الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

Guide to Organizations' Social Media Accounts Cybersecurity Controls Implementation **(GOSMACC– 1 : 2023)**

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

إخلاء مسؤولية: طُور هذا الدليل الإرشادي عن طريق الهيئة الوطنية للأمن السيبراني لتمكين الجهات من تطبيق ضوابط الامن السيبراني لحسابات التواصل الإجتماعي، كما تخلي الهيئة الوطنية للأمن السيبراني مسؤوليتها من الاعتماد على هذه الوثيقة فقط؛ وتؤكد على ضرورة الأخذ بعين الاعتبار المتطلبات الخاصة بالجهة وبيئتها؛وتؤكد الهيئة الوطنية للأمن السيبراني بأن هذه الوثيقة ماهي إلا دليل إرشادي يمكن استخدامه كمثال ولا تعني بالضرورة أن تكون الطريقة الوحيدة لتطبيق الضوابط على ألا تتعارض الطرق الأخرى مع متطلبات الهيئة الوطنية للأمن السيبراني.تحتوي هذه الوثيقة على بعض الأمثلةللمخرجات ذات العلاقة بتطبيق الضوابط، ويحق للمقيم أو المدقق أن يطلب أدلة أخرى حسب ما يراه المقيم أو المدقق لضمان التأكد من تطبيق جميع الضوابط.

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 للإستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنين 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 الأشكال

مقدمة

طورت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC-1:2021) (ويشار لها في هذه الوثيقة بـ "الضوابط")، وذلك للمساهمة في تمكين الجهات الوطنية من تطبيق متطلبات الالتزام بضوابط الأمن السيبراني لحسابات التواصل الاجتماعي. حيث تم بناء هذا الدليل الإرشادي بالاعتماد على المعلومات والخبرات التي قامت الهيئة بجمعها وتحليلها منذ نشر الضوابط ومواءمة هذا الدليل الإرشادي مع أفضل الممارسات الرائدة في الأمن السيبراني لتسهيل تطبيق الضوابط في الجهات الوطنية.

الهدف

الهدف الرئيسي من هذا الدليل الإرشادي هو المساهمة في تمكين الجهات الوطنية لتحقيق متطلبات الالتزام بتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي في الجهة، وذلك بهدف رفع وتعزيز مستوى الأمن السيبراني لديها، وتقليل مخاطر الأمن السيبراني التي تنشأ من التهديدات السيبرانية الداخلية والخارجية.

نطاق العمل

نطاق العمل لهذا الدليل كما هو مذكور في ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC-1:2021) وهو:

- 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).

- تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات في ما يتعلق بتحسن الأمن السيبراني وتطويره داخل الجهة.

مكونات وهيكلية ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

يوضح الشكل رقم (١) أدناه المكونات الأساسية والفرعية لضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.

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

هيكلية الدليل الإرشادي

يوضح الشكل رقم (٢) أدناه هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.

	اسم المكون الأساسي
الرقم المرجعي للمكون الأساسي	
الرقم المرجعي للمكون الفرعي	اسم المكون الفرعي
الهدف	
الضوابط	
الرقم المرجعي للضابط	بنود الضابط
إرشادات تطبيق الضوابط:	
المخرجات المتوقعة:	

شكل ٢: هيكلية الدليل الإرشادي لتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات.

إرشادات عامة لتطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

إرشادات عامة
• حصر جميع حسابات وسائل التواصل الاجتماعي في جميع منصات التواصل الاجتماعي التي تستخدمها الجهة، ومراجعتها بشكل دوري. • تحديد الأصول التقنية والتطبيقات والأنظمة التي تتعامل مع حسابات وسائل التواصل الاجتماعي في جميع المنصات الخاصة بالجهة. • تحديد وتوثيق متطلبات الأمن السيبراني لحسابات التواصل الاجتماعي والأدوار والمسؤوليات المتعلقة بها، واعتمادها من قبل صاحب الصلاحية ومراجعتها بشكل دوري. • مراجعة الدليل الإرشادي لتطبيق الضوابط الأساسية للأمن السيبراني والعمل على تطبيق الضوابط ذات العلاقة بضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات. • وضع خطة لتطبيق الضوابط لحسابات التواصل الاجتماعي في جميع المنصات ، ومتابعتها بشكل مستمر.

إرشادات تطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

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	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.
		أدوات الأمن السيبراني: • نموذج إجراء تطوير وثائق الأمن السيبراني • **إرشادات تطبيق الضوابط:** • تحديد وتوثيق متطلبات الأمن السيبراني لحسابات التواصل الاجتماعي ضمن سياسات الأمن السيبراني للجهة. • التأكّد من نشر الوثيقة للعاملين في الجهة والأطراف المعنية بها الداخليين والخارجيين، من خلال قنوات الاتصال المعتمدة وذلك حسب النطاق المحدد في السياسة (مثال: نشر السياسات والإجراءات عن طريق البوابة الداخلية للجهة، أو نشر السياسات والإجراءات عن طريق البريد الإلكتروني).
		المخرجات المتوقعة: • وثيقة تحتوي على متطلبات الأمن السيبراني لحسابات التواصل الاجتماعي معتمدة من صاحب الصلاحية. • التأكد على العمل بالوثيقة بالإضافة إلى نشر الوثيقة للعاملين والأطراف المعنية.

