



سياسة حسابات مواقع التواصل الاجتماعي

الرقم:
التاريخ:
المرفقات:



٧٠٠٠٨٧٥٠٠٠

١٠٤

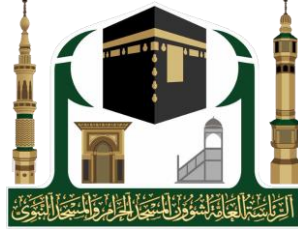
نسخة الوثيقة

النسخة	التاريخ	عدل بواسطة	الدور
V1	١٤٤٣/٩/١٠ هـ	مناع بن جمعان الغامدي	سياسة جديدة

المراجعة والتدقيق

النسخة	التاريخ	بواسطة	الدور	الإدارة
V1	١٤٤٣/٩/٢٠ هـ	م. سامي بن منير الوديناني	مراجعة وتدقيق	إدارة الحوكمة الرقمية
	١٤٤٣/١١/١ هـ	عبدالإله بن محمد الخزيم	مراجعة وتدقيق	إدارة الشؤون القانونية

الرقم:
التاريخ:
المرفقات:



٧٠٠٠٨٧٥٠٠٠

١٠٤

الأهداف

الغرض من هذه السياسة هو تحقيق الأهداف التالية:

- الاسهام في رفع مستوى الأمن السيبراني.
- تمكين مديري ومستخدمي حسابات التواصل الاجتماعي من استخدام شبكات التواصل الاجتماعي بطريقة آمنة.
- الاستعداد للاستجابة الفاعلة للحوادث السيبرانية التي قد ينجم عنها تأثيرات سلبية.
- الالتزام بضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات (OSMACC-1:2021) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

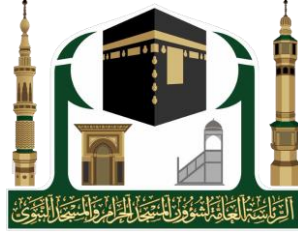
تطبق هذه السياسة على مديري ومستخدمي حسابات التواصل الاجتماعي.

بنود السياسة

الحسابات الرسمية الخاصة بالرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي:

- تدريب مديري الحسابات على الإجراءات اللازمة لضمان تطبيق متطلبات الأمن السيبراني.
- تحديد وحصر حسابات التواصل الاجتماعي للرئاسة والأصول المعلوماتية والتقنية المتعلقة بها، وتحديثها مرة واحدة سنوياً على الأقل.
- الالتزام بالمتطلبات التالية في إدارة هويات الدخول والصلاحيات:
 - استخدام حسابات التواصل الاجتماعي المخصصة للجهات، وليس الأفراد.
 - التسجيل باستخدام معلومات رسمية (بريد إلكتروني رسمي خاص لوسائل التواصل الاجتماعي للرئاسة ورقم جوال رسمي) وعدم استخدام معلومات شخصية.
 - توثيق حسابات التواصل الاجتماعي للرئاسة والمحافظة على هوية متسقة في جميع حسابات التواصل الاجتماعي؛ لتسهيل معرفة الحسابات الرسمية، واكتشاف حسابات الاحتيال.
 - استخدام كلمة مرور آمنة وخاصة لكل حساب من حسابات التواصل الاجتماعي للرئاسة وتغيير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل.
 - استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) لعمليات الدخول لحسابات التواصل الاجتماعي للرئاسة.
 - تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.
 - إدارة صلاحيات المستخدمين لحسابات التواصل الاجتماعي بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، وتنوعية الأجهزة والأنظمة المستخدمة.
 - حصر صلاحيات مقدمي خدمة إدارة حسابات التواصل الاجتماعي أو المراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الجهة من الانتحال.
 - الدخول لحسابات التواصل الاجتماعي للرئاسة من جهاز محدد.

الرقم:
التاريخ:
المرفقات:



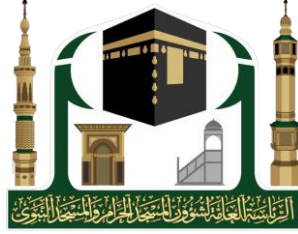
المملكة العربية السعودية
الوزارة الداخلية
الإدارة العامة للأمن السيبراني
إدارة الحوكمة الرقمية

