بين الجغرافيا والعمل الفعلي. وتبعا لتلك المتغيرات فقد شرعت المملكة في التوجه نحو تعزيز المرونة في العمل وتطوير أداء الأعمال عن بعد لتحقيق عدد من الأهداف الاقتصادية والتنموية والأمنية وفقاً لرؤية المملكة ٢٠٣٠، وهي تدرك أن هذا النوع من العمل عن بعد يتطلب وجود ضوابط أمن سيبراني تساعد على تفادي التهديدات السيبرانية المتزايدة والخروج منها بأقل ضرر في حال حدوثها بما يحافظ على المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، ومن هنا فقد حرصت الهيئة الوطنية للأمن السيبراني وفقا لتنظيمها على إصدار ضوابط الأمن السيبراني للعمل عن بعد (TCC – 1: 2020)، وتمثل هذه الضوابط الحد الأدنى من متطلبات الأمن السيبراني، الواجب الالتزام المستمر بها، من قبل الجهة التي تسمح لمنسوبيها بالعمل عن بعد.

وقد شملت مراحل إعداد هذه الضوابط مايلي:

- دراسة عدد من المعايير، والأطر والضوابط، ذات الأهداف المماثلة لدى جهات ومنظمات دولية.
- مراعاة متطلبات التشريعات، والتنظيمات والقرارات الوطنية، ذات العلاقة.
- الاطلاع على أفضل الممارسات، والتجارب في مجال الأمن السيبراني، والاستفادة منها.
- تحليل ما تم رصده من مخاطر وتهديدات وحوادث سيبرانية على المستوى الوطني.

وقد حرصت الهيئة في إعدادها لضوابط الأمن السيبراني للعمل عن بعد، على مواءمة مكوناتها مع مكونات الضوابط الأساسية للأمن السيبراني التي تعد متطلباً أساسياً لها؛ ولا يمكن تحقيق الالتزام بها إلا من خلال تحقيق الالتزام المستمر بالضوابط الأساسية للأمن السيبراني في المقام الأول كما هي مرتبطة مع المتطلبات التشريعية، والتنظيمية الوطنية والدولية، ذات العلاقة.

تتكون ضوابط الأمن السيبراني للعمل عن بعد من:

- ٣ مكونات أساسية (MAIN DOMAINS 3)
- ١٦ مكوناً فرعياً (SUBDOMAINS 16)
- ٢١ ضابطاً أساسياً (MAIN CONTROLS 21)
- ٤٢ ضابطاً فرعياً (SUBCONTROLS 42)

الأهداف

تهدف ضوابط الأمن السيبراني للعمل عن بعد إلى:

- الإسهام في رفع مستوى الأمن السيبراني على المستوى الوطني.
- تمكين الجهة من أداء أعمالها عن بعد بطريقة آمنة والتكيف مع التغييرات في بيئة الأعمال وأنظمة العمل عن بعد.
- تعزيز قدرات الأمن السيبراني والصمود، عند إتاحة العمل عن بعد ضد التهديدات السيبرانية التي قد ينجم عنها تأثيرات سلبية وخسائر مكلفة.

نطاق العمل وقابلية التطبيق

نطاق عمل الضوابط

تطبق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية وتشمل الوزارات والهيئات والمؤسسات وغيرها، والجهات والشركات التابعة لها، وتطبق على جهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها، وذلك عند إتاحة العمل عن بعد، ويشار لها جميعاً في هذه الوثيقة بـ (الجهة).

كما تشجع 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 لمتطلبات الأمن السيبراني لجميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على الجهة التي تتيح لمنسوبيها العمل عن بعد، الالتزام بجميع الضوابط القابلة للتطبيق عليها.

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

- الضوابط ضمن المكون الفرعي رقم (٣-١) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة (CLOUD COMPUTING AND HOSTING CYBERSECURITY) تكون قابلة للتطبيق؛ وملزمة للجهة التي تستخدم حالياً خدمات الحوسبة السحابية، والاستضافة، أو تخطط لاستخدامها.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة الـعـاشـرة من تنظيم الـهـيـئـة الـوطـنـيـة للأمن السيبراني، وكـذلـك مـا ورد فـي الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٤٣٩/١١/١٠ هـ، يجب على جميع الجهات ضمن نطاق عمل هذه الضوابط تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، ولا يمكن تحقيق ذلك إلا من خلال تحقيق الالتزام الدائم والمستمر بالضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وفقاً لقابلية تطبيقها في الجهة بحسب طبيعة أعمالها.