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 لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل.
		أدوات الأمن السيبراني: • نموذج سياسة إدارة مخاطر الأمن السيبراني • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • إجراء تقييم لمخاطر الأمن السيبراني لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل بحيث يتم اكتشاف و تحديد ومعالجة المخاطر المحتملة لحسابات التواصل الإجتماعي. • مراجعة المخاطر المحددة لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل.
		المخرجات المتوقعة: • تقرير تقييم المخاطر لجميع حسابات وسائل التواصل الاجتماعي الخاصة بالجهة وفقًا لمتطلبات الأمن السيبراني في الجهة و مراجعتة دوريا حسب التاريخ المحدد.
	٢-١-٢-١	تقييم مخاطر الأمن السيبراني عند التخطيط وقبل السماح باستخدام شبكات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة مخاطر الأمن السيبراني • نموذج إجراء إدارة مخاطر الأمن السيبراني

		• نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط وقبل السماح باستخدام شبكات التواصل الاجتماعي. **المخرجات المتوقعة:** • تقرير تقييم المخاطر لجميع حسابات وسائل التواصل الاجتماعي عند التخطيط وقبل السماح باستخدامها وفقًا لمتطلبات الأمن السيبراني في الجهة.
	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. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة إدارة مخاطر الأمن السيبراني • نموذج إجراء إدارة مخاطر الأمن السيبراني • نموذج سجل مخاطر الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي للجهة. • التأكد من أن مخاطر الأمن السيبراني المتعلقة بحسابات التواصل الاجتماعي قد تم تضمينها في سجل مخاطر الأمن السيبراني. • متابعة مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي، مرة واحدة سنويا على الأقل. **المخرجات المتوقعة:** • تضمين مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي في سجل المخاطر. • مراجعة سجل المخاطر الذي يحتوي على مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي مرة واحدة سنوياً، 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:	
	١-٣-١-١	التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني • نموذج سياسة الاستخدام المقبول للأصول • نموذج سياسة الأمن السيبراني للموارد البشرية **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل إستخدام حسابات التواصل الاجتماعي، ما يجب فعله وما لا يجب فعله في وسائل التواصل الاجتماعي، إدارة الوصول الى حسابات التواصل الاجتماعي، الخصوصية على حسابات التواصل الاجتماعي، أنواع الجرائم الإلكترونية التي يمكن أن تكون حسابات التواصل الاجتماعي للجهة عرضة لها، هوية الجهة على وسائل التواصل الاجتماعي وما إلى ذلك. • يجب أن يتعهد جميع الأفراد المسؤولين بإدارة حسابات وسائل التواصل الاجتماعي بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • التوعية بالأمن السيبراني للعاملين والمسؤولين عن إدارة حسابات التواصل الاجتماعي بشكل دوري، والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج التوعية بالأمن السيبراني موثق ومعتمد لوسائل التواصل الاجتماعي الخاصة بالجهة. • سجلات دورات التوعية / التدريب التي يتم إجراؤها بشكل دوري.

	١-٣-١-٢	تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني لحسابات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: ● نموذج سياسة الأمن السيبراني للموارد البشرية ● نموذج الالتزام بسياسات الأمن السيبراني ● نموذج اتفاقية السرية **إرشادات تطبيق الضوابط:** ● تطبيق جميع متطلبات الأمن السيبراني ومن ضمنها متطلبات حسابات وسائل التواصل الاجتماعي. ● التحقق من الامتثال لمتطلبات الأمن السيبراني لحسابات التواصل الاجتماعي بشكل دوري، على النحو المحدد في سياسات وإجراءات الجهة. ● التأكد من أن جميع الموظفين قاموا بقراءة سياسة الاستخدام المقبول والإقرار عليها.
		المخرجات المتوقعة: ● تقرير الامتثال لمتطلبات الأمن السيبراني لحسابات التواصل الاجتماعي الخاصة بالجهة. ● عينة من تطبيق متطلبات الأمن السيبراني لحسابات التواصل الاجتماعي. ● عينة من نماذج سياسة الاستخدام المقبول الموقعة من قبل موظفي الجهة.
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.
		أدوات الأمن السيبراني: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل: الاستخدام الآمن للأجهزة المستخدمة لحسابات التواصل الاجتماعي الخاصة بالجهة، ومراجعة إعدادات الحماية والتحصين للأجهزة المخصصة لحسابات التواصل الاجتماعي، وحماية البيانات على الأجهزة المخصصة لحسابات التواصل الاجتماعي، وعدم استخدام البيانات عالية الحساسية أو البيانات الشخصية الخاصة بالموظفين على الأجهزة المخصصة لحسابات التواصل الاجتماعي. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن أساليب الاستخدام الآمن للأجهزة المخصصة لحسابات التواصل الاجتماعي والمحافظة عليها وحمايتها، وعدم احتوائها على بيانات مصنفة أو استخدامها لأغراض شخصية. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
	٢-١-٤-١	التعامل الآمن مع هويات الدخول وكلمات المرور والأسئلة الأمنية.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:**

		• تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل: إدارة الهويات لحسابات التواصل الاجتماعي، وسياسة كلمة المرور، والتعامل الآمن مع معلومات تسجيل الدخول، وإعداد أسئلة الأمان، والتحقق من الهوية متعدد العناصرعلى حسابات وسائل التواصل الاجتماعي. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن أساليب التعامل الآمن مع هويات الدخول وكلمات المرور والأسئلة الأمنية والوصول إلى حسابات وسائل التواصل الاجتماعي. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
	١-٤-١-٣	خطة استعادة حسابات التواصل الاجتماعي والتعامل مع الحوادث السيبرانية.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل: إدارة حوادث وتهديدات الأمن السيبراني لحسابات التواصل الاجتماعي، وتحديد الحادثة، والإبلاغ عن الأنشطة المشبوهه على حسابات وسائل التواصل الاجتماعي، وخطة استعادة حسابات التواصل الاجتماعي. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب. • انشاء و توثيق خطة لاستعادة حسابات التواصل الإجتماعي مع ضمان وجود التالي في خطة الاستعادة لحسابات التواصل الاجتماعي: - معلومات التواصل الخاصة بفريق الاستجابة لحوادث الأمن السيبراني. - إخطار فريق الاستجابة للحوادث في الوقت المناسب.

		- توثيق الحادثة بعد استعادة الحساب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن التوعية بخطط استعادة حسابات التواصل الاجتماعي والتعامل مع الحوادث السيبرانية. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة. • خطة موثقة لاستعادة حسابات التواصل الاجتماعي الخاصة بالجهة
	٤-١-٤-١	التعامل الآمن مع التطبيقات والحلول المستخدمة لحسابات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل تطبيقات وتقنيات حلول الأمن السيبراني لحسابات التواصل الاجتماعي، ومراقبة وتسجيل الأحداث على تطبيقات حسابات التواصل الاجتماعي. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن محتوى توعوي للتعامل الآمن مع التطبيقات والحلول المستخدمة لحسابات التواصل الاجتماعي. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
	٤-١-٤-١-٥	عدم استخدام حسابات التواصل الاجتماعي الرسمية لأغراض شخصية مثل التصفح.

		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل: طرق استخدام حسابات وسائل التواصل الاجتماعي الخاصة بالجهة، وآداب استخدام حسابات التواصل الاجتماعي، وعدم الاستخدام الشخصي لحسابات التواصل الاجتماعي الخاصة بالجهة. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن محتوى توعوي لضمان عدم استخدام حسابات التواصل الاجتماعي الرسمية لأغراض شخصية مثل التصفح. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
	٦-١-٤-١	تجنب الدخول لحسابات التواصل الاجتماعي باستخدام أجهزة أو شبكات عامة غير موثوقة.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل: الوصول إلى حسابات التواصل الاجتماعي الخاصة بالجهة، وتجنب الأجهزة / الشبكات العامة أو تلك التي لم تحددها سياسات الجهة، والمخاطر المرتبطة بالوصول إلى حسابات التواصل الاجتماعي الخاصة بالجهة من خلال أجهزة أوشبكات عامة غير موثوق بها. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي.

		• عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن منع الوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة بالجهة من خلال أجهزة أو شبكات عامة غير موثوق بها. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
	١-٤-١-٧	التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في الجهة حال الاشتباه بتهديد أمن سيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق برنامج للتوعية بالأمن السيبراني، والذي يجب أن يحتوي على موضوعات مثل الاستجابة لحوادث وتهديدات الأمن السيبراني لحسابات التواصل الاجتماعي، وكيفية الاتصال مباشرة مع الإدارة المعنية بالأمن السيبراني في حالة وجود أي تهديدات. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال برنامج التوعية بالأمن السيبراني لحسابات التواصل الاجتماعي. • عمل برنامج التوعية بالأمن السيبراني المتعلق بوسائل التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
		المخرجات المتوقعة: • برنامج توعية موثق ومعتمد لوسائل التواصل الاجتماعي يتضمن كيفية التواصل مباشرة مع الإدارة المعنية بالأمن السيبراني في حال الاشتباه بتهديد أمن سيبراني. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.
١-٤-٢		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.

	أدوات الأمن السيبراني ذات العلاقة: • خطة برنامج التوعية بالأمن السيبراني **إرشادات تطبيق الضوابط:** • تطوير وتوثيق محتوى تدريبي للموظفين المسؤولين عن إدارة حسابات التواصل الاجتماعي للجهة، ويجب أن يحتوي المحتوى على المهارات المطلوبة لإدارة الحسابات، كيفية تطبيق ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي وفقا لسياسات وإجراءات الجهة، وتشغيل ومراقبة الأنشطة على حسابات وسائل التواصل الاجتماعي لإدارة التهديدات. • يجب أن يتعهد جميع الموظفين في الجهة بإكمال التدريب المتعلق بإدارة حسابات التواصل الاجتماعي. • تقديم المحتوى التدريبي المتعلق بإدارة حسابات التواصل الاجتماعي بشكل دوري والاحتفاظ بسجلات التدريب.
	المخرجات المتوقعة: • منهج تدريبي موثق ومعتمد للموظفين المسؤولين عن إدارة حسابات التواصل الاجتماعي للجهة. • عينة من المحتوى والمواضيع التوعوية المقدمة لموظفي الجهة.