٧٠٠٠٨٧٥٠٠٠

١٠٤

- يجب تحقيق المتطلبات التالية لحماية حسابات التواصل الاجتماعي للرئاسة والأصول المعلوماتية والتقنية المتعلقة بها:
 - تطبيق حزم التحديثات، والإصلاحات الأمنية لتطبيقات التواصل الاجتماعي مرة واحدة شهرياً على الأقل.
 - مراجعة إعدادات الحماية والتحصين لحسابات التواصل الاجتماعي للرئاسة والأصول التقنية الخاصة بها (Secure Configuration and Hardening) مرة واحدة سنوياً على الأقل.
 - مراجعة وتحسين الإعدادات الافتراضية (Default Configuration) لحسابات التواصل الاجتماعي والأصول التقنية، ومنها وجود كلمات مرور ثابتة أو تسجيل الدخول المسبق، وإقفال الأجهزة (Lockout).
 - تقييد تفعيل الخصائص والخدمات في حسابات التواصل الاجتماعي حسب الحاجة، على أن يتم تحليل المخاطر السيبرانية المحتملة في حال الحاجة لتفعيلها.
- يجب تحقيق المتطلبات التالية على الأجهزة المحمولة لحسابات التواصل الاجتماعي للرئاسة:
 - إدارة الأجهزة المحمولة لحسابات التواصل الاجتماعي للرئاسة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management- MDM)
 - تطبيق حزم التحديثات، والإصلاحات الأمنية للأجهزة المحمولة، مرة واحدة شهرياً على الأقل.
- يجب ألا تحتوي الأصول التقنية الخاصة بإدارة حسابات التواصل الاجتماعي للرئاسة على بيانات مصنفة، حسب التشريعات ذات العلاقة.
- يجب على إدارة الأمن السيبراني، بالتعاون مع مديري حسابات التواصل الاجتماعي، العمل على تقييم مخاطر الأمن السيبراني لحسابات التواصل الاجتماعي، مرة واحدة سنوياً، على الأقل.
- يجب على الإدارة العامة للموارد البشرية تضمين مسؤولية تطبيق متطلبات الأمن السيبراني والالتزام بها وفقاً لسياسات وإجراءات وعمليات الأمن السيبراني لحسابات التواصل الاجتماعي للعاملين في الإدارة العامة للإعلام والعلاقات العامة في الرئاسة.
- يجب على الإدارة العامة للإعلام تدريب العاملين المسؤولين عن الإدارة العامة للإعلام والعلاقات العامة في الرئاسة على المهارات التقنية والخطط والإجراءات اللازمة لضمان تطبيق متطلبات وممارسات الأمن السيبراني عند استخدام حسابات التواصل الاجتماعي.
- يجب تحقيق المتطلبات التالية في إدارة سجلات الأحداث ومراقبة الأمن السيبراني لحسابات التواصل الاجتماعي للرئاسة والأصول التقنية التابعة لها:
 - تفعيل جميع الإشعارات وتنبيهات الأمن السيبراني الخاصة بحسابات التواصل الاجتماعي للرئاسة وسجلات الأحداث (Event Logs) الخاصة بالأمن السيبراني على الأصول التقنية الخاصة بحسابات التواصل الاجتماعي للرئاسة.
 - متابعة حسابات التواصل الاجتماعي ومراقبتها للتأكد من عدم نشر أي محتوى غير مصرح، أو تسجيل أي دخول غير مصرح.
 - متابعة شبكات التواصل الاجتماعي ومراقبتها للتأكد من عدم انتحال هوية الرئاسة.
 - المراقبة الآلية لأي تغيير في نمط الحسابات أو مؤشرات اختراق أو نشر أي محتوى غير مصرح أو انتحال هوية الرئاسة.
- يجب تحقيق المتطلبات التالية في إدارة حوادث وتهديدات الأمن السيبراني:
 - وضع خطة استعادة حسابات التواصل الاجتماعي والتعامل مع الحوادث السيبرانية.
- تقييم مدى الحاجة لاستخدام خدمات إدارة الحسابات والمراقبة الآلية أو حماية هوية الجهة والمخاطر المتعلقة بها.
- يجب تحقيق المتطلبات التالية عند استخدام خدمات إدارة حسابات التواصل الاجتماعي (social media management) والمراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الرئاسة من الانتحال (brand protection)، بحد أدنى، ما يلي:
 - بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قبل الطرف الخارجي لبيانات الرئاسة عند انتهاء الخدمة.

الرقم:
التاريخ:
المرفقات:



٧٠٠٠٨٧٥٠٠٠

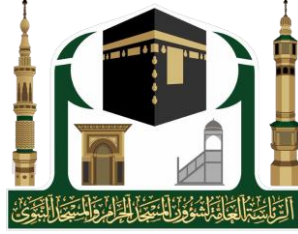
١٠٤

- إجراءات التواصل للإبلاغ عن الثغرات وفي حال اكتشاف حادثة أمن سيبراني.
- إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لحماية حسابات التواصل الاجتماعي للرئاسة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- يجب ألا يتم حذف أو تعطيل حسابات الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي بصورة مفاجئة وإنما ينبغي أن يكون ذلك عبر إبلاغ الإدارة العليا بذلك مع اتخاذ الترتيبات اللازمة حتى تتولى قنوات التواصل الاجتماعي الأخرى التعامل مع الخدمات التي كانت تقدم عبر الحساب الذي سوف يتم إغلاقه.
- يتحمل مشرف حسابات وسائل التواصل الاجتماعي للرئاسة كافة المسؤولية عما ينشر.
- عدم متابعة أي حسابات لا علاقة لها بأنشطة الرئاسة أو الانضمام لأي نشاط اجتماعي.
- عدم نشر الوثائق أو التعميم التي تصنف على أنها سرية أو سرية للغاية.
- يجب التأكد من المعلومة قبل النشر وربطها بالمصدر وأن المعلومة ضمن نطاق المسؤولية.
- يجب ألا يتم عمل إعادة نشر للحسابات الشخصية، ويمكن إعادة النشر لحسابات الجهات الحكومية الأخرى إذا توفر محتوى يفيد متابعي الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي.
- الالتزام باللغة العربية الفصحى وضوابط الإملاء في النشر، إلا إذا كان الموضوع يتطلب النشر بلغة أخرى.

❖ الحسابات الخاصة بمنسوبي الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي:

- يجب عدم نشر الوثائق والمعلومات التي تتعلق بالرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي.
- لا تجوز الإساءة إلى أي شخص، أو متابعة حسابات عنصرية، أو إباحية، أو حسابات تثير الفتن أو تتعارض مع سياسات الدولة.
- إذا عرف الشخص نفسه في مواقع التواصل الاجتماعي كمنسوب بالرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي أو تم ذكر الصفة (وكيل الرئيس العام، وكيل مساعد، مدير عام، مساعد المدير العام، مدير، وكيل، موظف) يجب توضيح أن الحساب يمثل كـ شخص ولا يمثل الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي.
- يجب ألا يستغل المنصب الإداري في المصالح الشخصية.
- لا يسمح بأن يتم التواصل باسم الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي أو تمثيلها أبداً من خلال الحسابات الشخصية.
- يجب عدم استخدام شعار الرئاسة أو أرقام التواصل الخاصة بالرئاسة أو أي معلومات في المعرف الشخصي.
- لا يحق للموظف التسجيل في برامج التواصل الاجتماعي بالبريد الإلكتروني الخاص بالرئاسة.
- لا يحق للموظف نشر الأخبار قبل أن تصدر عن الجهة المسؤولة أو المتحدث الرسمي باسم الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي.

الرقم:
التاريخ:
المرفقات:



المملكة العربية السعودية
الرئاسة العامة لشؤون الحرمين والمسجد النبوي
الإدارة العامة للأمن السيبراني
إدارة الحوكمة الرقمية

٧٠٠٠٨٧٥٠٠٠

١٠٤

الأدوار والمسؤوليات

راعي ومالك وثيقة السياسة: الإدارة العامة للأمن السيبراني.

مراجعة السياسة وتحديثها: إدارة الحوكمة الرقمية.

تنفيذ السياسة وتطبيقها: الإدارة العامة للأمن السيبراني ومديري حسابات التواصل الاجتماعي ومنسوبي الرئاسة.

الالتزام بالسياسة

- يجب على الإدارة العامة للأمن السيبراني ضمان التزام الرئاسة بهذه السياسة دورياً.
- يجب على جميع العاملين في الرئاسة الالتزام بهذه السياسة.
- أن عدم الالتزام بهذه السياسة يعد مخالفة إدارية تستدعي تطبيق العقوبات المقررة بأنظمة الموارد البشرية، مع عدم اغفال إحالة المخالف إلى الجهات المختصة في تطبيق الأنظمة الأخرى ذات العلاقة مثل نظام مكافحة الجرائم المعلوماتية، ونظام عقوبات نشر الوثائق والمعلومات السرية وافشاؤها، نظام المطبوعات والنشر، ونظام التعاملات الالكترونية.