وتقوم الهيئة بتقييم التزام الجهات بما ورد في هذه الضوابط بطرق متعددة، منها: التقييم الذاتي للجهات، و/أو الزيارات الميدانية للتدقيق، وذلك وفقاً للآلية المناسبة التي تراها الهيئة.

التحديث والمراجعة

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

مكونات وهيكلية ضوابط الأمن السيبراني للعمل عن بعد

المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للعمل عن بعد

يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للعمل عن بعد. كما يوضح ملحق (أ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

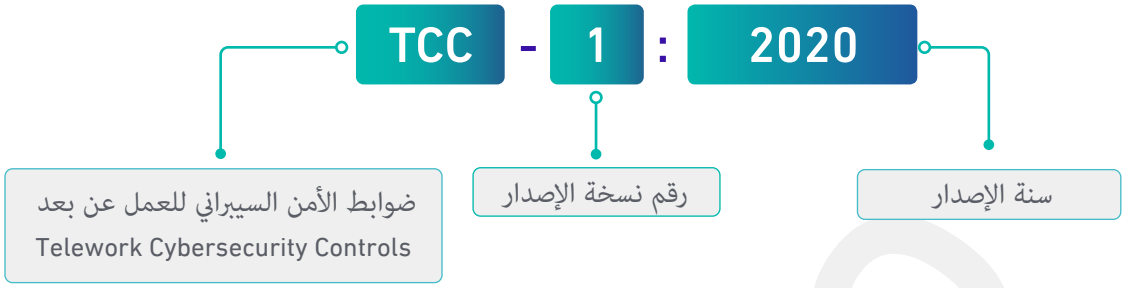
شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للعمل عن بعد

١. حوكمة الأمن السيبراني Cybersecurity Governance	١-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١-٣	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program		
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	حماية البيانات والمعلومات Data and Information Protection
	٢ - ٧	التشفير Cryptography	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management

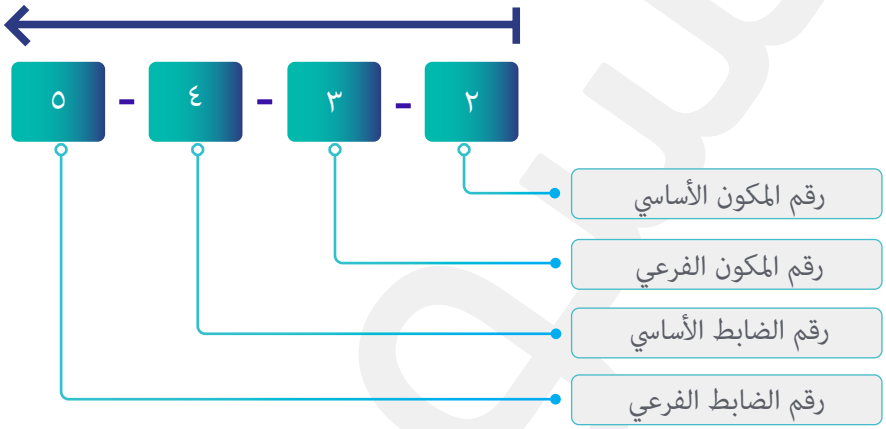
	٢ - ٩	إدارة الثغرات Vulnerabilities Management	٢ - ١٠	اختبار الاختراق Penetration Testing
	٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
٣ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	٣-١	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity		

الهيكلية

يوضح الشكلان (٢) و (٣) أدناه معنى رموز ضوابط الأمن السيبراني للعمل عن بعد.



شكل ٢ : معنى رموز ضوابط الأمن السيبراني للعمل عن بعد



شكل ٣ : هيكلية ضوابط الأمن السيبراني للعمل عن بعد

يوضح الجدول ١ طريقة هيكلية ضوابط الأمن السيبراني للعمل عن بعد.