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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة الأصول • نموذج معيار إدارة الأصول بحيث يشمل إرشادات التصنيف **إرشادات تطبيق الضوابط:** • تحديد وتوثيق قائمة بجميع حسابات التواصل الاجتماعي على كل منصات التواصل الاجتماعي التي تستخدمها الجهة، وحصر الأصول المعلوماتية والتقنية المتعلقة بها. • الاحتفاظ بسجل حصر لحسابات التواصل الاجتماعي والأصول المعلوماتية والتقنية المتعلقة بها ومراجعتها بشكل دوري، مرة واحدة كل سنة؛ على الأقل.
		المخرجات المتوقعة: • سجل حصر موثق ومعتمد لأصول حسابات التواصل الاجتماعي والأصول المعلوماتية والتقنية المتعلقة بها.

		• تقرير دوري لمراجعة سجل حصر حسابات التواصل الاجتماعي والأصول المعلوماتية والتقنية المتعلقة بها.
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		
١-٢-٢	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:	
	١-١-٢-٢	استخدام حسابات التواصل الاجتماعي المخصصة للجهات، وليس الأفراد.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • تحديد حسابات التواصل الاجتماعي الخاصة بالجهة في جميع منصات وسائل التواصل الاجتماعي، ويستثنى من ذلك الحسابات الخاصة بالأفراد ذوي الشخصية الاعتبارية (مثل: أصحاب المعالي والسعادة). • التأكد من استخدام تلك الحسابات وإدارتها بشكل آمن.
		المخرجات المتوقعة: • عينة من حسابات التواصل الاجتماعي المستخدمة في الجهة للتحقق من أنها مخصصة فقط للجهات وليس للأفراد. ويُشار إلى أن الأفراد المقصود بهم في الجهة قد يكونون مسؤولين عن إدارة حسابات التواصل الاجتماعي الخاصة بالجهة، أو قد يكونون مجرد مستخدمين عاديين لهذه الحسابات مثل: الموظفين او العملاء والتابعين لهذه الجهة. وفي كلتا الحالتين، ينبغي عليهم الالتزام بسياسة الجهة بشأن استخدام حسابات التواصل الاجتماعي.

	٢-١-٢-٢	التسجيل باستخدام معلومات رسمية (بريد إلكتروني رسمي خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي)، وعدم استخدام معلومات شخصية.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التحقق من أن حسابات التواصل الاجتماعي الخاصة بالجهة مسجلة باستخدام البريد الإلكتروني الرسمي ورقم الهاتف المحمول الرسمي المخصصين فقط لحسابات التواصل الاجتماعي. والتأكد من عدم استخدام المعلومات الشخصية لأي فرد لإنشاء حسابات التواصل الاجتماعي للجهة.
		المخرجات المتوقعة: • عينة من المعلومات الرسمية المستخدمة في تسجيل حسابات التواصل الاجتماعي.
	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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التحقق من أن حسابات التواصل الاجتماعي الخاصة بالجهة تم توثيقها في خلال منصات التواصل الاجتماعي المستخدمة من قبل الجهة، والتأكد من أن حسابات التواصل الاجتماعي لها هوية متسقة في جميع منصات وسائل التواصل الاجتماعي.
		المخرجات المتوقعة: • عينة من حسابات التواصل الاجتماعي التي تستخدمها الجهة والتي تم توثيقها في منصات التواصل الاجتماعي.

	٢-٢-١-٤	استخدام كلمة مرور آمنة وخاصة لكل حسابات التواصل الاجتماعي. وتغيير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات • نموذج معيار إدارة هويات الدخول والصلاحيات، بحيث يشمل إدارة كلمات المرور **إرشادات تطبيق الضوابط:** • التحقق من تسجيل كل حساب على وسائل التواصل الاجتماعي باستخدام كلمات مرور آمنة ومختلفة عن كلمات المرور المستخدمة لحسابات وسائل التواصل الاجتماعي الأخرى. بالإضافة إلى التغيير الدوري لكلمات المرور وعدم إعادة استخدام كلمات مرور تم استخدامها من قبل.
		المخرجات المتوقعة: • ضوابط موثقة لحسابات التواصل الاجتماعي تحدد متطلبات الأمن السيبراني لإدارة كلمات المرور لحسابات وسائل التواصل الاجتماعي. • التقارير الدورية التي توضح تغيير كلمات المرور لحسابات التواصل الاجتماعي.
	٢-٢-١-٥	استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول لحسابات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التحقق من أن حسابات التواصل الاجتماعي الخاصة بالجهة تستخدم تقنية التحقق من الهوية متعدد العناصر لعمليات تسجيل الدخول. ويجب أن يتم تسجيل الدخول إلى حسابات التواصل الاجتماعي باستخدام أجهزة ومعلومات تسجيل الدخول الخاصة بالجهة.

		المخرجات المتوقعة: • عينة من حسابات التواصل الاجتماعي التي تستخدم تقنية التحقق من الهوية متعدد العناصر لعمليات تسجيل الدخول.
	٢-٢-١-٦	تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التحقق من أن حسابات التواصل الاجتماعي الخاصة بالجهة تستخدم أسئلة الأمان. والقيام بمراجعة أسئلة الأمان وتحديثها بشكل دوري، أو بعد استخدامها وتوثيقها بشكل آمن وضمان عدم الوصول إليها الا من قبل الأفراد المصرح لهم فقط.
		المخرجات المتوقعة: • ضوابط موثقة لحسابات التواصل الاجتماعي تحدد متطلبات الأمن السيبراني التي تتطلب إعداد وتحديث أسئلة الأمان لحسابات التواصل الاجتماعي الخاصة بالجهة. • أسئلة أمنية موثقة في ملف بمكان آمن مع إمكانية عدم الوصول إليها الا من قبل الأفراد المصرح لهم فقط.
	٢-٢-١-٧	إدارة صلاحيات المستخدمين لحسابات التواصل الاجتماعي بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، ونوعية الأجهزة والأنظمة المستخدمة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:**

		• التحقق من أن صلاحيات الوصول إلى حسابات التواصل الاجتماعي يتم منحها للموظفين بناء على احتياج العمل، وحساسية الحسابات، ونوعية الأجهزة والأنظمة المستخدمة.
		المخرجات المتوقعة: • ضوابط موثقة لحسابات التواصل الاجتماعي تحدد متطلبات الأمن السيبراني التي تتطلب تقييد حق الوصول إلى حسابات التواصل الاجتماعي داخل الجهة مع مراعاة احتياج العمل، وحساسية الحسابات، ونوعية الأجهزة والأنظمة المستخدمة. • إجراءات موافقة محددة لمنح الصلاحيات لحسابات التواصل الاجتماعي في الجهة. • عينة من طلبات منح الصلاحيات لحسابات التواصل الاجتماعي المعتمدة والتي تم تنفيذها سابقاً.
	٢-٢-١-٨	حصر صلاحيات مقدمي خدمة إدارة حسابات التواصل الاجتماعي أو المراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الجهة من الانتحال.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد صلاحيات مزودي خدمة إدارة حسابات التواصل الاجتماعي أو مراقبة وسائل التواصل الاجتماعي أو حماية هوية الجهة من الانتحال.
		المخرجات المتوقعة: • ضوابط موثقة لحسابات التواصل الاجتماعي تحدد متطلبات الأمن السيبراني التي تتطلب تقييد حق الوصول إلى حسابات التواصل الاجتماعي لمزودي الخدمات. • عينة من الصلاحيات التي تم منحها لموزودي الخدمات على حسابات التواصل الاجتماعي.

	٢-٢-١-٩	حصر إمكانية الدخول لحسابات التواصل الاجتماعي للجهة من أجهزة محددة. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • التحقق من أن حق الوصول إلى حسابات التواصل الاجتماعي الخاصة بالجهة محصور على أجهزة محددة. • استخدام منصات وخدمات إدارة حسابات التواصل الاجتماعي. **المخرجات المتوقعة:** • ضوابط موثقة لحسابات التواصل الاجتماعي تحدد متطلبات الأمن السيبراني التي تتطلب تقييد حق الوصول إلى حسابات التواصل الاجتماعي الخاصة بالجهة من خلال أجهزة محددة. • عينة من إعدادات حسابات التواصل الاجتماعي التي تضمن إمكانية الدخول للحسابات من أجهزة محددة فقط. • عينة من إعدادات منصات و خدمات إدارة حسابات التواصل الاجتماعي التي تسمح بتحديد الأجهزة التي يمكنها الدخول لحسابات التواصل الاجتماعي للجهة.
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. **أدوات الأمن السيبراني ذات العلاقة:** • نموذج سياسة إدارة هويات الدخول والصلاحيات **إرشادات تطبيق الضوابط:** • حصر وتوثيق هويات الدخول والصلاحيات للمسؤولين عن حسابات التواصل الاجتماعي. • الحفاظ على هويات الدخول والصلاحيات للمسؤولين عن حسابات التواصل الاجتماعي ومراجعتها بشكل دوري، مرة واحدة سنوياعلى الأقل.

	المخرجات المتوقعة: • تقرير لمراجعة هويات الدخول والصلاحيات للمسؤولين عن حسابات التواصل الاجتماعي الخاصة بالجهة.
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، ما يلي:
٢-٣-١-١	تطبيق حزم التحديثات، والإصلاحات الأمنية لتطبيقات التواصل الاجتماعي، مرة واحدة شهرياً على الأقل.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج معيار إدارة التحديثات والإصلاحات • نموذج سياسة إدارة حزم التحديثات والإصلاحات **إرشادات تطبيق الضوابط:** • تحديد التطبيقات التي تستخدمها الجهة لحسابات التواصل الاجتماعي. • مراجعة إرشادات وإجراءات التحديثات والإصلاحات المتعلقة بتطبيقات حسابات التواصل الاجتماعي واتباعها عند تطبيق التحديثات والإصلاحات. • يجب إجراء التحديثات والإصلاحات الأمنية للتطبيقات التي تستخدمها الجهة لحسابات التواصل الاجتماعي، مرة واحدة كل شهر على الأقل.
	المخرجات المتوقعة: • إجراءات موثقة للتحديثات والإصلاحات الأمنية لتطبيقات حسابات التواصل الاجتماعي. • التقارير الدورية للتحديثات والإصلاحات الأمنية التي يتم عملها على تطبيقات حسابات التواصل الاجتماعي.

	٢-١-٣-٢	مراجعة إعدادات الحماية والتحصين لحسابات التواصل الاجتماعي للجهة والأصول التقنية الخاصة بها (Secure Configuration and Hardening)، مرة واحدة كل سنة على الأقل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الإعدادات والتحصين • نموذج معيار الإعدادات والتحصين الآمن • نموذج معيار أمن وسائل التواصل الاجتماعي **إرشادات تطبيق الضوابط:** • تحديد التطبيقات التي تستخدمها الجهة لحسابات التواصل الاجتماعي. • مراجعة إرشادات وإجراءات الحماية والتحصين المتعلقة بتطبيقات حسابات التواصل الاجتماعي واتباعها عند تطبيق الحماية والتحصين على التطبيقات. • يجب إجراء الحماية والتحصين للتطبيقات التي تستخدمها الجهة لحسابات التواصل الاجتماعي، مرة واحدة سنوياً على الأقل.
		المخرجات المتوقعة: • إجراءات موثقة للحماية والتحصين لتطبيقات حسابات التواصل الاجتماعي. • التقارير الدورية للحماية والتحصين التي يتم عملها على تطبيقات حسابات التواصل الاجتماعي.
	٢-١-٣-٣	مراجعة وتحصين الإعدادات المصنعية (Default Configuration) لحسابات التواصل الاجتماعي والأصول التقنية، ومنها وجود كلمات مرور ثابتة أو تسجيل الدخول المسبق، وإقفال الأجهزة (Lockout).
		إرشادات تطبيق الضوابط: • تحديد الأصول التقنية والأنظمة التي تتعامل مع حسابات التواصل الاجتماعي. • توثيق واعتماد سياسات وإجراءات لتحصين الإعدادات المصنعية لجميع الأصول التقنية. • مراجعة الإعدادات الافتراضية التي تشمل، على سبيل المثال لا الحصر: كلمات المرور الافتراضية، تسجيل الدخول المسبق، تأمين الحساب، حسابات الضيوف،

		حسابات الخدمة، الخلفيات، المسؤولين الافتراضيين، البروتوكولات القديمة، المنافذ المفتوحة في النظام. • التأكد من عدم وجود إعدادات الأمان الافتراضية على جميع الأصول التقنية المتعلقة بحسابات التواصل الاجتماعي.
		المخرجات المتوقعة: • سياسات واجراءات موثقة لتحصين الإعدادات المصنعة. • عينة من الإعدادات الخاصة بحسابات التواصل الاجتماعي ومكوناتها التقنية. • تقرير مراجعة الإعدادات لحسابات التواصل الاجتماعي ومكوناتها التقنية.
	٤-١-٣-٢	تقييد تفعيل الخصائص والخدمات في حسابات التواصل الاجتماعي حسب الحاجة على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.
		إرشادات تطبيق الضوابط: • تحديد الأصول التقنية والأنظمة التي تتعامل مع حسابات التواصل الاجتماعي. • توثيق واعتماد سياسات وإجراءات لتحصين الإعدادات المصنعة لجميع الأصول التقنية. • مراجعة الخصائص والخدمات الموجودة في حسابات التواصل الاجتماعي، ولا يتم تنشيط الخصائص والخدمات إلا بعد عمل تقييم للمخاطر.
		المخرجات المتوقعة: • تقرير موثق لمخاطر حسابات التواصل الاجتماعي قبل تفعيل الخصائص والخدمات عليها.
٤-٢	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		

٢-٤-١	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).
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية • نموذج معيار امن الأجهزة المحمولة **إرشادات تطبيق الضوابط:** • تحديد قائمة الأجهزة المحمولة التي يتم استخدامها للتعامل مع حسابات التواصل الاجتماعي الخاصة بالجهة. • تحديد وتطبيق نظام إدارة الأجهزة المحمولة (MDM) ، وفقًا لمتطلبات الجهة، لإدارة الأجهزة المحمولة التي من خلالها يتم الدخول على حسابات التواصل الاجتماعي.
		المخرجات المتوقعة: • قائمة محددة بالأجهزة المحمولة التي يتم استخدامها للتعامل مع حسابات التواصل الاجتماعي الخاصة بالجهة. • عيّنة من إعدادات نظام إدارة الأجهزة المحمولة (MDM).
	٢-٤-١-٢	تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهرياً، على الأقل.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة امن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية **إرشادات تطبيق الضوابط:** • تحديد قائمة الأجهزة المحمولة التي يتم استخدامها للتعامل مع حسابات التواصل الاجتماعي الخاصة بالجهة. • مراجعة إرشادات وإجراءات التحديثات والإصلاحات المتعلقة بالاجهزة المحمولة التي تتعامل مع حسابات التواصل الاجتماعي، واتباعها عند تطبيق الحماية والتحصين على الأجهزة المحمولة.

