هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملوّن بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار أمن وسائل التواصل الاجتماعي

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <1.0>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	تفاصيل الإصدار
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف الإصدار>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

اختر التصنيف

الإصدار <1.0>

الغرض

الغرض من هذا المعيار هو تحديد كيف تضمن <اسم الجهة> أمن وسائل التواصل الاجتماعي من حيث إعداد المحتوى وإدارته ونشره وكذلك مراقبته على حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> على منصات التواصل الاجتماعي. إن قدرة <اسم الجهة> على استخدام وسائل التواصل الاجتماعي وفقًا لهذا المعيار سيساعد في الحفاظ على سرية وسلامة وتوافر بيانات <اسم الجهة> ومعلوماتها.

تمت مواءمة متطلبات هذا المعيار مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC-1: 2021) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة بـ <اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	إدارة الأصول (Asset Management)
الهدف	التأكد من أن <اسم الجهة> تحتفظ بقائمة جرد دقيقة ومفصّلة للأصول المعلوماتية والتقنية ذات العلاقة بوسائل التواصل الاجتماعي، من أجل دعم العمليات التشغيلية ومتطلبات الأمن السيبراني في <اسم الجهة> للحفاظ على سرية وسلامة وتوافر الأصول المعلوماتية والتقنية.
المخاطر المحتملة	إذا لم تتم إدارة قائمة جرد الأصول المعلوماتية والتقنية المتعلقة بوسائل التواصل الاجتماعي بشكل صحيح لدى <اسم الجهة>، فقد يؤدي ذلك إلى عدم التحكم في استخدام وسائل التواصل الاجتماعي والتعرض لانتهاكات السرية وتسريبات البيانات .
الإجراءات المطلوبة	
1-1	تحديد حسابات وسائل التواصل الاجتماعي والأصول المعلوماتية والتقنية المرتبطة بها لدى <اسم الجهة> وإعداد قائمة جرد خاصة بتلك الحسابات والأصول. ويجب تحديث قائمة الجرد سنويًا على الأقل.
2-1	بمجرد إنشاء حساب جديد على وسائل التواصل الاجتماعي خاص ب<اسم الجهة>، يجب إضافته إلى قائمة الجرد.

3-1	إذا تم حذف حساب <اسم الجهة> على وسائل التواصل الاجتماعي، فيجب التأشير على الحساب في قائمة الجرد بما يفيد ذلك.
2	إدارة هويات الدخول والصلاحيات (Identity and Access Management)
الهدف	ضمان حماية الوصول الآمن والمقيد إلى الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> من أجل منع الوصول غير المصرح به والسماح للمستخدمين بالوصول المصرح به فقط لإنجاز المهام المكلفين بها المتعلقة بوسائل التواصل الاجتماعي.
المخاطر المحتملة	إذا لم تتم إدارة الوصول إلى الأصول المعلوماتية والتقنية المتعلقة بوسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> بشكل صحيح، فقد يترتب على ذلك الكشف عن بيانات الاعتماد والوصول غير المصرح به وإلحاق أضرار جسيمة بالسمعة.
الإجراءات المطلوبة	
1-2	عند إنشاء الحساب، لا يجب استخدام سوى حسابات وسائل التواصل الاجتماعي المخصصة للجهات وليس الأفراد. إن أمكن، يجب التحقق من حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> وتأشيرها وفقًا لذلك من قبل مقدمي منصات التواصل الاجتماعي.
2-2	يجب عدم التسجيل على منصات التواصل الاجتماعي إلا باستخدام المعلومات الرسمية (البريد الإلكتروني الرسمي الخاص بوسائل التواصل الاجتماعي ورقم الجوال الرسمي)، وليس المعلومات الشخصية.
3-2	بالنسبة لعناوين البريد الإلكتروني المنشورة للعامة لأغراض التواصل على حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة>، يجب أن تكون هذه العناوين عامة وغير محددة ولا تشبه عناوين البريد الإلكتروني المؤسسية الخاصة بموظفي <اسم الجهة>.
4-2	استخدام عنوان بريد إلكتروني مختلف لكل حساب رسمي خاص ب<اسم الجهة> على وسائل التواصل الاجتماعي.
5-2	التحقق من حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> كلما أمكن ذلك، مع الحفاظ على هويات دخول وصلاحيات متسقة عبر جميع حسابات وسائل التواصل الاجتماعي التي تستخدمها <اسم الجهة>، وذلك لتسهيل معرفة الحسابات الرسمية واكتشاف عمليات الاحتيال أو الحسابات غير الرسمية.
6-2	استخدام كلمة مرور آمنة ومحددة وفريدة لكل حساب من حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة>. ويجب تغيير كلمة المرور بانتظام وعدم تكرار استخدام كلمات المرور.
7-2	يجب عدم نسخ كلمات المرور أو مشاركتها تحت أي ظرف من الظروف خارج <اسم الجهة> أو داخلها.

