مَمْلَكَة البَحْرَيْن

وَزَارَة شُؤُون الإِعْلَام

الدليل الإسترشادي لاستخدام شبكات التواصل الإجتماعي في الجهات الحكومية

الإصدار الأول 2019

وزارة شؤون الإعلام

الدليل الإسترشادي لاستخدام
شبكات التواصل الاجتماعي
في الجهات الحكومية

المحتويات

حرصت حكومة مملكة البحرين على تعزيز دور تقنية المعلومات في الارتقاء بالخدمات الحكومية التي تقدمها وزاراتها وهيئاتها المختلفة، وذلك لتحقيق خدمات أكثر جودة وسرعة وأمان للمواطنين والمقيمين على السواء في إطار مبادئ رؤية ٢٠٣٠.

وشهدت مملكة البحرين تقدماً كبيراً في قطاع تقنية المعلومات، كما حققت مراكز متقدمة إقليميا ودوليا في مؤشرات نمو قطاع تقنية المعلومات والحكومة الإلكترونية، وكان من بين الجوانب: إنشاء وتفعيل الحسابات الرسمية للجهات الحكومية في شبكات التواصل الاجتماعي، وذلك للتواصل الفعّال مع الجمهور، حيث أصبحت هذه الحسابات في وقتنا الحالي من أهم مصادر التواصل المباشر والأكثر فعالية لنشر الأخبار والمعلومات والرد على الاستفسارات والتساؤلات.

من هذا المنطلق، بادرت وزارة شؤون الاعلام بتكوين فريق عمل حكومي يضم خبراء تقنيين وقانونيين وممثلين عن وزارة شؤون الإعلام وهيئة المعلومات والحكومة الإلكترونية وجامعة البحرين لإعداد هذا الدليل الإرشادي، وذلك بهدف تحديد ضوابط استخدام شبكات التواصل الاجتماعية في الجهات الحكومية، ومساعدة القائمين على حسابات الجهات الحكومية على تحقيق الاستخدام الأمثل والآمن لها.

1.1. نطاق التطبيق

يستهدف هذا الدليل الإرشادي الجهات والهيئات الحكومية التي تملك حسابات رسمية في شبكات التواصل الاجتماعي، كما يستهدف جميع موظفي الحكومة بمختلف مستوياتهم الذين يملكون حسابات شخصية.

1.2. المصطلحات

- **شبكات التواصل الاجتماعي:** هي منصات إلكترونية تتيح للمستخدمين إنشاء ملفات تعريفية للتواصل مع باقي المستخدمين داخل حدود الشبكة، والدخول في مناقشات مشتركة وأنشطة تعاونية معهم، ونشر المحتوى بصيغ عديدة كالنص والصور وملفات الفيديو، إلى غير ذلك.
- **الجهة الحكومية:** أي جهة حكومية أو شبة حكومية تابعة لمجلس الوزراء في مملكة البحرين، ويشمل ذلك الوزارات والهيئات والإدارات والمؤسسات وغيرها.
- **التقنيات:** كافة الوسائل والأجهزة والأنظمة والإجراءات التي يمكن استخدامها من خلال شبكة الإنترنت للوصول إلى خدمة أو معلومة معينة لتحقيق الهدف الذي يسعى إليه المستخدم.
- **البرامج الخبيثة أو الفيروسات:** برامج يتم تضمينها عمداً لأغراض ضارة دون علم المستخدم،

والتـي يتـم تفعيلهـا لانتهـاك خصوصيـة المسـتخدم، وسرقـة المعلومـات، أو إتـلاف الأنظمـة، أو نـشر معلومـات خاطئـة، أو الوصـول إلى الحسـابات الخاصـة أو أجهـزة الحاسـوب الأخـرى.

- **الجمهـور المسـتهدف:** مجموعـة مسـتخدمي شـبكات التواصـل الاجتماعـي، والذين يتفاوت مسـتوى نشـاطهم مـن فعـال إلى متوسـط الى غـير فعـال، ويشـملون جميـع فئـات المجتمـع بمختلـف أطيافـه وتوجهاتـه وفئاتـه العمرية.

- **الحسـاب الرسـمي:** الحسـاب الخـاص بالجهـة الحكوميـة عـلى شـبكات التواصـل الاجتماعـي الـذي تـم اعتـماده، ويمثـل الوجهـة الإعلاميـة لتلـك الجهـة، وينـشر الأخبـار والتصريحـات الخاصـة بهـا.

- **الحسـاب الشـخصي:** الحسـاب الخـاص بالموظـف العـام في شـبكات التواصـل الاجتماعـي، والـذي لا يمثـل الجهـة الحكوميـة التـي يعمـل بهـا.

- **التصيـد الإلكـتروني:** نـوع مـن الهجـمات الإلكترونيـة يسـتهدف مسـتخدمًا أو مجموعـة بعينهـا، ويعمـل عـلى خـداع المسـتخدم، واسـتدراجه للقيـام بخطـوة معينـة، كفتـح مسـتند أو النقـر فـوق رابـط، ليتـم فتـح ثغـرة تـؤدي إلى بـدء هجـوم إلكـتروني عـلى الأنظمـة.

- **الهندسـة الاجتماعيـة:** عـدة تقنيـات تعتمـد عـلى اسـتغلال عنـصر الثقـة البـشري لجمـع المعلومـات الشـخصية عـن المسـتخدم المسـتهدف، ويمكـن مـن خـلال جمـع تلـك المعلومـات اختراق الحسـابات أو الاحتيـال الإلكتروني.

1.3. تصنيفات حسابات شبكات التواصل الاجتماعي

1.3.1 الحسابات الرسمية

وهـي الحسـاب الخـاص بجهـة حكوميـة مـا، وعـادة مـا تحمـل اسـم وشـعار الجهـة الرسـميين أو أحـد البرامـج أو المبـادرات التابعـة لهـا، ويُسـتخدم هـذا الحسـاب مـن قبـل الموظـف المكلّـف بـإدارة الحسـاب الرسـمي لنـشر توجهـات وتصريحـات وأخبـار الجهـة الحكوميـة بالنيابـة عنهـا بشـكل صحيـح ودقيـق.

1.3.2 الحسابات الشخصية

وهـي الحسـاب الخـاص بالموظـف العـام، وعـادة مـا تحمـل اسـم الموظـف نفسـه، وتشـمل فئتـين مـن الاسـتخدام:

- **اسـتخدام تنفيـذي:** يسـتخدم مسـؤول حكومـي رفيـع المسـتوى حسـاباته عـلى شـبكات التواصـل الاجتماعـي، وقـد يناقـش هـذا المسـؤول عـبر هـذه الحسـابات مواضيـع وقضايـا لهـا علاقـة بالجهـة

الحكومية التي يعمل بها، أو يركز على مناقشة مواضيع أخرى تعكس اهتماماته الشخصية مع المجتمع.

- **استخدام خاص:** يستخدم الموظف حساباته على شبكات التواصل الاجتماعي بصفته الشخصية لتنفيذ أنشطة خاصة به مثل: التواصل مع العائلة أو الأصدقاء، أو للوصول إلى محتوى ترفيهي، أو لتنفيذ أنشطة لها علاقة بمجال عمله كالحصول على معلومات جديدة، أو التواصل مع مجتمعات أخرى في مجال عمله.

1.4. المخاطر الأمنية

قد تتعرض حسابات شبكات التواصل الحكومية الرسمية لمخاطر أمنية من قبل المخترقين باستخدام تقنيات وأساليب مختلفة ومتعددة، لذلك ينبغي على الجهات الحكومية إجراء تقييم كامل للمخاطر الأمنية بشكل دوري على حسابات شبكات التواصل الاجتماعي الخاصة بها بحيث تشمل: نوعية المستخدمين، والتقنيات المتعلقة بالشبكات، وآلية إدارتها، وذلك بالتنسيق مع فرق أمن المعلومات أو تقنية المعلومات المختصة، والتي يتعين عليها تقديم النصح والإرشاد لفريق التواصل الاجتماعي حول المخاطر الأمنية المحتملة لتجنب الأخطاء والإبلاغ عنها.

وتتركز المخاطر الأمنية في: التعرض للبرامج الخبيثة أو الفيروسات، والتصيد الإلكتروني، والهندسة الاجتماعية، واختراق أمن كلمات السر، وكشف هوية المستخدم، وتسريب المعلومات وغيرها.

وقد يؤدي عدم وعي الموظفين العموميين بالمخاطر الأمنية إلى اختراق الحسابات، ما يؤدى إلى الإضرار بالجهة الحكومية المستهدفة.

2.1. شبكات التواصل الاجتماعية المعتمدة

يعتمد هذا الدليل الإرشادي شبكات التواصل الاجتماعي المذكورة أدناه ـ على سبيل المثال لا الحصر ـ وذلك لإنشاء حسابات الجهات الحكومية عبرها، وهي:

- تويتر (Twitter)
- انستغرام (Instagram)
- اليوتيوب (YouTube)
- لينكدان (LinkedIn)
- فيسبوك (Facebook)

2.2. ضوابط إدارة الحسابات

2.2.1 ضوابط إدارة الحسابات الرسمية

2.2.1.1 إجراءات إنشاء فريق لإدارة حسابات شبكات التواصل الاجتماعي في الجهات الحكومية:

- تخصيص فريق معني بإنشاء وإدارة الحسابات على شبكات التواصل الاجتماعي بناءً على توجيهات الإدارة العليا في الجهة الحكومية.
- ينحصر إنشاء حسابات الجهات الحكومية في شبكات التواصل الاجتماعي الملائمة لطبيعة ومتطلبات العمل.
- تحديد متطلبات تقنية المعلومات والقدرات التشغيلية المطلوبة وآليات متابعة ومراقبة الحسابات.
- الفريق المكلف في الجهة الحكومية هو المسؤول عن فتح وإلغاء وإدارة الحسابات الرسمية في الجهات الحكومية، وذلك حسب توجيهات الإدارة العليا.
- تدريب وتوعية فريق العمل المكلف بمخاطر أمن المعلومات وطرق الوقاية منها وبمهارات العلاقات العامة والتشريعات ذات العلاقة والتحديثات التقنية الخاصة بالشبكات.

2.2.1.2 آلية نشر ومتابعة المحتوى على حسابات شبكات التواصل الاجتماعي:

- يجب أن يتميز محتوى الحساب الرسمي للجهة الحكومية بالوضوح والشفافية والمسؤولية لتحقق الهدف المرجو من إنشائه، وبما يضمن توافر بيئة إيجابية تخلو من أي محتويات قد تعتبر مسيئة أو تمثل انتهاكا أو تجاوزا للقوانين والأعراف السائدة.

- الابتعاد عن المحتويات السلبيّة، إذ يجب على فريق العمل المعني بإدارة حسابات الجهة الحكومية حذف جميع الردود المسيئة، أو التي تحث على الكراهية، أو تخالف القانون أو الإعلانات أو أي محتوى آخر يخالف شروط الخدمة الخاصة بموقع التواصل الاجتماعي، أو يتناقض مع أية إرشادات منشورة ضمن شروط التواصل المحددة من قبل الجهة الحكومية في المنصات التي توفر خاصية الحذف.

- اتباع آلية لمراجعة واعتماد المحتوى قبل النشر من قبل المشرفين على شبكات التواصل الاجتماعي، ويفضل أن تكون من شخصين أو أكثر لضمان عدم نشر محتوى غير ملائم أو يسيء لسمعة الجهة الحكومية.

- مراعاة الالتزام بنشر المحتوى الخاص بالجهة الحكومية عبر جميع حساباتها الخاصة على شبكات التواصل، وبما يتوافق مع المستجدات.

- عدم نشر المحتويات غير اللائقة أو تخالف حقوق النشر أو معلومات الجهة الحكومية غير القابلة للنشر أو المخالفة للقانون.

- على المشرفين على حسابات التواصل الاجتماعية الرسمية نشر المحتوى المتعلق بالجهة الحكومية التي يمثلها بعيداً عن الآراء والتوجهات الشخصية.

- مراقبة المحتوى المنشور بشكل دائم، والتأكد من عدم تسبب هذا المحتوى في ردة فعل سلبية لدى المتابعين.

- استخدام الأجهزة المخصصة التي توفرها الجهة الحكومية ليتم فتح حسابات شبكات التواصل الاجتماعي الخاصة بها والعمل من خلالها، مع التأكيد على عدم فتح الحسابات الشخصية في هذه الأجهزة، وكذلك عدم إنشاء أو فتح وتفعيل الحسابات الرسمية في الأجهزة الشخصية.

- في حال عدم استخدام الجهة الحكومية لأحد حساباتها على شبكات التواصل لفترة تزيد عن الثلاثة أشهر، يتعين عليها مراجعة احتياجها لهذا الحساب، واتخاذ الإجراءات اللازمة لإلغائه.

2.2.1.3 آلية التفاعل مع استفسارات الجمهور:

- عند الرد على استفسارات الجمهور وأسئلتهم عبر الحسابات الرسمية يجب الحرص على أن يكون الرد بطريقة مناسبة ووافية.

- الرد على الاستفسارات من قبل الفريق المعني فقط مع ضرورة عدم الرد إلا بعد توافر المعلومات اللازمة مع مراعاة الضوابط الأمنية.

- التعامل مع الملاحظات السلبية ضمن آلية معتمدة ومعروفة ويجب عدم تجاهلها.

- يجب ألا يتم الاعتماد على الاجتهادات الفردية للرد على الملاحظات والاستفسارات السلبية، ويجب التعامل معها دائماً بمنهجية موحدة تتسم بالحرفية والإيجابية.

- في حال اعتماد الجهة الحكومية على طرف ثالث مثل شركة خاصة لإدارة حسابات شبكات التواصل الاجتماعي الرسمية، فعليها اتخاذ الإجراءات اللازمة لضمان عدم إساءة الاستخدام أو تشويه سمعة الجهة الحكومية، كما يجب على الجهة الحكومية ضمان توافر الصلاحيات اللازمة لإدارة الحسابات لديها متى ما تطلبت الحاجة.

2.2.2 ضوابط إدارة الحسابات الشخصية

- على جميع موظفي الجهات الحكومية الذين لديهم حسابات في شبكات التواصل الاجتماعي التحلي بأعلى معايير الأخلاق والقواعد السلوكية المتعارف عليها، والامتناع عن الإساءة أو التحريض ضد الآخرين، والالتزام بالنظام والآداب العامة، مع مراعاة الالتزام بمبادئ سرية المعلومات، وذلك من خلال عدم الكشف عنها أو استخدامها أو نسخها أو نقلها في شبكات التواصل الاجتماعي أو الكشف عن معلومات أو أخبار قد تعرض مصلحة أي جهة حكومية أو خاصة أو فرد للخطر أو الضرر، ويمكن الرجوع في هذا الشأن إلى مدونة قواعد السلوك الوظيفي وأخلاقيات الوظيفة العامة الصادرة عن ديوان الخدمة المدنية بمملكة البحرين رقم ١٦ لسنة ٢٠١٦.

- وبناء على التقسيم المعتمد في تصنيفات حسابات شبكات التواصل الاجتماعي حسب الاستخدام (البند 1-3)، فهناك ضوابط متعلقة بحسابات التنفيذيين وحسابات الموظفين الخاصة:

2.2.2.1 ضوابط استخدام حسابات التنفيذيين

- على المسؤول الحكومي التنفيذي أن يضع في الاعتبار أن أنشطته على شبكات التواصل الاجتماعي مرتبطة دوما بمنصبه كموظف عام، وقد يكون لذلك تأثير مباشر على أنشطة الجهة الحكومية أو صورتها. ويشمل ذلك المواد التي يشاركها عبر هذه الأنشطة، والموضوعات التي يناقشها مع الآخرين.

- التنسيق بين الحساب الشخصي للتنفيذيين والحسابات الرسمية الأخرى الخاصة بالجهة الحكومية، لتجنب أي تضارب في الأخبار أو التحديثات التي تنشرها هذه الحسابات أو الاستفسارات التي قد تردها من الجمهور، ولا ينبغي أن تنشر معلومات أو أخبار مخالفة لما يُنشر في حساب الجهة الحكومية.

- كجزء من استراتيجية التواصل الشاملة للجهة الحكومية، يُفضل دارسة الفوائد والمخاطر المحتملة المرتبطة بوجود المسؤولين التنفيذيين على شبكات التواصل الاجتماعي، كما يفضل

تحديد أهدافهم وجمهورهم المستهدف بشكل واضح، على أن يتم تقييم كل ذلك قبل البدء في استخدام شبكات التواصل.

- لا ينبغي الالتزام أو تقديم وعود لاتخاذ إجراء معين مع عدم وجود الصلاحيات اللازمة لذلك، كما يجب عدم نشر معلومات أو حقائق عن جهة حكومية تم رصدها بشكل شخصي أو بناءً على تحليلات شخصية.

2.2.2.2 ضوابط استخدام حسابات الموظفين الخاصة

- عدم نشر المعلومات الرسمية أو التعليق عليها أو تأكيد الشائعات المتعلقة بالجهة الحكومية.
- عدم استخدام البريد الإلكتروني الرسمي في إنشاء حسابات شبكات التواصل الاجتماعي الشخصية.
- تحويل الاستفسارات المتعلقة بالجهة الحكومية للأشخاص المعنيين بالتواصل مع الجمهور.
- على الموظف أن يعكس في حسابه الشخصي وجهة نظره الشخصية، وألا يتحدث باسم الجهة الحكومية التي يعمل بها.

2.3. ضوابط أمن المعلومات

2.3.1 تقييم المخاطر

على كل جهة حكومية القيام بتقييم كامل للمخاطر المحتملة باستخدام إطار معتمد من قبل الإدارة العليا بشكل دوري عند إنشاء واستخدام حسابات شبكات التواصل الاجتماعي بمشاركة الفرق المعنية مثل تقنية المعلومات والإعلام وغيرهم، كما ينبغي تحديد الحلول والإجراءات اللازمة للتعامل مع هذه المخاطر.

2.3.2 دخول الحسابات

- استخدام جهاز مستقل خاص بالجهة الحكومية، وربطه بحساباتها على شبكات التواصل الاجتماعي.
- ضمان تطبيق ضوابط أمن المعلومات في الأجهزة التي تُستخدم لإدارة حسابات شبكات التواصل الاجتماعي.
- استخدام شبكات موثوقة ومعتمدة من قبل الجهة الحكومية للاتصال بالإنترنت.

- تطبيق معايير الدخول الثنائي لدخول حسابات التواصل الاجتماعي الخاصة بالجهة الحكومية.
- على فريق العمل الذي يدير حسابات التواصل الاجتماعي للجهة الحكومية استخدام صلاحيات الدخول الخاصة بكل شخص، ويمكن تطبيق ذلك باستخدام أنظمة موثوقة ومعتمدة.

2.3.3 إدارة كلمة المرور

- يجب أن تكون كلمة المرور متوافقة لمتطلبات سياسة أمن كلمة المرور الصادرة من قبل هيئة المعلومات والحكومة الإلكترونية.
- استخدام كلمة مرور قوية لا تقل عن ٨ خانات، وبحيث تتكون من أحرف كبيرة وصغيرة ورموز وأرقام، وأن يتم تغييرها بشكل دوري.
- في حال استخدام برامج إدارة الحسابات، يتوجب على كل شخص من فريق العمل المكلف استخدام كلمة مرور خاصة به بحسابات التواصل الاجتماعي للجهة الحكومية في حال وجود أكثر من شخص يدير الحسابات.
- عدم استخدام كلمة مرور واحده لجميع حسابات التواصل الاجتماعي الخاصة بالجهة الحكومية ويجب استخدام كلمات مرور مختلفة.

2.3.4 إعدادات الحسابات

- مراجعة وتغيير إعدادات حسابات شبكات التواصل الاجتماعي، وذلك طبقاً لأفضل الممارسات.
- عدم اهمال إعدادات الخصوصية وأمن المعلومات.
- تدريب الموظفين على كيفية تحديث وضبط إعدادات الحسابات.
- العمل على توثيق الحسابات قدر الإمكان من قبل الشركات التي توفر هذه الخدمة.

2.3.5 المراقبة

- وضع آلية لمراقبة ومراجعة حسابات التواصل الاجتماعي على مدار الساعة من قبل الموظفين المعنيين للتأكد من المعلومات المنشورة وعدم وجود مخالفات أو محاولات اختراق.
- التحقق من بيانات دخول المستخدمين للتأكد من عدم وجود عمليات دخول ناجحة لأشخاص غير مصرح لهم، أو وجود صلاحيات دخول لأشخاص غادروا فريق العمل.

2.3.6 الحوادث الأمنية

عندما تتعرض الحسابات الرسمية للجهة الحكومية أو حسابات التنفيذيين على شبكات التواصل لحادث أمني كالاختراق، أو إنشاء حساب شبيه، أو تسريب لمعلومات سرية، فيجب على القائمين على إدارة الحساب التواصل مع إدارة الجرائم الإلكترونية في وزارة الداخلية في أسرع وقت ممكن لاتخاذ الإجراءات اللازمة، مع الحرص على إعادة ضبط كلمات المرور للحسابات الأخرى في شبكات التواصل الاجتماعي التي تملكها الجهة الحكومية، والعمل على نشر ما يفيد بحدوث اختراق أمني، خصوصا إذا تم نشر بيانات من قبل جهة الاختراق عبر الحساب الرسمي.

ويجب تحديد آلية التعامل مع الأخطاء التي قد تؤدي إلى تشويه صورة أو سمعة الجهة الحكومية. كما ينبغي تحديد آلية وقنوات التواصل مع شركات شبكات التواصل الاجتماعي للتواصل معها للتعامل مع الحوادث الأمنية.

تعتبر عملية تدريب وتوعية موظفي الجهات الحكومية ضرورية لمساعدة هذه الجهات على تقليل المخاطر الأمنية التي قد تتعرض لها، ومن الضروري أن يطلع الموظفون المكلفون على كيفية إدارة حسابات شبكات التواصل الاجتماعي الرسمية بطريقة صحيحة ومثلى، ومعرفة الحقوق والواجبات القانونية التي يتعين الالتزام بها.

وينبغي على الجهة الحكومية أن تكون على دراية تامة بأدوات التحكم الخاصة بالأمن والخصوصية، والتركيز على أهمية عدم تسريب أي معلومات سرية، والتدريب على بيانات الخصوصية الخاصة باستخدام شبكات التواصل الاجتماعي، ويمكن أن يتم التركيز في عملية التدريب والتوعية على الآتي:

- تدريب فرق عمل التواصل الاجتماعي باستمرار حول الاستخدامات المحدثة لشبكات التواصل الاجتماعي والمهارات ذات الصلة، بما في ذلك التدريب على متطلبات العلاقات والتشريعات ذات العلاقة.
- توعية فرق العمل عن المخاطر الأمنية المحتملة وكيفية تجنبها والخطوات التي يجب اتباعها في حال تعرض الحساب الرسمي إلى أحد المخاطر الأمنية.

يخضع جميع موظفي الجهات الحكومية أثناء إدارة والتعامل مع حسابات شبكات التواصل الاجتماعية الرسمية إلى القوانين الآتية:

- قانون ديوان الخدمة المدنية واللوائح والقرارات التابعة له.
- قانون حماية معلومات ووثائق الدولة.

ويجب على الموظفين العموميين الأخذ في الاعتبار القوانين ذات العلاقة مثل: قانون جرائم تقنية المعلومات، وقانون حماية البيانات الشخصية، وقانون النشر، وقانون العقوبات وغيرها. كما ينبغي عليهم الالتزام بمراعاة الآداب العامة وتجنب استخدام أية لغة مسيئة أو عنصرية بما يتعارض مع قوانين مملكة البحرين.

Ministry of Information Affairs
Media Administration
Printed at Government Printing Press

وزارة شؤون الإعلام
إدارة وسائل الإعلام
طبع بالمطبعة الحكومية