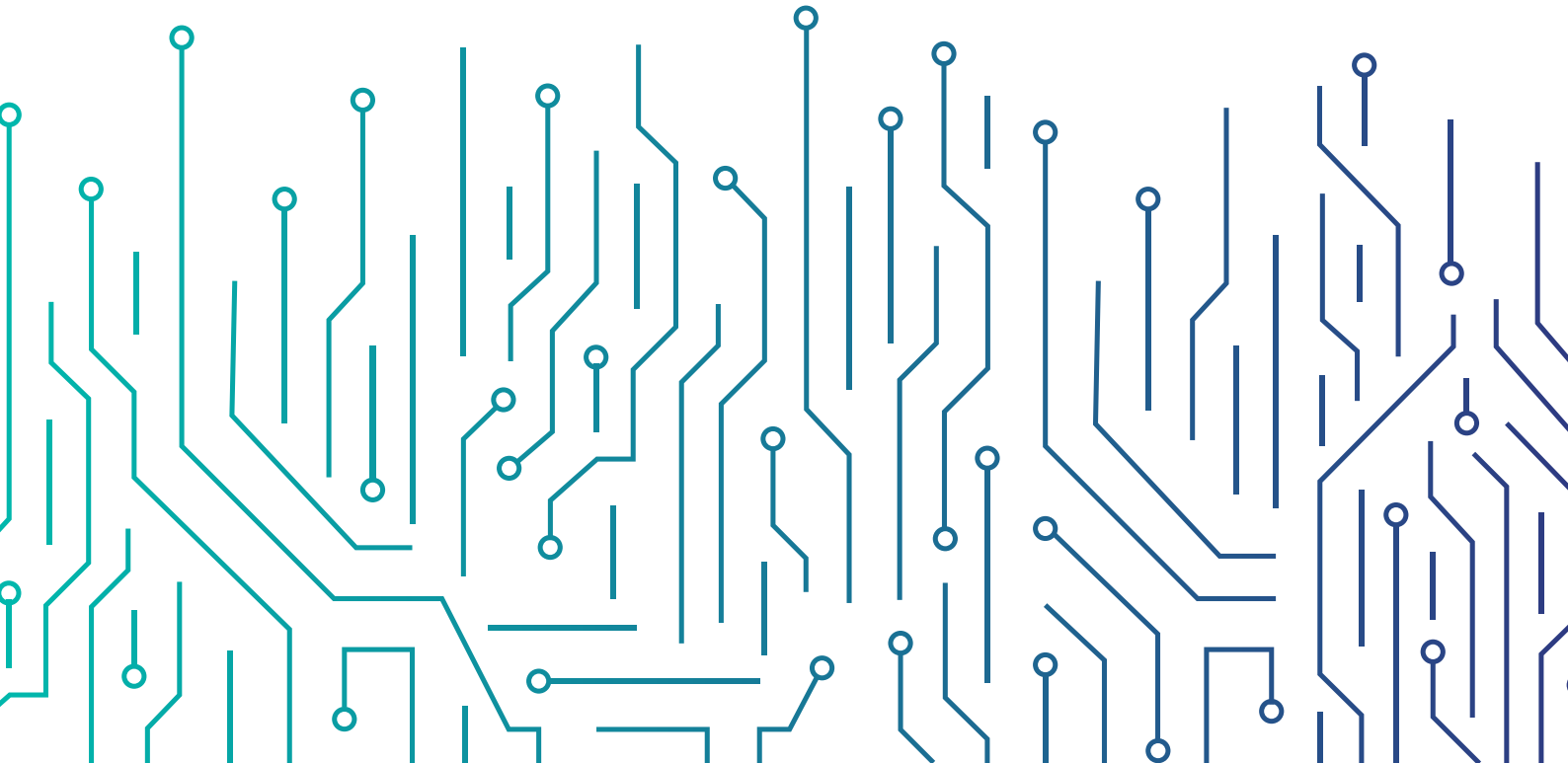
الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ضوابط الأمن السيبراني
لحسابات التواصل الاجتماعي للجهات