8-2	استخدام التحقق من الهوية متعدد العناصر لتسجيل الدخول إلى حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة>.
9-2	تطبيق تسجيل الدخول الموحد (SSO) لجميع حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة>.
10-2	تفعيل الأسئلة الأمنية وتحديثها وتوثيقها بانتظام في مكان آمن.
11-2	إدارة حقوق الوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى حقوق الوصول ونوع الأجهزة والأنظمة المستخدمة.
12-2	إتاحة الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> للموظفين المصرح لهم فقط، عند الطلب والتحقق.
13-2	منح حق الوصول إلى كل حساب رسمي خاص ب<اسم الجهة> على وسائل التواصل الاجتماعي لشخصين (2) مخولين على الأقل.
14-2	تحديد الأدوار ذات الصلة للأشخاص الذين يمكنهم الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> وتحديد حقوقهم وتصاريحهم الإدارية فيما يتعلق بتشغيل الحساب.
15-2	التقيد بمنح الحد الأدنى من حقوق الوصول لمقدمي خدمات إدارة منصات التواصل الاجتماعي أو مراقبة وسائل التواصل الاجتماعي أو حماية العلامة التجارية.
16-2	أن يقتصر الوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> على أجهزة محددة.
17-2	مراجعة هويات المستخدمين وحقوق الوصول المستخدمة لحسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> مرة واحدة سنويًا على الأقل.
18-2	إبلاغ العاملين بأن الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> يكون عند الضرورة فقط، ويجب على العاملين تسجيل الخروج بمجرد الانتهاء من استخدامهم للحساب الرسمي الخاص ب <اسم الجهة> على وسائل مواقع التواصل الاجتماعي.
3	حماية أنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)
الهدف	ضمان حماية أنظمة المعلومات وأجهزة معالجة المعلومات (بما في ذلك أجهزة المستخدمين والبنى التحتية) من المخاطر السيبرانية المتعلقة بوسائل التواصل الاجتماعي.