		• يجب عمل التحديثات والإصلاحات على الأجهزة المحمولة التي تتعامل مع حسابات ال تواصل الاجتماعي، مرة واحدة شهرياً على الأقل.
		المخرجات المتوقعة: • إجراءات موثقة للتحديثات والإصلاحات الأمنية للأجهزة المحمولة التي تتعامل مع حسابات التواصل الاجتماعي. • تقارير المراجعة للتحديثات والإصلاحات الأمنية للأجهزة المحمولة التي تتعامل مع حسابات التواصل الاجتماعي.
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.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني للبيانات • نموذج معيار الأمن السيبراني للبيانات **إرشادات تطبيق الضوابط:** • المراجعة والتأكد من أن الأصول التقنية المتعلقة بحسابات التواصل الاجتماعي لا تحتوي إلا على بيانات مصرح بها وفقاً لسياسات وإجراءات الجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة، ويجب أن لا تحتوي على بيانات مصنفة عالية الحساسية.

		المخرجات المتوقعة: • تقرير لمراجعة تصنيف البيانات في الأصول المستخدمة للتعامل مع حسابات التواصل الاجتماعي الخاص بالجهة.
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:	
	٢-١-٦-١	تفعيل جميع الإشعارات وتنبيهات الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي وسجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية الخاصة بحسابات التواصل الاجتماعي.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني • نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد الأصول التقنية والأنظمة التي تتعامل مع حسابات التواصل الاجتماعي. • تفعيل جميع إشعارات وتنبيهات سجلات الأحداث الخاصة بالأمن السيبراني على الأصول التقنية الخاصة بحسابات التواصل الاجتماعي.
		المخرجات المتوقعة: • عينة من إشعارات وتنبيهات الأمن السيبراني التي تم تنشيطها للأحداث على الأصول المستخدمة للتعامل مع حسابات التواصل الاجتماعي الخاصة بالجهة.
	٢-١-٦-٢	متابعة حسابات التواصل الاجتماعي و مراقبتها للتأكد من عدم نشر أي محتوى غير مصرح، أو تسجيل أي دخول غير مصرح.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق واعتماد إجراءات لمتابعة حسابات التواصل الاجتماعي وآلية مراقبتها للتأكد من عدم نشر أي محتوى غير مصرح به، أو تسجيل أي دخول غير مصرح به. • مراجعة محتوى حسابات التواصل الاجتماعي الخاصة بالجهة من خلال متابعة الحسابات ومراقبة محتواها وأنشطتها. • التحقق من أن المحتوى المنشور عبر حسابات التواصل الاجتماعي مصرح به. • مراجعة إجراءات متابعة حسابات التواصل الاجتماعي بشكل دوري. **المخرجات المتوقعة:** • إجراءات موثقة لمتابعة حسابات التواصل الاجتماعي. • مراجعة المنشورات التي يتم نشرها على حسابات وسائل التواصل الاجتماعي الخاصة بالجهة.
	٢-٦-١-٣	متابعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الجهة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • مراقبة شبكات حسابات التواصل الاجتماعي في الجهة والتأكد من أن حسابات وقنوات وسائل التواصل الاجتماعي في الشبكة مصرح بها، ولا يوجد حساب ينتحل الهوية وينشر نيابة عنهم. في حال حدوث انتحال الهوية للجهة، فينبغي اتخاذ إجراء بشأن الحساب المنتحل وتنفيذ آلية الإبلاغ لحسابات وسائل التواصل الاجتماعي. **المخرجات المتوقعة:** • مراجعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الجهة.

		• عينة من الخدمة المستخدمة لحماية هوية الجهة من الانتحال. • توثيق اجراءات للتعامل في حال انتحال هوية الجهة مع تحديد الاجراء اللازم اتخاذه. • خطة الإبلاغ في حال انتحال حسابات التواصل الاجتماعي للجهة. • تحديد و توثيق بنود المحافظة على السرية NDA للمحافظة على سرية معلومات حسابات التواصل الإجتماعي للجهة.
	٢-٦-١-٤	المراقبة الآلية لأي تغير في نمط الحسابات أو مؤشرات اختراق أو نشر أي محتوى غير مصرح أو انتحال هوية الجهة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني **إرشادات تطبيق الضوابط:** • المراجعة وضمان والمراقبة الآلية لأي تغير في نمط الحسابات أو مؤشرات اختراق أو نشر أي محتوى غير مصرح به أو انتحال هوية الجهة.
		المخرجات المتوقعة: • سجل المراقبة الآلية لحسابات التواصل الاجتماعي الخاصة بالجهة بحثاً عن أي سلوك غير مألوف.
٢-٧	**إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)**	
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة، مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨ هـ.	
الضوابط		
٢-٧-١	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:	
	٢-٧-١-١	وضع خطة استعادة حسابات التواصل الاجتماعي والتعامل مع الحوادث السيبرانية.

		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة إدارة حوادث وتهديدات الأمن السيبراني • نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني • الدليل الإرشادي للاستجابة لحوادث الأمن السيبراني • نماذج الخطط التفصيلية للاستجابة لحوادث الأمن السيبراني **إرشادات تطبيق الضوابط:** • تحديد وتوثيق خطة لاستعادة حسابات التواصل الاجتماعي وتطبيقها في حال فقدان أي حساب بسبب حوادث الأمن السيبراني وغيرها. • ضمان وجود التالي في خطة الاستعادة لحسابات التواصل الاجتماعي: - معلومات التواصل الخاصة بفريق الاستجابة لحوادث الأمن السيبراني. - إخطار فريق الاستجابة للحوادث في الوقت المناسب. - توثيق الحادثة بعد استعادة الحساب.
		المخرجات المتوقعة: • خطة موثقة لاستعادة حسابات التواصل الاجتماعي الخاصة بالجهة.

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

٣-١	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). وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
٣-١-١	يجب تقييم مدى الحاجة لاستخدام خدمات إدارة حسابات التواصل الاجتماعي (Social media management) والمراقبة الآلية لحسابات التواصل الاجتماعي أو لحماية هوية الجهة من الانتحال (brand protection) ومخاطر الأمن السيبراني المتعلقة بها.
	أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • في حال الحاجة إلى استخدام خدمات إدارة حسابات التواصل الاجتماعي والمراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الجهة من الانتحال، يجب إجراء دراسة وتقييم مدى الحاجة إلى ذلك، مع الأخذ بالاعتبار مخاطر الأمن السيبراني المتعلقة بها، وتوثيق النتائج واعتمادها من قبل صاحب الصلاحية.
	المخرجات المتوقعة: • تقرير موثق لتقييم احتياجات الجهة وذلك قبل الاستعانة بخدمات أطراف خارجية لإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال. • تقرير موثق لتقييم المخاطر الذي تم إجراؤه قبل الاستعانة بخدمات أطراف خارجية لإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال. • تقرير موثق لتقييم احتياجات الجهة من خدمات إدارة حسابات التواصل الاجتماعي والمراقبة الآلية لحسابات التواصل الاجتماعي وحماية هوية الجهة من الانتحال.

٣-١-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٤-١-٢ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني الخاصة باستخدام خدمات إدارة حسابات التواصل الاجتماعي (social media management) والمراقبة الآلية لحسابات التواصل الاجتماعي أو لحماية هوية الجهة من الانتحال (brand protection) بحد أدنى مايلي:	
	٣-١-٢-١	بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قبَل الطرف الخارجي لبيانات الجهة عند إنتهاء الخدمة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية التي تقوم بإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال. • التأكد من أن العقود والاتفاقيات مع الأطراف الخارجية تحتوي على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قبَل الطرف الخارجي لبيانات الجهة عند إنتهاء الخدمة. علاوة على ذلك ، يجب الاطلاع على أدلة من مقدم الخدمة توضح الإجراءات المخصصة للإزالة الآمنة للبيانات الخاصة بالجهة.
		المخرجات المتوقعة: • اتفاقية مستوى الخدمة الموثقة مع الأطراف الخارجية التي تقوم بإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال، والتي تتضمن بنوداً تتعلق بعدم الإفصاح وإزالة البيانات بشكل آمن عند إنهاء الخدمة.
	٣-١-٢-٢	إجراءات التواصل للإبلاغ عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية التي تقوم بإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال.

		• التأكد من أن العقود والاتفاقيات مع الأطراف الخارجية تحتوي على إجراءات التواصل والإبلاغ، في وقت مناسب، عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني.
		المخرجات المتوقعة: • عقود واتفاقيات مستوى الخدمة التي تحتوي على إجراءات التواصل والإبلاغ عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني.
	٣-١-٢-٣	إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لحماية حسابات التواصل الاجتماعي للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
		أدوات الأمن السيبراني ذات العلاقة: • نموذج سياسة الأمن السيبراني المتعّلق بالأطراف الخارجية **إرشادات تطبيق الضوابط:** • مراجعة اتفاقية مستوى الخدمة بين الجهة والأطراف الخارجية التي تقوم بإدارة حسابات التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية هوية الجهة من الانتحال. • التأكد من أن العقود والاتفاقيات مع الأطراف الخارجية تحتوي على بنود إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
		المخرجات المتوقعة: • عقود واتفاقيات مستوى الخدمة التي تحتوي على إجراءات إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority