قرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات
رقم (37) لسنة 2024 ميلادي بشأن
إعتماد ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي

مدير عام الهيئة الوطنية لأمن وسلامة المعلومات:

- بعد الإطلاع على الإعلان الدستوري الصادر في أغسطس 2011ميلادي وتعديلاته.
- وعلى الاتفاق السياسي الليبي الموقع بتاريخ 17 ديسمبر 2015 ميلادي.
- وعلى مخرجات ملتقى الحوار الليبي المنعقد بتاريخ 9 نوفمبر 2020 ميلادي.
- وعلى ما قرره مجلس النواب بتاريخ 10 مارس 2021 بمنح الثقة لحكومة الوحدة الوطنية.
- وعلى القانون رقم (12) لسنة 2010 ميلادي بإصدار قانون علاقات العمل ولائحته التنفيذية.
- وعلى القانون رقم (5) لسنة 2022 ميلادي بشأن مكافحة الجرائم الإلكترونية.
- وعلى القانون رقم (6) لسنة 2022 ميلادي بشأن المعاملات الإلكترونية.
- وعلى قرار مجلس الوزراء رقم (28) لسنة 2013 ميلادي بشأن إنشاء الهيئة الوطنية لأمن وسلامة المعلومات.
- وعلى قرار رئيس الهيئة العامة للاتصالات والمعلوماتية رقم(55) لسنة 2018ميلادي بشأن تكليف بمهام.
- وعلى كتاب السيد/ مدير مكتب المدير العام رقم (2/748) بتاريخ 2024/10/14 ميلادي.

قـــــــــــرر

المادة الأولى

يتم بموجب أحكام هذا القرار اعتماد ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي بالدولة الليبية.

المادة الثانية

على كافة الوزارات والقطاعات والجهات التابعة لها الإلتزام بالضوابط الخاصة بإنشاء وإدارة الحسابات على منصات التواصل الاجتماعي المعتمدة بموجب أحكام هذا القرار لضمان أمن وسلامة معلوماتها وأصولها ضد التهديدات السيبرانية.

المادة الثالثة

يعمل بهذا القرار إعتبارا من تاريخ صدوره، وعلى كافة الجهات المعنية تنفيذه.

م. صلاح الدين ابوزيد التبيني
مدير عام الهيئة الوطنية لأمن وسلامة المعلومات

صدر في طرابلس بتاريخ 20 / ١٥ /2024 ميلادي

رئيس مجلس الشؤون القانونية ... محمد

ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي

المرفقة بقرار مدير عام الهيئة الوطنية لأمن وسلامة المعلومات رقم (37) لسنة 2024 ميلادي

ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي

الإصدار الأول

Ver. 1.0

© NISSA Oct. 2024

جدول المحتويات

المقدمة: 3
الغرض: 3
النطاق: 3
تحديد المسؤوليات: 3
المخاطر الأمنية: 4
إدارة حسابات الجهة على منصات التواصل الاجتماعي: 4
إدارة المحتوى المنشور: 5
الخصوصية وحماية البيانات: 6
التوعية والتدريب: 6
المراقبة والتقييم: 6
خطة الاستجابة السريعة: 7
الخطوات الرئيسية لكتابة خطة الاستجابة السريعة للتعامل مع الحوادث السيبرانية: 7
القوانين والآداب العامة: 9
مراعاة حقوق النشر والملكية الفكرية: 9

مقدمة:

تُعد منصات التواصل الاجتماعي أدوات فعّالة للتواصل بين الجهات الحكومية والجمهور من خلال إنشاء قنوات تواصل تسهل التفاعل المباشر مع الجمهور، مما يعزز الشفافية ويحسّن الأداء الحكومي، ومع ازدياد استخدام منصات التواصل الاجتماعي بشكل رسمي من قبل الجهات الحكومية داخل الدولة الليبية تطلب ذلك وضع ضوابط (دليل إرشادي) لضمان استخدامها بشكل آمن، وإدارة المحتوى الذي يتم نشره بما يتماشى مع القيم والأخلاقيات العامة للمجتمع، وبما لا يخالف القوانين واللوائح وأهداف المؤسسة، ولتعزيز الثقة بين الجهات الحكومية والمواطنين.

أصدرت الهيئة الوطنية لأمن وسلامة المعلومات النسخة الأولى من ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي، ويأتي ذلك ضمن اختصاصات ومهام الهيئة الواردة بقرار إنشائها.

الغرض:

تهدف هذه الضوابط إلى وضع إطار يضمن الاستخدام الآمن والمسؤول لحسابات الجهات الحكومية في الدولة الليبية على منصات التواصل الاجتماعي، وذلك لحماية البيانات والمعلومات، وتقليل التهديدات السيبرانية المصاحبة لاستخدام التقنية، ولتمكين الجهات الحكومية من استخدام حساباتها بطريقة آمنة للحد من مخاطر جرائم اختراق حسابات التواصل الاجتماعي الخاصة بالمؤسسات أو انتحال شخصياتها أو سوء استغلالها.

النطاق:

تُطبق هذه الضوابط على جميع الجهات الحكومية في الدولة الليبية من وزارات وهيئات ومؤسسات وغيرها، والتي تمتلك حسابات رسمية على منصات التواصل الاجتماعي، وعلى جميع الحسابات الأخرى المستخدمة للتواصل لأغراض رسمية.

كما تشجع الهيئة الجهات الأخرى في الدولة الليبية للاستفادة من هذه الضوابط في إدارة حساباتها على منصات التواصل الاجتماعي.

تحديد المسؤوليات:

تضع العديد من الجهات الحكومية أهمية بالغة لاستخدام منصات التواصل الاجتماعي في نشر محتواها وإيصال المعلومات وتقديم الخدمات، والوصول لأكبر عدد ممكن من الجمهور المستهدف. نظرًا لحساسية المعلومات، تم تحديد مسؤوليات إدارة الحسابات بحيث تشمل تعيين موظف من الجهة المسؤولة عن الأمن السيبراني في الجهة كمدير رئيسي لحسابات الجهة على منصات التواصل الاجتماعي، وتكون مسؤولياته:

- إنشاء أو تعطيل أو حذف الحسابات الرسمية للجهة على منصات التواصل الاجتماعي بناءً على تعليمات رسمية وموثقة من إدارة الجهة.
- تأمين حسابات الجهة باستخدام كلمات مرور قوية وتفعيل المصادقة الثنائية.
- وضع آلية لإدارة ومتابعة سجلات الأنشطة.
- وضع خطة الاستجابة السريعة في حالة التعرض لحادث سيبراني.

- التواصل مع الوحدة الإدارية المسؤولة عن الأمن السيبراني في الجهة لمعالجة الحوادث بشكل فعال.
- توثيق الحوادث الإلكترونية والتهديدات التي تتعرض لها حسابات التواصل الاجتماعي الخاصة بالجهة.
- حماية الجمهور والمتلقين من الإعلانات الزائفة والتصيد الإلكتروني.

المخاطر الأمنية:

تتعرض حسابات الجهات الحكومية على منصات التواصل الاجتماعي للمخاطر السيبرانية باستمرار حيث يستخدم المخترقون تقنيات وأساليب متعددة وجديدة، ولتقليل تلك المخاطر والوقاية منها، أصبح من الضرورة إعداد ضوابط وإرشادات محلية للاستخدام الآمن لمنصات التواصل الاجتماعي والتزام هذه الجهات بها، والتي تمثّل أفضل الممارسات المعنيّة بالحماية عند استخدام منصّات التواصل الاجتماعي.

والجدير بالذكر، أنّ أغلب المخاطر الأمنية تكمن في التعرض للبرمجيات الخبيثة أو الفيروسات، والتصيد الإلكتروني واختراق كلمة المرور وتسريب المعلومات وغيرها، كما أنّ عدم وعي الموظفين بالمخاطر الأمنية يُعد سبباً رئيسياً لاختراق الحسابات مما يؤدي إلى الإضرار بالجهة الحكومية المستهدفة.

إدارة حسابات الجهة على منصات التواصل الاجتماعي:

- استعمال أجهزة مخصصة توفرها الجهة الحكومية لإدارة واستخدام الحسابات على منصات التواصل الاجتماعي من خلالها، وعدم استخدام الأجهزة المخصصة في إدارة الحسابات الشخصية للموظفين، كما يحظر على الموظفين فتح الحسابات الرسمية للجهة في أجهزتهم الشخصية.
- تسجيل وتوثيق جميع حسابات الجهة على منصات التواصل الاجتماعي متضمناً تفاصيل الحساب وبيانات الموظفين المخولين باستعماله واتباع نسق واحد للحفاظ على هوية موحدة للجهة في جميع حسابات الجهة على منصات التواصل الاجتماعي لتسهل على الجمهور التميز بين الصفحات الرسمية والمزورة.
- يجب أن يتم التسجيل في حسابات منصات التواصل الاجتماعي باستخدام بريد إلكتروني رسمي ومعتمد من الجهة مخصص لإدارة حسابات التواصل الاجتماعي، وعدم استخدام معلومات شخصية لمديري هذه الحسابات.
- يجب استخدام كلمات مرور آمنة وتغييرها بشكل دوري كل 90 يومًا على الأكثر، مع الالتزام بعدم مشاركة كلمة المرور أو إعادة استخدامها لأي حساب آخر، وعدم استخدام كلمات مرور سبق استخدامها سابقا، كما يجب أن تتوافق مع متطلبات سياسة كلمات المرور الواردة في دليل السياسات الوطنية لأمن وسلامة المعلومات.
- استخدام شبكات موثوقة للاتصال بالإنترنت من مزود خدمة موثوق.
- الاحتفاظ بسجلات النشاط، ومراجعة عمليات الدخول والخروج من الحسابات بشكل دوري (التاريخ، الوقت، وهوية المستخدم، مكان الدخول).

- توثيق جميع الصلاحيات الممنوحة للموظفين المكلفين بإدارة حسابات الجهة على منصات التواصل الاجتماعي، وضمان تحديثها بانتظام، وضمان عدم منح صلاحيات دخول لأشخاص غادروا فريق العمل.
- يجب التواصل مع الوحدة الإدارية المختصة بالأمن السيبراني داخل الجهة في حالة حدوث أي تهديد سيبراني.
- التحكم في الصلاحيات: تقييد الوصول إلى الحسابات بناءً على مبدأ "الحاجة إلى المعرفة"، وضمان أن الصلاحيات تمنح فقط للموظفين المخولين بالمهام المحددة.

إدارة المحتوى المنشور:

يساعد نشر محتوى ثري وقيّم في بناء علاقة ثقة بين الجهات الحكومية والمواطنين، وتعزيز التواصل الفعّال، ورفع مستوى الوعي والمعرفة بالخدمات المقدمة مما يسهم في تحسين جودتها، مع مراعاة القواعد الواجب أخذها بعين الاعتبار عند إعداد ونشر المحتوى ولإدارة محتوى صفحات الجهة على منصات التواصل الاجتماعي بالشكل الأمثل يتم تشكيل فريق عمل "فريق إدارة المحتوى والتواصل" يلتزم بالتالي:

- توافق المحتوى مع الأهداف العامة للجهة، وإعداد محتوى قيّم للجمهور المستهدف يسهل الوصول إليه ويناسب جميع الفئات العمرية ويصاغ وينشر وفق معايير مهنية وتقنية.
- يجب أن يتميز المحتوى بالوضوح والشفافية وأن يكون خاليا من أي محتويات تعتبر مسيئة أو تُعد انتهاكاً للقوانين واللوائح والأعراف السائدة.
- اتباع آلية مراجعة واعتماد المحتوى قبل النشر من قبل فريق إدارة المحتوى والتواصل على منصات التواصل الاجتماعي، وذلك لضمان عدم نشر محتوى غير ملائم أو مسيء للجهة أو المجتمع والتأكد من سلامة المعلومات الواردة فيه.
- يجب أن تخضع جميع المواد المنشورة للمراجعة والتحرير من قبل المسؤولين المختصين قبل نشرها لضمان سلامتها لغوياً والتأكد من صحة المعلومات الواردة فيها.
- يجب على فريق إدارة المحتوى للحسابات الرسمية للجهة على منصات التواصل الاجتماعي نشر محتوى يحقق الأهداف والخطط المرسومة للجهة بعيدا عن الآراء والتوجهات الشخصية.
- تجنب المواضيع الحساسة التي قد تؤثر على سمعة الجهة، كما يحظر نشر أي معلومات سرية أو حساسة والالتزام بسياسة تصنيف البيانات الصادرة عن الهيئة العامة للمعلومات.
- يجب أن يكون التفاعل مع الجمهور مهنيًا ومحترمًا، ويُنصح بتجنب التفاعل مع التعليقات السلبية بطرق غير مهنية، وإزالة وحذف التعليقات المسيئة أو التي تحث على الكراهية أو المخالفة للقانون وإبلاغ الجهات المعنية عن مرتكبيها.

الخصوصية وحماية البيانات:

على الرغم من عدم قدرة أي مستخدم لمنصات التواصل الاجتماعي من حماية حسابه بشكل كامل من أي تهديد سيبراني محتمل، إلا أنه يمكنه مكافحة التهديدات السيبرانية بفاعلية من خلال اتباع أفضل الممارسات وتطبيق الإجراءات الوقائية الاستباقية للحد من المخاطر المصاحبة لاستخدام تكنولوجيا المعلومات والاتصالات.

الامتثال للسياسات :يجب على مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي الامتثال للسياسات الوطنية لأمن وسلامة المعلومات الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات.

حماية المعلومات :يجب عدم نشر أي معلومات سرية أو حساسة أو خاصة تتعلق بالجهة أو موظفيها أو عملائها على منصات التواصل الاجتماعي، والالتزام بسياسة تصنيف البيانات الصادرة عن الهيئة العامة للمعلومات.

التوعية والتدريب:

إنّ عملية تدريب وتوعية موظفي الجهات الحكومية على استخدام منصات التواصل الاجتماعي ضرورية لتمكين هذه الجهات من تجنب ومواجهة المخاطر السيبرانية التي قد تتعرض لها، ومن الضروري أيضاً أن يكون مشرفو الحسابات الرسمية للجهة على منصات التواصل الاجتماعي ملمين بكيفية إدارة الحسابات، ومعرفة الواجبات القانونية، وعلى دراية بالقوانين والتشريعات والأعراف السائدة.

- **تدريب الموظفين:** يجب تدريب مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي باستمرار حول تأمين الحسابات على هذه المنصات، بما في ذلك التدريب على استخدام أدوات المصادقة الثنائية وإدارة كلمات المرور والمهارات ذات الصلة.
- **التوعية بالمخاطر:** يجب تعزيز وعي مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي حول التهديدات السيبرانية المتعلقة بحسابات منصات التواصل الاجتماعي، والتعرف على أدوات الحماية المتقدمة مثل مراقبة الأنشطة غير الطبيعية، وتحليل السلوكيات المشبوهة، بالإضافة إلى استخدام برامج مكافحة التصيّد الإلكتروني والبرمجيات الخبيثة.

المراقبة والتقييم:

- **مراقبة الحسابات:** يجب مراقبة جميع الأنشطة المتعلقة بحسابات منصات التواصل الاجتماعي للتأكد من المعلومات المنشورة، والتعامل مع محاولات الاختراق باتباع أفضل الممارسات، وضمان الامتثال للسياسات الوطنية لأمن وسلامة المعلومات.
- **التدقيق على المستخدمين:** يجب التحقق بشكل دوري من سجل النشاطات (Activity Logs) لضمان عدم وجود عمليات دخول ناجحة لأشخاص غير مصرح لهم (اختراق) أو وجود صلاحيات دخول لأشخاص غادروا فريق العمل.
- فحص الأجهزة المستخدمة في إدارة الحسابات من قبل الوحدة المسؤولة عن الأمن السيبراني.

- **التقييم والتدقيق:** يجب إجراء تدقيق دوري لحسابات الجهة الرسمية على منصات التواصل الاجتماعي للتأكد من التزام الجميع بالسياسات المعمول بها، واتخاذ إجراءات تصحيحية عند الحاجة.

خطة الاستجابة السريعة:

على مشرفي صفحات منصات التواصل الاجتماعي للجهة وضع آلية تواصل مشتركة مع الوحدة الإدارية المسؤولة عن الأمن السيبراني داخل الجهة لتسهيل التنسيق.

- **إجراءات التصحيح السريعة:** تحديد إجراءات فورية لاستعادة السيطرة على الحساب، تشمل تعطيل الحساب، إعادة تعيين كلمات المرور، وتحديث إعدادات الأمان.
- **تدريب مشرفي الحسابات على تنفيذ الخطة:** يجب تدريب مشرفي الحسابات بشكل دوري على كيفية تنفيذ خطة الاستجابة السريعة لضمان جاهزيتهم للتعامل مع الهجمات فور وقوعها.

الخطوات الرئيسية لكتابة خطة الاستجابة السريعة للتعامل مع الحوادث السيبرانية:

تُعد حسابات الجهات الحكومية على منصات التواصل الاجتماعي هدفًا محتملاً للهجمات السيبرانية، ونظراً لأهمية تلك الحسابات في نشر المعلومات والتواصل مع الجمهور؛ وللتعامل مع هذه الهجمات بفعالية، عند إعداد خطة الطوارئ يجب اتباع الخطوات التالية بشكل مفصل:

1. التعرف على نوع الهجوم السيبراني:

- يجب على مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي التعرف على أنواع الهجمات السيبرانية الشائعة التي تستهدف حسابات التواصل الاجتماعي، مثل:
- التصيد الإلكتروني(Phishing) : محاولات خداع الموظفين للحصول على بيانات تسجيل الدخول.
- الهجمات عبر البرمجيات الخبيثة (Malware) استخدام روابط أو مرفقات تحتوي على برمجيات خبيثة تؤدي إلى اختراق الحسابات.
- الهجمات بالقوة الغاشمة :(Brute Force) محاولات تخمين كلمة المرور بشكل متكرر حتى الوصول إلى الحساب.
- الهجمات عن طريق الهندسة الاجتماعية :(Social Engineering) إقناع الموظفين بالكشف عن بيانات سرية أو كلمات المرور.

2. الخطوات الفورية عند اكتشاف الهجوم:

عند اكتشاف اختراق أو محاولة اختراق حسابات الجهة على منصات التواصل الاجتماعي يجب اتخاذ الإجراءات التالية على الفور:

- **عزل الحسابات:** يجب على الفور تغيير كلمة المرور المرتبطة بالحساب المتضرر، ومنع الوصول غير المصرح به؛ وإذا لم يكن ذلك ممكنًا، فيجب تعطيل الحساب مؤقتًا حتى استعادة السيطرة عليه.
- **إبلاغ الفريق الفني المختص بالأمن السيبراني:** يجب التواصل مع الوحدة الإدارية المسؤولة عن الأمن السيبراني في المؤسسة بشكلٍ فوري عقب اكتشاف الهجوم، للإبلاغ عن الحادث وتقديم التفاصيل اللازمة.

- **تنبيه المستخدمين والمشرفين:** يجب تنبيه جميع مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي حول الحادث لمنع حدوث أي تسرب إضافي للمعلومات.

3. إجراءات التصحيح واستعادة السيطرة على الحساب:

بعد اكتشاف الهجوم، يجب اتباع هذه الخطوات لاستعادة السيطرة على الحساب وتأمينه:

- **إعادة تعيين كلمات المرور:** يجب إعادة تعيين كلمات المرور فورًا لجميع الحسابات المتأثرة، ويجب أن تكون كلمات المرور الجديدة متوافقة مع سياسة كلمة المرور الواردة في دليل السياسات الوطنية لأمن وسلامة المعلومات، ويجب تمكين المصادقة الثنائية (2FA) على جميع الحسابات.
- **مراجعة سجل الأنشطة:** يجب تحليل سجل الأنشطة الخاص بالحساب المتأثر (التاريخ، الوقت، هوية المستخدم، موقع الدخول) لتحديد مصدر الهجوم ومعرفة ما إذا كان هناك محاولات اختراق أخرى.
- **التحقق من البريد الإلكتروني المرتبط:** يجب التحقق من أي تغييرات غير مصرح بها في البريد الإلكتروني المرتبط بالحساب أو أي تعديلات أخرى على إعدادات الحساب.

4. تحليل الهجوم وتقييم الأضرار:

بعد السيطرة على الحساب المتضرر، يجب إجراء تحليل شامل للهجوم لتحديد حجم الأضرار الناتجة، يتضمن ذلك:

- **تحديد نوع الهجوم:** هل كان الهجوم ناجمًا عن تصيّد إلكتروني، برمجيات خبيثة، أو استغلال ثغرة أخرى؟
- **تقييم المعلومات المسرّبة:** مراجعة المحتوى المنشور خلال فترة الاختراق، لتحديد ما إذا تم تسريب معلومات سرية أو نشر معلومات مضلّلة من قبل المخترقين.
- **تحليل أثر الهجوم على الجمهور:** يجب تقييم الأضرار التي قد تكون لحقت بالجمهور، مثل نشر روابط خبيثة أو استغلال المعلومات العامة.

5. إجراءات التواصل مع الجمهور:

- **في حال فقدان السيطرة على الحسابات:** في حال نشر معلومات من قبل المخترِقين، أو إذا تم اكتشاف أن الحساب قد تعرض للاختراق، فيجب على الجهة نشر بيان رسمي توضيحي على حساباتها على منصات التواصل الاجتماعي لإبلاغ الجمهور بحدوث الاختراق.
- **تنبيه الجمهور من الروابط الضارّة:** إذا كان الهجوم يتضمن نشر روابط أو محتوى ضار، يجب تحذير الجمهور بوضوح من النقر على تلك الروابط واتخاذ الإجراءات اللازمة لإزالة أي محتويات غير مرغوب فيها.

6. التوثيق والتقارير:

- **توثيق الحادث بالكامل:** يجب توثيق جميع الخطوات المتخذة أثناء الحادث، بما في ذلك وقت الاكتشاف، الإبلاغ، والإجراءات التصحيحية، وذلك لتقديم تقرير شامل للإدارة المختصة والأجهزة الرقابية ذات العلاقة.
- **تقديم تقرير تقني مفصل:** يجب تقديم تقرير فني يتضمن تحليل الهجوم والتدابير المتخذة لمنع تكرار الحادث، مع توصيات لتحسين الإجراءات الاستباقية للحد من مخاطر الهجمات السيبرانية في المستقبل.

7. المراجعة والتقييم بعد الحادث:

- **تقييم فعالية الاستجابة:** بعد انتهاء الحادث واستعادة الحساب، يجب إجراء مراجعة شاملة لتقييم مدى فعالية استجابة الفريق التقني ومدى سرعة استعادة السيطرة على الحسابات.
- **إدخال التحسينات** :بناءً على الدروس المستفادة من الحادث، يجب تحديث خطة الطوارئ والسياسات الأمنية لتحسين الحماية والاستجابة للهجمات السيبرانية مستقبلاً.

القوانين والآداب العامة:

ينبغي على جميع مشرفي الحسابات الرسمية للجهة على منصات التواصل الاجتماعي أثناء إدارتهم لهذه الحسابات الالتزام بالقوانين ذات العلاقة، ومراعاة الآداب العامة، ومراجعة أي محتوى بعناية قبل نشره، كما يتعين على الجهات الحكومية الالتزام بحظر نشر معلومات تضر بالأمن القومي أو استخدام الإنترنت لأغراض غير مشروعة، وتجنب نشر معلومات أو بيانات مسيئة أو عنصرية، يجب استخدام تكنولوجيا المعلومات والاتصالات بشكل يتماشى مع معايير الأمان والحماية المنصوص عليها في القانون، بما في ذلك حماية البيانات الشخصية والالتزام بالمعايير المعتمدة .

مراعاة حقوق النشر والملكية الفكرية:

يجب أن يكون مشرفو الحسابات الرسمية للجهة على منصات التواصل الاجتماعي على دراية كافية بحقوق النشر والملكية الفكرية والمخاطر المرتبطة بانتهاك هذه الحقوق، والاطلاع على القوانين واللوائح المنظمة لها وفهمها.

هذه الضوابط توفر إطار عمل واضح لاستخدام منصات التواصل الاجتماعي من قبل الجهات الحكومية في الدولة الليبية بما يتماشى مع القوانين واللوائح النافذة.