المخاطر المحتملة	إذا لم تتم حماية أنظمة المعلومات وأجهزة معالجة المعلومات لدى <اسم الجهة> بشكل صحيح من المخاطر السيبرانية المتعلقة بوسائل التواصل الاجتماعي، فقد يترتب على ذلك التعرض للهجمات السيبرانية وتسرب البيانات وفقدانها.
الإجراءات المطلوبة	
1-3	تنزيل تطبيقات وسائل التواصل الاجتماعي وتثبيتها من مصادر معروفة وموثوقة فقط.
2-3	تثبيت التحديثات والإصلاحات الأمنية لتطبيقات وسائل التواصل الاجتماعي المستخدمة لدى <اسم الجهة> مرة واحدة شهريًا على الأقل (إن وجدت).
3-3	إجراء مراجعات وتحصين إعدادات حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> والأصول التقنية المتعلقة بها مرة واحدة سنويًا على الأقل.
4-3	إجراء مراجعات وتحصين الإعدادات الافتراضية -مثل كلمات المرور الافتراضية وتسجيل الدخول المسبق والإقفال- لحسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> والأصول التقنية المتعلقة به مرة واحدة سنويًا على الأقل.
5-3	التأكد من تقييد تفعيل الميزات والخدمات في حسابات وسائل التواصل الاجتماعي لتكون حسب الحاجة فقط، وضمان إجراء تقييم للمخاطر في حال الحاجة إلى تفعيلها.
4	أمن الأجهزة المحمولة (Mobile Device Security)
الهدف	ضمان حماية الأجهزة المحمولة (بما في ذلك أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية) من المخاطر السيبرانية، وضمان التعامل الآمن مع معلومات <اسم الجهة> (بما في ذلك معلوماتها الحساسة) عند استخدام الأجهزة الشخصية في مكان العمل (سياسة استخدام الأجهزة الشخصية في مكان العمل) (BYOD).
المخاطر المحتملة	إذا لم تتم حماية الأجهزة المحمولة بشكل صحيح من المخاطر السيبرانية وإدارتها بشكل ملائم، فقد يؤدي ذلك إلى انتهاك السرية والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-4	إدارة الأجهزة المحمولة المستخدمة في الوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> مركزيًا باستخدام نظام إدارة الأجهزة المحمولة.(MDM)
2-4	تثبيت التحديثات والإصلاحات الأمنية على الأجهزة المحمولة المستخدمة في الوصول إلى حسابات التواصل الاجتماعي الخاصة ب<اسم الجهة> مرة واحدة شهريًا على الأقل (إن وجدت).

3-4	حماية الأجهزة المحمولة المستخدمة في الوصول إلى حسابات التواصل الاجتماعي الخاصة ب<اسم الجهة> بشكل كافٍ باستخدام كلمة المرور أو المقاييس الحيوية.
4-4	ألا يتم الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> إلا من خلال جهاز يمتثل لسياسات <اسم الجهة> ذات الصلة.
5-4	أن يكون الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> من شبكة موثوقة فقط.
6-4	ألا يتم الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> إلا باستخدام جلسات آمنة كبروتوكول نقل النص الفائق الآمن HTTPS
7-4	في حال فقدان أو تلف أي جهاز محمول يُستخدم للوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة>، يجب الإبلاغ عن ذلك في حينه من أجل تنفيذ التدابير التصحيحية ذات الصلة.
5	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية بيانات ومعلومات <اسم الجهة> وسريتها وسلامتها وتوافرها، وفقًا للسياسات والإجراءات التنظيمية المؤسسية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
المخاطر المحتملة	إذا لم تتم حماية بيانات ومعلومات <اسم الجهة> بشكل صحيح و تم ضبط إعدادات الخصوصية بشكل خاطئ، فقد يؤدي ذلك إلى انتهاك السرية والإضرار بالسمعة والتعرض لتداعيات قانونية.
الإجراءات المطلوبة	
1-5	يجب ألا تحتوي الأصول التقنية لإدارة حسابات وسائل التواصل الاجتماعي الخاصة ب<اسم الجهة> على بيانات سرية، وفقًا للوائح التنظيمية ذات العلاقة.
2-5	قبل إنشاء واستخدام حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة>، يجب قراءة سياسات وقواعد الخصوصية ذات الصلة لمقدمي منصات وسائل التواصل الاجتماعي وفهمها وقبولها. فإذا لم تكن سياسات وقواعد الخصوصية هذه مقبولة من جانب <اسم الجهة>، فيجب تقييم المخاطر ذات الصلة ومن ثم يجب إما قبولها أو عدم إنشاء حسابات رسمية ل<اسم الجهة> على منصات التواصل الاجتماعي ذات الصلة.
3-5	يجب قراءة سياسات وقواعد الخصوصية الخاصة بمقدمي منصات وسائل التواصل الاجتماعي وفهمها وقبولها عند إجراء أي تغييرات أثناء استخدام حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة>. وإذا لم تعد سياسات وقواعد الخصوصية

	هذه مقبولة لدى <اسم الجهة> بعد التغييرات المستحدثة، فيجب تقييم المخاطر ذات الصلة ومن ثم يجب قبولها أو حذف حسابات وسائل التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة> ذات الصلة.
4-5	مراجعة إعدادات الخصوصية الافتراضية لحسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> وتعديلها لتحقيق التوازن بين الغرض من الحساب ومتطلبات الخصوصية الداخلية المطبقة لدى <اسم الجهة>.
5-5	يجب إلغاء تفعيل خاصية تحديد الموقع الجغرافي لحسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> وعدم إضافتها إلى المحتوى المنشور.
6-5	يجب عدم الإفصاح عن المعلومات الحساسة، ولا سيما: • المعلومات السرية ل<اسم الجهة> • والبيانات الشخصية دون الحصول على موافقة على وسائل التواصل الاجتماعي تحت أي ظرف من الظروف. ولا يجوز نشر هذه المعلومات، إذا لزم الأمر، إلا بعد الحصول على موافقة كتابية، ومن قبل الموظفين المصرح لهم من <اسم الجهة>.
7-5	لا تُنشر سوى المعلومات أو البيانات الإعلامية التي تم التحقق منها ومراجعتها باستخدام حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة>.
8-5	أن تكون جميع الصور والملفات المنشورة باستخدام حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> إما مملوكة من قِبل <اسم الجهة> أو تكون غير محمية بحقوق نشر.
9-5	أن يكون أي محتوى يتم إعادة نشره أو إعادة توجيهه عبر حسابات وسائل التواصل الاجتماعي الرسمية الخاصة ب<اسم الجهة> من مصادر معروفة وموثوقة.
6	إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Events (Logs and Monitoring Management
الهدف	ضمان جمع وتحليل ومراقبة أحداث الأمن السيبراني في حينه لتمكين اكتشاف الهجمات السيبرانية في وقت مبكر بهدف منع أو تقليل الآثار السلبية الناجمة عنها على عمليات <اسم الجهة>.
المخاطر المحتملة	إذا لم تتم إدارة جمع السجلات ومراقبة الأحداث المتعلقة بوسائل التواصل الاجتماعي بشكل صحيح، فقد يؤدي ذلك إلى التعرض للهجمات السيبرانية والإضرار بسمعة الجهة.

الإجراءات المطلوبة	
1-6	تفعيل جميع الإشعارات وتنبيهات الأمن السيبراني الخاصة بحسابات وسائل التواصل الاجتماعي الخاصة بـ<اسم الجهة> وسجلات أحداث الأمن السيبراني على الأصول التقنية ذات الصلة.
2-6	متابعة ومراقبة حسابات وسائل التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة> لضمان عدم نشرها لأي محتوى غير مصرح به أو تسجيل الدخول غير المصرح به إليها. ويجب مراقبة كل حساب رسمي لـ <اسم الجهة> على وسائل التواصل الاجتماعي، حتى وإن كان غير مستخدم حاليًا.
3-6	مراقبة شبكات التواصل الاجتماعي لضمان عدم انتحال صفة <اسم الجهة>.
4-6	مراقبة استخدام الحساب الرسمي لـ <اسم الجهة> على وسائل التواصل الاجتماعي للتحقق من الحقوق والصلاحيات الممنوحة لمختلف التطبيقات.
5-6	مراقبة ومراجعة المحتوى المنشور على حسابات وسائل التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة> بانتظام للتحقق مما إذا كان يمتثل للمتطلبات الداخلية.
6-6	مراقبة وجهة المراسلات الصادرة من حسابات وسائل التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة> بانتظام.
7-6	إجراء مسح لوسائل التواصل الاجتماعي بانتظام للتحقق من عدم احتوائها على أي أسرار أو معلومات سرية واستخدام غير مُصرح به للعلامة التجارية الخاصة بـ <اسم الجهة>.
8-6	إجراء المراقبة الآلية لأي تغيير في نمط سلوك الحسابات أو مؤشرات التعرض للاختراق أو نشر أي محتوى غير مصرح به أو انتحال صفة <اسم الجهة>.
9-6	ضبط إعدادات مراقبة وسائل التواصل الاجتماعي بطريقة تتيح التكامل مع خدمات مراقبة وحماية العلامة التجارية الخاصة بـ <اسم الجهة> (إذا كانت مقدمة داخل <اسم الجهة>).
7	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد واكتشاف حوادث وتهديدات الأمن السيبراني المتعلقة بوسائل التواصل الاجتماعي في حينه وإدارتها والتعامل معها بفعالية لمنع أو تقليل الآثار السلبية الناجمة عنها على عمليات <اسم الجهة>.
المخاطر المحتملة	إذا لم تتم إدارة قائمة الجرد للأصول المعلوماتية والتقنية المتعلقة بوسائل التواصل الاجتماعي الخاصة بـ <اسم الجهة> بشكل صحيح، فيمكن أن يؤدي ذلك إلى آثار سلبية.