جدول ١ : هيكلية ضوابط الأمن السيبراني للعمل عن بعد

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

ضوابط الأمن السيبراني للعمل عن بعد

تفاصيل ضوابط الأمن السيبراني للعمل عن بعد

١.حوكمة الأمن السيبراني (Cybersecurity Governance)	
١-١	سياسات وإجراءات الأمن السيبراني (Cybersecurity Policies and Procedures)
الهدف	ضمان توثيق واعتماد ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-١	رجوعا للضابط ١ -٣-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل سياسات وإجراءات الأمن السيبراني ما يأتي: ١-١-١-١ تحديد وتوثيق متطلبات وضوابط الأمن السيبراني للعمل عن بعد ضمن سياسات الأمن السيبراني للجهة.
٢-١	إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)
الهدف	ضمان إدارة مخاطر الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية للجهة، على نحو ممنهج؛ وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٢-١	بالإضافة للضوابط ضمن المكون الفرعي ١ - ٥ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يأتي: ١-١-٢-١ تقييم مخاطر الأمن السيبراني لأنظمة العمل عن بعد، مرة واحدة سنوياً، على الأقل. ١-٢-١-٢ تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح بالعمل عن بعد لأي خدمة أو نظام. ١-٢-١-٣ تضمين مخاطر الأمن السيبراني الخاصة بأنظمة العمل عن بعد والخدمات والأنظمة المسموح لها بالعمل عن بعد في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل.

١-٣	برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.
الضوابط	
١-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ١-١٠-٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المخاطر والتهديدات السيبرانية للعمل عن بعد والاستخدام الآمن للحد من هذه المخاطر والتهديدات، بما في ذلك: ١-١-٣-١ الاستخدام الآمن للأجهزة المخصصة للعمل عن بعد والمحافظة عليها وحمايتها. ٢-١-٣-١ التعامل الآمن مع هويات الدخول وكلمات المرور. ٣-١-٣-١ حماية البيانات التي يتم حفظها على الأجهزة المستخدمة للعمل عن بعد والتعامل معها حسب تصنيفها وإجراءات وسياسات الجهة. ٤-١-٣-١ التعامل الآمن مع التطبيقات والحلول المستخدمة للعمل عن بعد كالاجتماعات الافتراضية، والتعاون ومشاركة الملفات. ٥-١-٣-١ التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادت الحماية الخاصة بها. ٦-١-٣-١ تجنب العمل عن بعد باستخدام أجهزة أو شبكات عامة غير موثوقة أو أثناء التواجد في أماكن عامة. ٧-١-٣-١ الوصول المادي غير المصرح به والفقدان والسرقة والتخريب للأصول التقنية وأنظمة العمل عن بعد. ٨-١-٣-١ التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني.
٢-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠ - ٤ في الضوابط الأساسية للأمن السيبراني، فإنه يجب تدريب العاملين على المهارات التقنية اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند التعامل مع أنظمة العمل عن بعد.

٢. تعزيز الأمن السيبراني (Cybersecurity Defense)	
٢-١	إدارة الأصول (Asset Management)
الهدف	التأكد من أن الجهة لديها قائمة جرد دقيقة، وحديثة للأصول؛ تشمل التفاصيل ذات العلاقة، لجميع الأصول المعلوماتية، والتقنية المتاحة للجهة؛ وذلك من أجل دعم العمليات التشغيلية للجهة، ومتطلبات الأمن السيبراني، بهدف تحقيق سرية الأصول المعلوماتية والتقنية للجهة، وسلامتها ودقتها وتوافرها.
الضوابط	
٢-١-١	بالإضافة للضوابط ضمن المكون الفرعي ٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى، مايلي: ٢-١-١-١ تحديد وحصر الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد، وتحديثها مرة واحدة، كل سنة؛ على الأقل.
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 ماهو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.
الضوابط	
٢-٢-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول، والصلاحيات للأنظمة المستخدمة في العمل عن بعد في الجهة، بحد أدنى، مايلي: ٢-٢-١-١ إدارة صلاحيات المستخدمين للعمل عن بعد بناءً على احتياجات العمل، مع مراعاة حساسية الأنظمة ومستوى الصلاحيات، ونوعية الأجهزة المستخدمة من قبل الموظفين للعمل عن بعد. ٢-٢-١-٢ تقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت (Concurrent Logins). ٢-٢-١-٣ استخدام معايير آمنة لإدارة الهويات وكلمات المرور المستخدمة في أنظمة العمل عن بعد.
٢-٢-٢	رجوعاً للضابط الفرعي ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد، بحد أدنى مرة واحدة كل سنة.

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	
١-٣-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية أنظمة العمل عن بعد، وأجهزة المعلومات الخاصة بها، بحد أدنى، مايلي: ٢-١-٣-١ تطبيق حزم التحديثات، والإصلاحات الأمنية لأنظمة العمل عن بعد، مرة واحدة شهريا على الأقل. ٢-١-٣-٢ مراجعة إعدادات الحماية لأنظمة العمل عن بعد والتحصين (Secure Configuration and Hardening)، مرة واحدة كل سنة على الأقل. ٢-١-٣-٣ مراجعة وتحصين الإعدادت المصنعية (Default Configuration) للأصول التقنية لأنظمة العمل عن بعد، ومنها وجود كلمات مرور ثابتة، وخلفية افتراضية. ٢-١-٣-٤ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). ٢-١-٣-٥ تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.
٢-٤	إدارة أمن الشبكات (Network Security Management)
الهدف	ضمان حماية شبكات الجهة من المخاطر السيبرانية.
الضوابط	
١-٤-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٥-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة للعمل عن بعد، بحد أدنى، مايلي: ٢-١-٤-١ تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصاً على الأنظمة الداخلية، وفتحها حسب الحاجة.

	٢-١-٤-٢	مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد؛ مرة واحدة كل سنة على الأقل.
	٢-١-٤-٣	الحـــماية من هجـــمات تعـــطيل الشـــبكات (Distrbuted Denial of Service Attack <<DDoS>>) على أنظمة العمل عن بعد للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات.
	٢-١-٤-٤	الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة لأنظمة العمل عن بعد (Network APT).
٢-٥	أمن الأجهزة المحمولة (Mobile Device 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 ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة للعمل عن بعد في الجهة، بحد أدنى، مايلي:	
	٢-٥-١-١	إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management - MDM).
	٢-٥-١-٢	تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهريا، على الأقل.
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 ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات للعمل عن بعد في الجهة، بحد أدنى، مايلي:	

	٢-١-٦-١	تحديد البيانات المصنفة، حسب التشريعات ذات العلاقة، التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد.
	٢-١-٦-٢	حماية البيانات المصنفة، التي تم تحديدها في الضابط ٢-١-٦-١، باستخدام ضوابط مثل منع استخدام نوع من البيانات المصنفة أو تقنيات مثل منع تسريب البيانات (Data Leakage Prevention). ويمكن تحديد هذه الضوابط والتقنيات عن طريق تحليل المخاطر السيبرانية للجهة.
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 ٢-٨-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني للتشفير في الجهة، بحد أدنى، مايلي:	
	٢-١-٧-١	استخدام طرق وخوارزميات محدثة وآمنة للتشفير على كامل الاتصال الشبكي المستخدم للعمل عن بعد وفقاً للمستوى المتقدم (Advanced) ضمن المعايير الوطنية للتشفير (NCS – 1:2020).
٢-٨	إدارة النسخ الاحتياطية (Backup and Recovery Management)	
الهدف	ضمان حماية بيانات ومعلومات الجهة، والإعدادات 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 ٢-٩-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية لأنظمة العمل عن بعد في الجهة، بحد أدنى، مايلي:	
	٢-١-٨-١	عمل النسخ الاحتياطي على فترات زمنية مخطط لها؛ بناء على تقييم المخاطر للجهة، لأنظمة العمل عن بعد. وتوصي الهيئة بأن يتم عمل النسخ الاحتياطية، لأنظمة العمل عن بعد مرة واحدة كل أسبوع.

٢-٨-٢	رجوعاً للضابط ٢-٩-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب إجراء فحص دوري؛ كل ستة أشهر على الأقل، لتحديد مدى فعالية استعادة النسخ الاحتياطية، الخاصة بأنظمة العمل عن بعد.
٩-٢	إدارة الثغرات (Vulnerabilities Management)
الهدف	ضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال الجهة.
الضوابط	
١-٩-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٠-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، مايلي: ٢-٩-١-١ فحص الثغرات واكتشافها على أنظمة العمل عن بعد وتصنيفها حسب خطورتها، مرة واحدة كل ثلاثة أشهر على الأقل. ٢-٩-١-٢ معالجة الثغرات على أنظمة العمل عن بعد، مرة واحدة كل ثلاثة أشهر على الأقل.
١٠-٢	اختبار الاختراق (Penteration Testing)
الهدف	تقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في الجهة؛ وذلك من خلال عمل محاكاة لتقنيات الهجوم السيبراني الفعلية وأساليبه، وكذلك اكتشاف نقاط الضعف الأمنية غير المعروفةالتي قد تؤدي إلى الاختراق السيبراني للجهة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١٠-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١١-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق لأنظمة العمل عن بعد، بحد أدنى، ما يلي: ٢-١٠-١-١ نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية لأنظمة العمل عن بعد.

٢-١٠-٢	رجوعاً للضابط ٢-١١-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على أنظمة العمل عن بعد مرة واحدة كل ستة أشهر على الأقل.
٢-١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Events Logs and Monitoring Management)
الهدف	ضمان تجميع سجلات الأمن السيبراني وتحليلها ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار المترتبة على أعمال الجهة أو تقليلها.
الضوابط	
٢-١١-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، مايلي: ٢-١١-١-١ تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية وأنظمة العمل عن بعد. ٢-١١-١-٢ مراقبة سلوك مستخدمي أنظمة العمل عن بعد (User Behavior Analytics <<UBA>>) وتحليله. ٢-١١-١-٣ مراقبة سجلات الأحداث، الخاصة بالأصول التقنية وأنظمة العمل عن بعد على مدار الساعة. ٢-١١-١-٤ تحديث إجراءات مراقبة الأمن السيبراني على مدار الساعة وتطبيقها، بحيث تشمل مراقبة عمليات الدخول عن بعد، ولاسيما عمليات الدخول عن بعد من خارج المملكة والتحقق من صحتها.
٢-١١-٢	رجوعاً للضابط ٢-١٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب ألا تقل مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني لأنظمة العمل عن بعد عن ١٢ شهراً؛ حسب المتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة، مع مراعاة ماورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤٣٨/٨/١٤هـ.

الضوابط		
٢ -١٢ -١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة، بحد أدنى، مايلي:	
	٢-١٢-١-١	تحديث خطط الاستجابة لحوادث الأمن السيبراني ومعلومات التواصل داخل الجهة بما يتوافق مع حالة العمل عن بعد، وبما يضمن القدرة على التواصل وجاهزية فرق الاستجابة للحوادث.
	٢-١٢-١-٢	الحصول على المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري والتعامل معها.
	٢-١٢-١-٣	تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من مشرف القطاع أو الهيئة الوطنية للأمن السيبراني.

٣. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)	
٣-١	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	
٣-١-١	بالإضافة للضوابط الفرعية ضمن الضابط ٤ - ٢ - ٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات الحوسبة السحابية والاستضافة، بحد أدنى، ما يلي: ٣-١-١-١ موقع استضافة أنظمة العمل عن بعد يجب أن يكون داخل المملكة.

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني

تُعَد ضوابط الأمن السيبراني للعمل عن بعد؛ امتداداً للضوابط الأساسية للأمن السيبراني (ECC- 1: 2018) كما هو موضح في الشكلين (٤) و (٥)، من خلال الآتي:

- ستة عشر مكوناً فرعياً، أضيفت لها ضوابط خاصة بالأمن السيبراني للعمل عن بعد؛
- في حين أن هناك ثلاثة عشر مكوناً فرعياً، لم يضف لها ضوابط خاصة بالأمن السيبراني للعمل عن بعد.

	مكونات فرعية أضيف لها ضوابط خاصة للعمل عن بعد
	مكونات فرعية لم يضف لها ضوابط خاصة للعمل عن بعد

شكل٤: دليل ألوان المكونات الفرعية في الشكل ٥

١ - حوكمة الأمن السيبراني Cybersecurity Governance	إستراتيجية الأمن السيبراني Cybersecurity Strategy		إدارة الأمن السيبراني Cybersecurity Management
	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-١	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١ - ٢	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance		المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit
	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-٣	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
٢ - تعزيز الأمن السيبراني Cybersecurity Defense	إدارة الأصول Asset Management	٢ - ١	إدارة هويات الدخول والصلاحيات Identity and Access Management ٢ - ٢
	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٢ - ٣	حماية البريد الإلكتروني Email Protection
	إدارة أمن الشبكات Networks Security Management	٢ - ٤	أمن الأجهزة المحمولة Mobile Devices Security ٢ - ٥
	حماية البيانات والمعلومات Data and Information Protection	٢ - ٦	التشفير Cryptography ٢ - ٧

	٢ - ٨	إدارة النسخ الاحتياطية Backup and Recovery Management	٢ - ٩	إدارة الثغرات Vulnerabilities Management
	٢-١٠	اختبار الاختراق Penetration Testing	٢ - ١١	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢-١٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	الأمن المادي Physical Security	
	حماية تطبيقات الويب Web Application Security			
٣ - صمود الأمن السيبراني Cybersecurity Resilience	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	الأمن السيبراني المتعلق بالأطراف الخارجية	٤ - ١	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			

ملحق (ب): مصطلحات وتعريفات

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

جدول ٢ : مصطلحات وتعريفات

المصطلح	التعريف
أنظمة العمل عن بعد Telework Systems	هي أي أنظمة أو وسائل أو أدوات تقنية وماتحويها من مكونات تستخدم من قبل الجهة لتمكين العاملين من تأدية واجباتهم الوظيفية في غير مكان العمل الرسمي. ومن أمثلتها: أنظمة الاجتماعات الافتراضية وأنظمة التعاون ومشاركة الملفات وVPN وأنظمة الدخول عن بعد وغيرها من الأنظمة المستخدمة في بيئة العمل.
تحليل سلوك المستخدم User Behavior Analytics (UBA)	هي عملية تتبع لبيانات المستخدم وجمعها؛ والقيام بتحليلها، وتحديد أنماط أنشطة المستخدم؛ للكشف عن السلوكيات الضارة أو غير الاعتيادية.
تقنيات منع تسريب البيانات Data Leakage Prevention Technologies	هي تقنيات تستخدم للحفاظ على البيانات المهمة، من الأشخاص غير المصرح لهم بالاطلاع عليها، ومنع تداولها خارج نطاق المنظمة في أي صورة تكون عليه هذه البيانات، ومكانها؛ سواء أكانت مخزنة على وحدات التخزين (In-rest) أو أجهزة المستخدمين، والخوادم (In-Use) أو متنقلة من خلال الشبكة (In-transit).
هجمات تعطيل الخدمات الموزعة Distributed Denial of Service Attack (DDoS)	هي محاولة لتعطيل النظام، وجعل خدماته غير متوافرة؛ عن طريق إرسال طلبات كثيرة، من أكثر من مصدر في الوقت نفسه.
نظام إدارة الأجهزة المحمولة Mobile Device Management (MDM) System	هو نظام تقني يستخدم لإدارة الأجهزة المحمولة للعاملين، ومراقبتها، وحمايتها بتطبيق سياسات الأمن السيبراني.

ملحق (ج): 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
BCM	Business Continuity Management إدارة استمرارية الأعمال
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
DDoS	Distributed Denial of Service Attack هجمات تعطيل الخدمات الموزعة
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
ICS	Industrial Control System نظام التحكم الصناعي
MDM	Mobile Device Management إدارة الأجهزة المحمولة
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية
UBA	User Behavior Analytics تحليل سلوك المستخدم

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority