



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للعمل عن بعد

Telework Cybersecurity Controls
(TCC -1:2021)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

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 من داخل أو خارج الجهة خارج النطاق المحدد للاستلام.

برتقالي - مشاركة محدودة



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

أخضر - مشاركة في نفس المجتمع



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

أبيض - غير محدود



قائمة المحتويات

٦	الملخص التنفيذي
٧	المقدمة
٨	الأهداف
٩	نطاق العمل وقابلية التطبيق
٩	نطاق عمل الضوابط
٩	قابلية التطبيق داخل الجهة
١٠	التنفيذ والالتزام
١٠	التحديث والمراجعة
١١	مكونات وهيكلية ضوابط الأمن السيبراني للعمل عن بعد
١١	المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للعمل عن بعد
١٢	الهيكلية
١٤	ضوابط الأمن السيبراني للعمل عن بعد
٢٣	ملاحق
٢٣	ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني
٢٦	ملحق (ب): مصطلحات وتعريفات
٢٧	ملحق (ج): قائمة الاختصارات

قائمة الجداول

١٣	جدول ١ : هيكلية ضوابط الأمن السيبراني للعمل عن بعد
٢٦	جدول ٢ : مصطلحات وتعريفات
٢٧	جدول ٣ : قائمة الاختصارات

قائمة الأشكال والرسوم التوضيحية

١١	شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للعمل عن بعد
١٢	شكل ٢ : معنى رموز ضوابط الأمن السيبراني للعمل عن بعد
١٢	شكل ٣ : هيكلية ضوابط الأمن السيبراني للعمل عن بعد
٢٣	شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥
٢٥	شكل ٥ : مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للعمل عن بعد

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 اختصاصات الهيئة بموجب الأمر الملكي الكريم رقم (6801) وتاريخ 11/2/1439هـ، 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 يُخلى أي جهة عامة أو خاصة، أو غيرها من مسؤوليتها تجاه أمنها السيبراني؛ وهو ما تضمنه الأمر السامي الكريم رقم (57231) وتاريخ 10/11/1439هـ 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 أكدته الأمر السامي الكريم رقم (7732) وتاريخ 12/2/1440هـ.

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: 2021) 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 (57231) والتاريخ 10/11/1439هـ .

المقدمة

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. وتبعاً 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 2030م، 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 وفقاً لتنظيمها على إصدار ضوابط الأمن السيبراني للعمل عن بعد (TCC - 1: 2021)، 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. وتتكون ضوابط الأمن السيبراني للعمل عن بعد من:

- ٣ مكونات أساسية (3 Main Domains)
- ١٦ مكوناً فرعياً (16 Subdomains)
- ٢١ ضابطاً أساسياً (21 Main Controls)
- ٤٢ ضابطاً فرعياً (42 Subcontrols)

الأهداف

تهدف ضوابط الأمن السيبراني للعمل عن بعد إلى:

- 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.
- الإسهام في رفع مستوى الأمن السيبراني على المستوى الوطني.

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

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 (1-3) 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 العاشرة من تنظيم الهيئة الوطنية للأمن السيبراني، وكذلك ما ورد في الأمر السامي الكريم رقم (57231) وتاريخ 10/11/1439 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 تقييم الالتزام الخارجي، 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

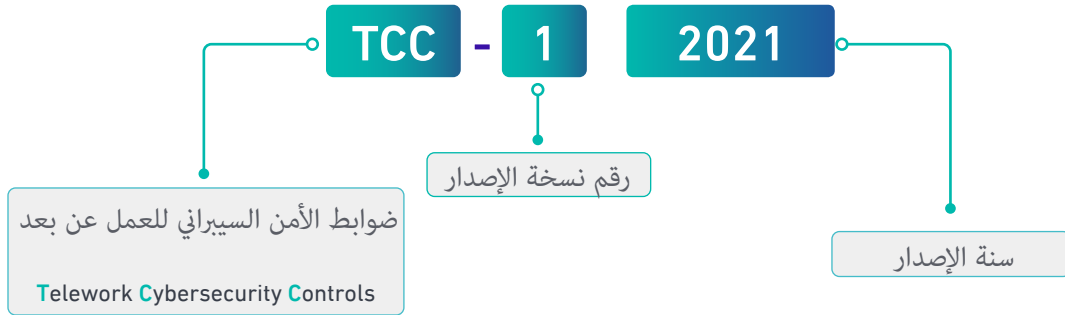
يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لضوابط الأمن السيبراني للعمل عن بعد. كما يوضح ملحق (أ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	٢-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-١	١- حوكمة الأمن السيبراني Cybersecurity Governance
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program			٣-١	
إدارة هويات الدخول والصلاحيات Identity and Access Management	٢-٢	إدارة الأصول Asset Management	١-٢	٢- تعزيز الأمن السيبراني Cybersecurity Defense
إدارة أمن الشبكات Networks Security Management	٤-٢	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٣-٢	
حماية البيانات والمعلومات Data and Information Protection	٦-٢	أمن الأجهزة المحمولة Mobile Devices Security	٥-٢	
إدارة النسخ الاحتياطية Backup and Recovery Management	٨-٢	التشفير Cryptography	٧-٢	
اختبار الاختراق Penetration Testing	١٠-٢	إدارة الثغرات Vulnerabilities Management	٩-٢	
إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	١٢-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١١-٢	
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity			١-٣	

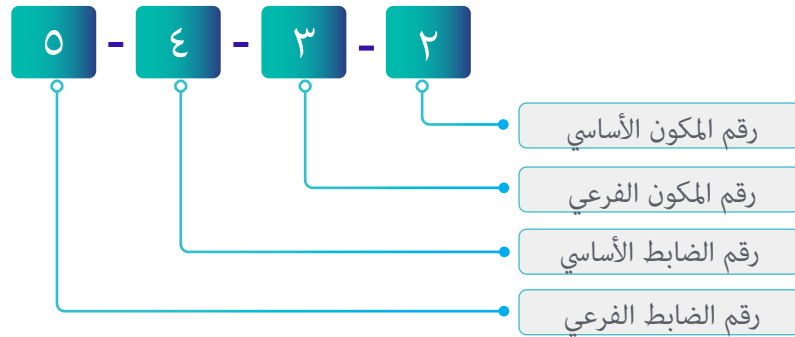
شكل ١: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للعمل عن بعد

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

يرجى ملاحظة أن الأرقام بالأخضر (مثل ١-٣-١)، هي عبارة عن إشارة مرجعية لمكون فرعي أو ضابط من الضوابط الأساسية للأمن السيبراني.

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

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

جدول ١ : هيكلية ضوابط الأمن السيبراني للعمل عن بعد

ضوابط الأمن السيبراني للعمل عن بعد

١ | حوكمة الأمن السيبراني (Cybersecurity Governance)



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

برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)	٣-١
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.	الهدف
الضوابط	
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 كاجتماعات الافتراضية، والتعاون ومشاركة الملفات. ٥-١-٣-١ التعامل الآمن مع الشبكات المنزلية والتأكد من إعدادات 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.	١-٣-١
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.	٢-٣-١

تعزيز الأمن السيبراني (Cybersecurity Defense)



إدارة الأصول (Asset Management)	١-٢
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.	الهدف
الضوابط	
بالإضافة للضوابط ضمن المكون الفرعي ١-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية، بحد أدنى، مايلي: ١-١-٢-٢ تحديد وحصر الأصول المعلوماتية والتقنية لأنظمة العمل عن بعد، وتحديثها مرة واحدة، كل سنة؛ على الأقل.	١-١-٢
إدارة هويات الدخول والصلاحيات (Identity and Access Management)	٢-٢
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.	الهدف
الضوابط	
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: ١-١-٢-٢ 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. ٢-١-٢-٢ تقييد إمكانية الوصول عن بعد لنفس المستخدم من أجهزة حاسبات متعددة في نفس الوقت (Concurrent Logins). ٣-١-٢-٢ استخدام معايير أمانة لإدارة الهويات وكلمات المرور المستخدمة في أنظمة العمل عن بعد.	١-٢-٢
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.	٢-٢-٢

حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Information Processing Facilities Protection)	٣-٢
ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية.	الهدف
الضوابط	
<p>بالإضافة للضوابط الفرعية ضمن الضابط ٣-٣-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية أنظمة العمل عن بعد، وأجهزة المعلومات الخاصة بها، بحد أدنى، مايلي:</p> <p>١-١-٣-٢ تطبيق حزم التحديثات، والإصلاحات الأمنية لأنظمة العمل عن بعد، مرة واحدة شهريا على الأقل.</p> <p>٢-١-٣-٢ مراجعة إعدادات الحماية لأنظمة العمل عن بعد والتحصين (Secure Configuration and Hardening)، مرة واحدة كل سنة على الأقل.</p> <p>٣-١-٣-٢ مراجعة وتحسين الإعدادات المصنعية (Default Configuration) للأصول التقنية لأنظمة العمل عن بعد، ومنها وجود كلمات مرور ثابتة، وخلفية افتراضية.</p> <p>٤-١-٣-٢ الإدارة الآمنة للجلسات (Secure Session Management)، ويشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).</p> <p>٥-١-٣-٢ تقييد تفعيل الخصائص والخدمات في أنظمة العمل عن بعد حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.</p>	١-٣-٢
إدارة أمن الشبكات (Networks Security Management)	٤-٢
ضمان حماية شبكات الجهة من المخاطر السيبرانية.	الهدف
الضوابط	
<p>بالإضافة للضوابط الفرعية ضمن الضابط ٣-٥-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة للعمل عن بعد، بحد أدنى، مايلي:</p> <p>١-١-٤-٢ تقييد منافذ وبروتوكولات وخدمات الشبكة المستخدمة لعمليات الدخول عن بعد، وخصوصاً على الأنظمة الداخلية، وفتحها حسب الحاجة.</p> <p>٢-١-٤-٢ مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) ذات العلاقة بأنظمة العمل عن بعد؛ مرة واحدة كل سنة على الأقل.</p> <p>٣-١-٤-٢ الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service (DDoS)) على أنظمة العمل عن بعد للحد من المخاطر الناتجة عن هجمات تعطيل الشبكات.</p> <p>٤-١-٤-٢ الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة لأنظمة العمل عن بعد (Network APT).</p>	١-٤-٢

5-2	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	
1-0-2	بالإضافة للضوابط الفرعية ضمن الضابط 3-6-2 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة للعمل عن بعد في الجهة، بحد أدنى، مايلي: 1-1-0-2 إدارة الأجهزة المحمولة وأجهزة (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة ((Mobile Device Management (MDM)). 2-1-0-2 تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهرياً، على الأقل.
6-2	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	
1-6-2	بالإضافة للضوابط الفرعية ضمن الضابط 3-7-2 في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات للعمل عن بعد في الجهة، بحد أدنى، مايلي: 1-1-6-2 تحديد البيانات المصنفة، حسب التشريعات ذات العلاقة، التي يمكن استخدامها أو الوصول إليها أو التعامل معها من خلال أنظمة العمل عن بعد. 2-1-6-2 حماية البيانات المصنفة، التي تم تحديدها في الضابط 1-1-6-2، 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.

التشفير (Cryptography)	٧-٢
الهدف	ضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات، والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية، ذات العلاقة.
الضوابط	
١-٧-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٨-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بالتشفير لدى المشتركين، بحد أدنى مايلي: ١-٧-٢-١ 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).
إدارة النسخ الاحتياطية (Backup and Recovery Management)	٨-٢
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	
١-٨-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٣-٩-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية لأنظمة العمل عن بعد في الجهة، بحد أدنى، مايلي: ١-٨-٢-١ 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 ٣-٩-٢-٣ 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.

إدارة الثغرات (Vulnerabilities Management)	٩-٢
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 ٣-١٠-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لإدارة الثغرات للأصول التقنية وأنظمة العمل عن بعد، بحد أدنى، ما يلي: ١-٩-٢-١ فحص الثغرات واكتشافها على أنظمة العمل عن بعد وتصنيفها حسب خطورتها، مرة واحدة كل ثلاثة أشهر على الأقل. ٢-٩-٢-٢ معالجة الثغرات على أنظمة العمل عن بعد، مرة واحدة كل ثلاثة أشهر على الأقل.
اختبار الاختراق (Penetration Testing)	١٠-٢
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 المعروفة التي قد تؤدي إلى الاختراق السيبراني للجهة؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١٠-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٣-١١-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لاختبار الاختراق لأنظمة العمل عن بعد، بحد أدنى، ما يلي: ١-١٠-٢-١ نطاق عمل اختبار الاختراق، ليشمل جميع المكونات التقنية لأنظمة العمل عن بعد.
٢-١٠-٢	رجوعاً للضابط ٢-٣-١١-٢ في الضوابط الأساسية للأمن السيبراني، يجب عمل اختبار الاختراق على أنظمة العمل عن بعد مرة واحدة كل سنة على الأقل.

إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)	١١-٢
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.	الهدف
الضوابط	
<p>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:</p> <p>١-١-١١-٢ تفعيل سجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية وأنظمة العمل عن بعد.</p> <p>٢-١-١١-٢ مراقبة سلوك مستخدمي أنظمة العمل عن بعد (User Behavior Analytics (UBA)) وتحليله.</p> <p>٣-١-١١-٢ مراقبة سجلات الأحداث، الخاصة بالأصول التقنية وأنظمة العمل عن بعد على مدار الساعة.</p> <p>٤-١-١١-٢ 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.</p>	١-١١-٢
رجوعاً للضابط ٢-١٢-٥ 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.	٢-١١-٢
إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)	١٢-٢
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 ١٤/٨/١٤٣٨هـ.	الهدف
الضوابط	
<p>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:</p> <p>١-١-١٢-٢ 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.</p> <p>٢-١-١٢-٢ الحصول على المعلومات الاستباقية (Threat Intelligence) ذات العلاقة بأنظمة العمل عن بعد بشكل دوري والتعامل معها.</p> <p>٣-١-١٢-٢ تنفيذ وتطبيق التوصيات والتنبيهات الخاصة بحوادث وتهديدات الأمن السيبراني الصادرة من مشرف القطاع أو الهيئة الوطنية للأمن السيبراني.</p>	١-١٢-٢

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



الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)	١-٣
الهدف	ضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعال؛ 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	١-١-٣
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: ١-١-٣-٣ موقع استضافة أنظمة العمل عن بعد يجب أن يكون داخل المملكة.	

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني

تُعد 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 يضاف لها ضوابط خاصة بالأمن السيبراني للعمل عن بعد.

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

شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥

إدارة الأمن السيبراني Cybersecurity Management		إستراتيجية الأمن السيبراني Cybersecurity Strategy		١- حوكمة الأمن السيبراني Cybersecurity Governance
أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities		سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-١	
الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects		إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	٢-١	
المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit		الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance		
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program	٣-١	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources		
إدارة هويات الدخول والصلاحيات Identity and Access Management	٢-٢	إدارة الأصول Asset Management	١-٢	
حماية البريد الإلكتروني Email Protection		حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٣-٢	
أمن الأجهزة المحمولة Mobile Devices Security	٥-٢	إدارة أمن الشبكات Networks Security Management	٤-٢	
التشفير Cryptography	٧-٢	حماية البيانات والمعلومات Data and Information Protection	٦-٢	
إدارة الثغرات Vulnerabilities Management	٩-٢	إدارة النسخ الاحتياطية Backup and Recovery Management	٨-٢	

٢- تعزيز الأمن
السيبراني
Cybersecurity
Defense

إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١١-٢	اختبار الاختراقات Penetration Testing	١٠-٢	
الأمن المادي Physical Security		إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	١٢-٢	
حماية تطبيقات الويب Web Application Security				
صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)				٣- صمود الأمن السيبراني Cybersecurity Resilience
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity	١-٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity		٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity
حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection				٥- الأمن السيبراني لأنظمة التحكم الصناعي ICS Cyberse- curity

شكل ٥. مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للعمل عن بعد

ملحق (ب): مصطلحات وتعريفات

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

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 والشبكة الخاصة الافتراضية (VPN) وأنظمة الدخول عن بعد وغيرها من الأنظمة المستخدمة في بيئة العمل.
تحليل سلوك المستخدم User Behavior Analytics (UBA)	هي عملية تتبع بيانات 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 تعطيل 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.

جدول ٢. مصطلحات وتعريفات

ملحق (ج): قائمة الاختصارات

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

الاختصار	معناه
APT	Advanced Persistent Threat التحديات المتقدمة المستمرة
BCM	Business Continuity Management إدارة استمرارية الأعمال
BYOD	Bring Your Own Device سياسة أحضر الجهاز الخاص بك
ECC	Essential Cybersecurity Controls الضوابط الأساسية للأمن السيبراني
ICS	Industrial Control System نظام التحكم الصناعي
TLP	Traffic Light Protocol بروتوكول الإشارة الضوئية

جدول ٣. قائمة الاختصارات



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