الإجراءات المطلوبة	
1-7	وضع خطة لاستعادة حسابات وسائل التواصل الاجتماعي الخاصة بـ <اسم الجهة> والتعامل مع الحوادث السيبرانية.
2-7	التعامل مع أي حادث يتعلق بحسابات التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة>، ولا سيما: ● الاحتيال على وسائل التواصل الاجتماعي ● انتحال صفة العلامة التجارية ● تسرب المعلومات السرية ● سرقة بيانات الاعتماد وفقًا لخطط وإجراءات الاستجابة للحوادث المطبقة في <اسم الجهة>.
3-7	أن يكون العاملون الذين يتمتعون بحق الوصول إلى حسابات وسائل التواصل الاجتماعي الرسمية الخاصة بـ <اسم الجهة> على دراية بكيفية الإبلاغ عن الأحداث والحوادث المشبوهة أو غير العادية المتعلقة بالتواجد على وسائل التواصل الاجتماعي، بحيث يتم التعامل معهم بشكل وافٍ.
8	الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)
الهدف	ضمان حماية أصول الجهة من المخاطر السيبرانية المتعلقة بالأطراف الخارجية، بما في ذلك خدمات الإسناد والخدمات المدارة وفقًا للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
المخاطر المحتملة	إذا لم تتم حماية أصول <اسم الجهة> بشكل وافٍ من المخاطر المتعلقة بالأطراف الخارجية على وسائل التواصل الاجتماعي، فقد يؤدي ذلك إلى الوصول غير المصرح به إليها وفقدان أو تسرب البيانات والإضرار بالسمعة ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-8	إجراء تقييم للاحتياجات لأغراض استخدام وسائل التواصل الاجتماعي أو المراقبة الآلية أو خدمات حماية العلامة التجارية إلى جانب مخاطر الأمن السيبراني ذات الصلة.
2-8	ضمان تطبيق بنود عدم الإفصاح عن المعلومات والإزالة الآمنة لبيانات <اسم الجهة> من قبل الطرف الخارجي بمجرد إنهاء الخدمة.

3-8	إنشاء وتنفيذ إجراءات الاتصالات للإبلاغ عن الثغرات والحوادث السيبرانية المتعلقة بوسائل التواصل الاجتماعي.
4-8	تطبيق المتطلبات المتعلقة بالتزام الأطراف الخارجية لمتطلبات وسياسات الأمن السيبراني لحماية حسابات وسائل التواصل الاجتماعي الخاصة بـ <اسم الجهة> والأنظمة واللوائح ذات الصلة.

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.
2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.
3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.
4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو عند حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.
2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.
3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.