Organizations' Social Media Accounts Cybersecurity Controls

(OSMACC - 1 : 2021)

إشـــــارة المـشـــــاركة: أبيـــض
تصنيـــــف الوثيقـــــة: مـــتاح



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

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

الملخص التنفيذي

تعد شبكات التواصل الاجتماعي إحدى الوسائل الممكنة للتواصل السريع والفعّال مع المستفيدين مما يسهم في سرعة الاستجابة وتحسين وتسهيل تجربة المستفيدين. ومع ازدياد استخدام شبكات التواصل الاجتماعي بشكل رسمي من قبل الجهات داخل المملكة للتواصل مع المستفيدين، ازداد خطر جرائم سرقة حسابات التواصل الرسمية أو سوء استغلالها أو انتحال شخصيتها، مما يستوجب وضع متطلبات الأمن السيبراني للحد من هذه المخاطر.

وللإسهام في تقليل هذه المخاطر وتعزيز حماية حسابات التواصل الاجتماعي الرسمية، بهدف الوصول إلى فضاء سيبراني سعودي آمن وموثوق يُمكن النمو والازدهار؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC – 1: 2021) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهات من استخدام شبكات التواصل الاجتماعي بطريقة آمنة. وتوضح هذه الوثيقة تفاصيل ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات، وأهدافها، ونطاق العمل، وآلية الالتزام والمتابعة.

وعلى الجهات تنفيذ ما يحقق الالتزام الدائم، والمستمر بهذه الضوابط؛ تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة، في تنظيم الهيئة الوطنية للأمن السيبراني.

المقدمة

طوّرت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ «الهيئة») ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC – 1: 2021) بعد دراسة أفضل ممارسات الأمن السيبراني وتحليل الحوادث والهجمات السيبرانية السابقة. ويأتي ذلك ضمن اختصاصات ومهمات الهيئة حسب تنظيمها بموجب الأمر الملكي الكريم رقم (٦٨٠١) وتاريخ ١٤٣٩/٢/١١هـ «وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها».

تعد مواقع وتطبيقات شبكات التواصل الاجتماعي إحدى الوسائل الممكنة للتواصل السريع والفعّال مع المستفيدين مما يسهم في سرعة الاستجابة وتحسين تجربة المستفيدين وتسهيلها؛ مما أدى إلى استخدامها من قبل العديد من الجهات. ومع ازدياد استخدام وسائل التواصل الاجتماعي بشكل رسمي من قبل الجهات داخل المملكة للتواصل مع المستفيدين، ازداد خطر جرائم سرقة حسابات التواصل الاجتماعي الرسمية أو سوء استغلالها. بالإضافة إلى خطر جرائم انتحال شخصية الجهات الرسمية في شبكات التواصل الاجتماعي.

وللإسهام في تقليل هذه المخاطر وتعزيز حماية حسابات التواصل الاجتماعي الرسمية، بهدف الوصول إلى فضاء سيبراني سعودي آمن وموثوق يُمكن النمو والازدهار؛ قامت الهيئة الوطنية للأمن السيبراني بإعداد ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC – 1: 2021) لوضع الحد الأدنى من متطلبات الأمن السيبراني لتمكين الجهة من استخدام شبكات التواصل الاجتماعي بطريقة آمنة.

وقد حرصت الهيئة في إعدادها لضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات، 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 أنها مرتبطة مع المتطلبات التشريعية، والتنظيمية الوطنية والدولية، ذات العلاقة.

تتكون ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات من:

- 3 مكونات أساسية (3 Main Domains)
- 12 مكوناً فرعياً (12 Subdomains)
- 15 ضابطاً أساسياً (15 Main Controls)
- 38 ضابطاً فرعياً (38 Subcontrols)

الأهداف

تهدف ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات إلى:

- الإسهام في رفع مستوى الأمن السيبراني على المستوى الوطني.
- تمكين الجهات من استخدام شبكات التواصل الاجتماعي بطريقة آمنة.
- الاستعداد للاستجابة الفاعلة للحوادث السيبرانية التي قد ينجم عنها تأثيرات سلبية.

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 استخدام شبكات التواصل الاجتماعي، 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 الجهات ضمن نطاق عمل الضوابط الالتزام بجميع الضوابط القابلة للتطبيق عليها.

التنفيذ والالتزام

تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة من تنظيم الهيئة الوطنية للأمن السيبراني، 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 لحسابات التواصل الاجتماعي للجهات حسب متطلبات الأمن السيبراني والمستجدات ذات العلاقة. كما تتولى إعلان الإصدار المحدث من الضوابط لتطبيقه والالتزام به.

مكونات وهيكلية ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

المكونات الأساسية والفرعية، لضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

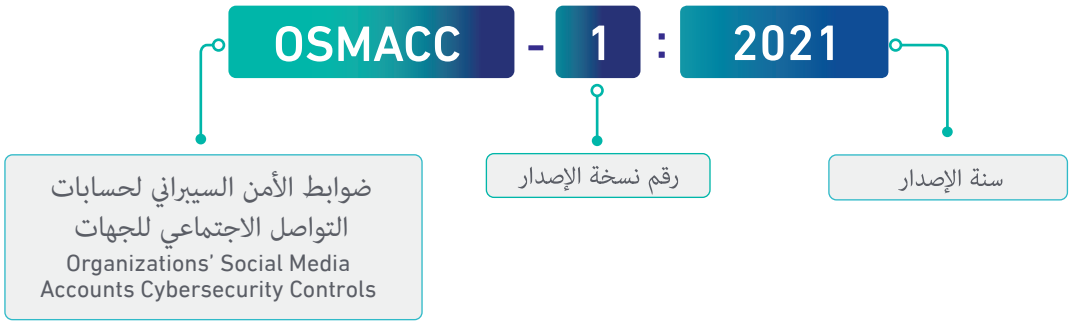
يوضح الشكل (١) أدناه، المكونات الأساسية والفرعية، لضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات. كما يوضح ملحق (أ) العلاقة مع الضوابط الأساسية للأمن السيبراني.

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	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١ - ٤	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	أمن الأجهزة المحمولة Mobile Devices Security
	٢ - ٥	حماية البيانات والمعلومات Data and Information Protection	٢ - ٦	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢ - ٧	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 بالأطراف الخارجية Third-Party Cybersecurity		

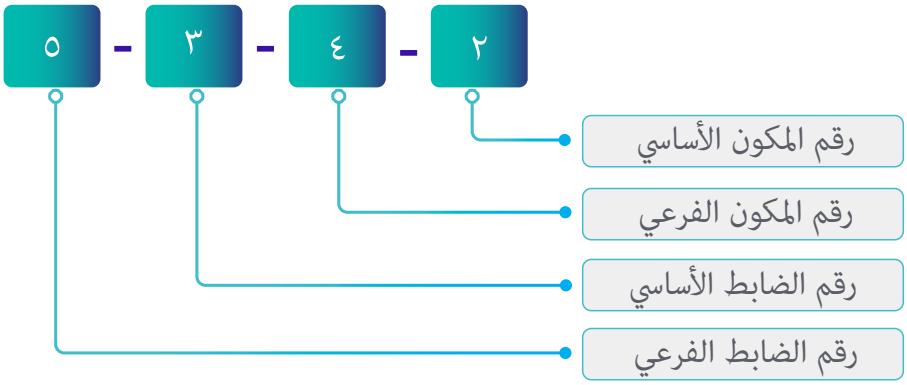
شكل ١ : المكونات الأساسية والفرعية لضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

الهيكلية

يوضح الشكلان (٢) و (٣) أدناه معنى رموز ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.



شكل ٢ : معنى رموز ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات



شكل ٣ : هيكلية ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

يوضح الجدول ١ طريقة هيكلية ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.

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

جدول ١ : هيكلية ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

1 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	رجوعاً 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 لحسابات التواصل الاجتماعي ضمن سياسات الأمن السيبراني للجهة.
١-٢	**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: ١-٢-١-١ تقييم مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل. ١-٢-١-٢ تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح باستخدام شبكات التواصل الاجتماعي. ١-٢-١-٣ تضمين مخاطر الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي والخدمات والأنظمة المستخدمة في ذلك في سجل مخاطر الأمن السيبراني الخاص بالجهة، ومتابعته مرة واحدة سنويا، على الأقل.
١-٣	**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	
١-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ – ٩ – ٤ في الضوابط الأساسية للأمن السيبراني، يجب أن تشمل متطلبات الأمن السيبراني المتعلقة بالعاملين المسؤولين عن إدارة حسابات التواصل الاجتماعي للجهة بحد أدنى ما يأتي: ١-١-٣-١ التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. ٢-١-٣-١ تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني لحسابات التواصل الاجتماعي.
١-٤	**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	
١-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠- ٣ في الضوابط الأساسية للأمن السيبراني، فإنه يجب أن يغطي برنامج التوعية بالأمن السيبراني المخاطر والتهديدات السيبرانية لحسابات التواصل الاجتماعي والاستخدام الآمن للحد من هذه المخاطر والتهديدات، بما في ذلك: ١-١-٤-١ الاستخدام الآمن للأجهزة المخصصة لحسابات التواصل الاجتماعي والمحافظة عليها وحمايتها. وعدم احتوائها على بيانات مصنفة أو استخدامها لأغراض شخصية. ٢-١-٤-١ التعامل الآمن مع هويات الدخول وكلمات المرور والأسئلة الأمنية. ٣-١-٤-١ خطة استعادة حسابات التواصل الاجتماعي والتعامل مع الحوادث السيبرانية. ٤-١-٤-١ التعامل الآمن مع التطبيقات والحلول المستخدمة لحسابات التواصل الاجتماعي. ٥-١-٤-١ عدم استخدام حسابات التواصل الاجتماعي الرسمية لأغراض شخصية مثل التصفح. ٦-١-٤-١ تجنب الدخول لحسابات التواصل الاجتماعي باستخدام أجهزة أو شبكات عامة غير موثوقة. ٧-١-٤-١ التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني.
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ١ - ١٠ - ٤ في الضوابط الأساسية للأمن السيبراني، فإنه يجب تدريب العاملين المسؤولين عن إدارة حسابات التواصل الاجتماعي للجهة على المهارات التقنية والخطط والإجراءات اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند استخدام حسابات التواصل الاجتماعي.

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 يجب تحديد وحصر حسابات التواصل الاجتماعي والأصول المعلوماتية والتقنية المتعلقة بها، 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 لحسابات التواصل الاجتماعي للجهة، بحد أدنى، مايلي: ٢-١-٢-١ استخدام حسابات التواصل الاجتماعي المخصصة للجهات، وليس الأفراد. ٢-١-٢-٢ التسجيل باستخدام معلومات رسمية (بريد إلكتروني رسمي خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي)، وعدم استخدام معلومات شخصية. ٢-١-٢-٣ توثيق حسابات التواصل الاجتماعي والمحافظة على هوية متسقة في جميع حسابات التواصل الاجتماعي المستخدمة؛ لتسهيل معرفة الحسابات الرسمية، واكتشاف حسابات الاحتيال. ٢-١-٢-٤ استخدام كلمة مرور آمنة وخاصة لكل حسابات التواصل الاجتماعي. وتغيير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل. ٢-١-٢-٥ استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول لحسابات التواصل الاجتماعي. ٢-١-٢-٦ تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.

	٢-١-٢-٧ إدارة صلاحيات المستخدمين لحسابات التواصل الاجتماعي بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، ونوعية الأجهزة والأنظمة المستخدمة. ٢-١-٢-٨ حصر صلاحيات مقدمي خدمة إدارة حسابات التواصل الاجتماعي أو المراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الجهة من الانتحال. ٢-١-٢-٩ حصر إمكانية الدخول لحسابات التواصل الاجتماعي للجهة من أجهزة محددة.
٢-٢-٢	رجوعاً للضابط الفرعي ٢-٢-٣-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة هويات الدخول والصلاحيات المستخدمة لحسابات التواصل الاجتماعي للجهة، 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	
٢-٣-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٣-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية حسابات التواصل الاجتماعي للجهة، والأصول التقنية الخاصة بها، بحد أدنى، مايلي: ٢-٣-١-١ تطبيق حزم التحديثات، والإصلاحات الأمنية لتطبيقات التواصل الاجتماعي، مرة واحدة شهرياً على الأقل. ٢-٣-١-٢ مراجعة إعدادات الحماية والتحصين لحسابات التواصل الاجتماعي للجهة والأصول التقنية الخاصة بها (Secure Configuration and Hardening)، مرة واحدة كل سنة على الأقل. ٢-٣-١-٣ مراجعة وتحصين الإعدادات المصنعية (Default Configuration) لحسابات التواصل الاجتماعي والأصول التقنية، ومنها وجود كلمات مرور ثابتة أو تسجيل الدخول المسبق، وإقفال الأجهزة (Lockout). ٢-٣-١-٤ تقييد تفعيل الخصائص والخدمات في حسابات التواصل الاجتماعي حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.
٢-٤	**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	
٢-٤-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٦-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة لحسابات التواصل الاجتماعي للجهة، بحد أدنى، مايلي: ٢-٤-١-١ إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management - MDM). ٢-٤-١-٢ تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهرياً، على الأقل.
٢-٥	**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	
٢-٥-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٧-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات لحسابات التواصل الاجتماعي للجهة، بحد أدنى، مايلي: ٢-٥-١-١ يجب أن لا تحتوي الأصول التقنية الخاصة بحسابات التواصل الاجتماعي للجهة على بيانات مصنفة، حسب التشريعات ذات العلاقة.
٢-٦	**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	
٢-٦-١	بالإضافة للضوابط الفرعية ضمن الضابط ٢-١٢-٣ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات إدارة سجلات الأحداث، ومراقبة الأمن السيبراني لحسابات التواصل الاجتماعي للجهة والأصول التقنية التابعة لها، بحد أدنى، مايلي: ٢-٦-١-١ تفعيل جميع الإشعارات وتنبيهات الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي وسجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية الخاصة بحسابات التواصل الاجتماعي. ٢-٦-١-٢ متابعة حسابات التواصل الاجتماعي و مراقبتها للتأكد من عدم نشر أي محتوى غير مصرح، أو تسجيل أي دخول غير مصرح. ٢-٦-١-٣ متابعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الجهة. ٢-٦-١-٤ المراقبة الآلية لأي تغيير في نمط الحسابات أو مؤشرات اختراق أو نشر أي محتوى غير مصرح أو انتحال هوية الجهة.

٢-٧	إدارة حـوادث وتهديـدات الأمـن السـيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضـمان تحديـد واكتشـاف حـوادث الأمـن السـيبراني في الوقـت المناسـب وإدارتهـا بشـكل فعـال والتعامـل مـع تهديـدات الأمـن السـيبراني اسـتباقياً مـن أجـل منـع أو تقليـل الآثـار المترتبـة عـلى أعـمال الجهـة، مـع مراعـاة مـاورد في الأمـر السـامي الكريـم رقـم ٣٧١٤٠ وتاريـخ ١٤٣٨/٨/١٤هـ
الضوابط	
٢-٧-١	بالإضافـة للضوابـط الفرعيـة ضمـن الضابـط ٢-١٣-٣ في الضوابـط الأساسـية للأمـن السـيبراني، يجب أن تغطـي متطلبـات إدارة حـوادث وتهديـدات الأمـن السـيبراني في الجهـة، بحـد أدنى، مايلي: ٢-٧-١-١ وضـع خطـة اسـتعادة حسـابات التواصـل الاجتماعـي والتعامـل مـع الحـوادث السـيبرانية.

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

٣-١	الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)
الهدف	ضـمان حمايـة أصـول الجهـة مـن مخاطـر الأمـن السـيبراني المتعلقـة بالأطـراف الخارجيـة (بمـا في ذلـك خدمـات الإسـناد لتقنيـة المعلومـات "Outsourcing" والخدمـات المـدارة "Managed Services"). وفقـاً للسياسـات والإجـراءات التنظيميـة للجهـة، والمتطلبـات التشريعيـة والتنظيميـة ذات العلاقـة.
الضوابط	
٣-١-١	يجـب تقييـم مـدى الحاجـة لاسـتخدام خدمـات إدارة حسـابات التواصـل الاجتماعـي (social media management) والمراقبـة الآليـة لحسـابات التواصـل الاجتماعـي أو لحمايـة هويـة الجهـة مـن الانتحـال (brand protection) ومخاطـر الأمـن السـيبراني المتعلقـة بهـا.
٣-١-٢	بالإضافـة للضوابـط الفرعيـة ضمـن الضابـط ٤ - ١ - ٢ في الضوابـط الأساسـية للأمـن السـيبراني، يجـب أن تغطـي متطلبـات الأمـن السـيبراني الخاصـة باسـتخدام خدمـات إدارة حسـابات التواصـل الاجتماعـي (social media management) والمراقبـة الآليـة لحسـابات التواصـل الاجتماعـي أو لحمايـة هويـة الجهـة مـن الانتحـال (brand protection)، بحـد أدنى، مـا يـلي: ٣-١-٢-١ بنـود المحافظـة عـلى سريـة المعلومـات (Non-Disclosure Clauses) والحـذف الآمـن مـن قبـل الطـرف الخارجـي لبيانـات الجهـة عنـد انتهـاء الخدمـة. ٣-١-٢-٢ إجراءات التواصل للإبلاغ عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني. ٣-١-٢-٣ إلـزام الطـرف الخارجـي بتطبيـق متطلبـات وسياسـات الأمـن السـيبراني لحمايـة حسـابات التواصـل الاجتماعـي للجهـة والمتطلبـات التشريعيـة والتنظيميـة ذات العلاقـة.

ملاحق

ملحق (أ): العلاقة مع الضوابط الأساسية للأمن السيبراني

تُعَد ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات؛ امتداداً للضوابط الأساسية للأمن السيبراني (ECC- 1: 2018) كما هو موضح في الشكلين (4) و (5)، من خلال الآتي:

- اثنا عشر (١٢) مكوناً فرعياً، أضيفت لها ضوابط خاصة بالأمن السيبراني لحسابات التواصل الاجتماعي للجهات؛
- في حين أن هناك سبعة عشر (١٧) مكوناً فرعياً، لم يضف لها ضوابط خاصة بالأمن السيبراني لحسابات التواصل الاجتماعي للجهات.

	مكونات فرعية أضيف لها ضوابط خاصة لحسابات التواصل الاجتماعي للجهات
	مكونات فرعية لم يضف لها ضوابط خاصة لحسابات التواصل الاجتماعي للجهات

شكل ٤: دليل ألوان المكونات الفرعية في الشكل ٥

١ - حوكمة الأمن السيبراني Cybersecurity Governance	استراتيجية 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
		١-٤	

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		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		التشفير Cryptography
		إدارة النسخ الاحتياطية Backup and Recovery Management		إدارة الثغرات Vulnerabilities Management
		اختبار الاختراق Penetration Testing	٢ - ٦	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢ - ٧	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	٣ - ١	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	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 ٥ : مكونات الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority