3-STEP ACTION PLAN FOR GOVERNMENT

MINIMIZE SOCIAL MEDIA SECURITY RISK IN 2019

Does your agency have a plan in place for a social media account breach? Build your agency's security confidence with a strong action plan.

Only 39% of government social media officials are confident in their agency's current security practices.

Hootsuite,
The Social Government Benchmark Report 2018

Government agencies are using social media to enhance citizen engagement, deliver better services, and meet their agency goals. Security is the underlying factor in achieving those benefits—but many agencies fail to address this critical element.

Today, agency staff must be able to reliably access their social media accounts from multiple devices, and often share access with multiple team members, which significantly increases the risk involved. For example, what happens if you're managing a military account that's breached, and the hacker tries to declare war via social media? That's an extreme example, but it underscores the need for agencies to prepare a multi-layer security plan to protect themselves and citizens.

Agencies evaluating their social media security must ensure adequate security measures are in place for every layer of activity, as well as a planned strategic response for any adverse events.

START WITH THIS 3-STEP PLAN TO SECURE YOUR AGENCY'S SOCIAL MEDIA USE:

1. Plan your team's access
2. Use multi-factor authentication
3. Build a strategic emergency response plan

PLAN YOUR TEAM’S ACCESS

As social media becomes a primary communications channel for government agencies, a social media management platform becomes crucial to ensure security.

Instead of sharing social media account passwords with a whole team, make a plan that identifies who needs account access, to which accounts, and to what level of usability. Select a platform that lets you set customizable permissions based on roles, as well as workflows for content approval and publishing.

ACTION PLAN

- Maintain an active directory listing the exact individuals who have the password(s) for each account.
- Use single sign-on for systems that provide a one-time sign-in option if team members are trying to access accounts via mobile or offsite.
- Put a plan in place for when someone leaves, including how to quickly revoke access and change account passwords.

> “This year, agencies are going to need to take a more proactive approach to their social media security. By putting the right tools and processes in place, government can enjoy the benefits of engaging with citizens on social media without the risk of access breaches or hacks.”

Ben Cathers
Principal Government Solutions Consultant, Hootsuite

1 Plan your team’s access
2 Use multi-factor authentication
3 Build a strategic emergency response plan

USE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication requires a user to present two or more pieces of evidence to sign in to a system (typically a password followed by an approval from a separate device).

With multi-factor authentication in place, it's much more difficult for unauthorized users to access—or potentially take control of—your systems, even if they gain access to an employee's credentials.

ACTION PLAN

- Decide whether multi-factor authentication will be done via app-based integration, email, or text.
- Designate who will be in charge of receiving and approving multi-factor notifications.
- Create a security plan for investigating any failed login attempts.
- Build a culture that enforces use of multi-factor authentication for all types of login, not only social media.
- Recognize that multi-factor authentication isn't a cure-all, but will contribute to a more secure digital environment for your agency.

> "Hootsuite Enterprise helps ensure security, which breeds credibility."
>
> **Greg Licamele**
> Director of External Communications,
> Fairfax County Government

1 Plan your team's access

2 Use multi-factor authentication

3 Build a strategic emergency response plan

BUILD A STRATEGIC EMERGENCY RESPONSE PLAN

What happens if your account is taken over? What steps can you take to regain control?

Responding to emergency events is a reality for every government agency. To ensure your plan is effective, consider security goals alongside overall social media goals.

ACTION PLAN

- Create an easily accessible first-response plan if passwords need to be changed on multiple social media accounts. Communicate the plan location to the team clearly and often.
- Include your social media handles in communications, on signage, and in email signatures to encourage citizens to engage—particularly regarding security concerns.
- Maintain regular communication on social media:
  - Set a standard: Post once a day if possible, and at least 3–5 times per week. Respond to inquiries within 24–48 hours.
  - During a crisis: Post updates and respond to citizen inquiries in real time on a 24–hour cycle.
- Develop a crisis response plan for how you'll communicate information to citizens in case of a breach, including:
  - What happened, and what the agency knows so far.
  - What actions are being taken to correct the issue.
  - What citizens can do, and where they can go to find out more.
- Monitor what influencers are saying about your agency, or about topics relevant to to your agency, to gain insight into potential concerns and better tailor messaging to address citizens' needs.

1 Plan your team's access

2 Use multi-factor authentication

3 Build a strategic emergency response plan

WHY USE A SOCIAL MEDIA MANAGEMENT PLATFORM?

A social media management platform guards agencies against risk from preventable breaches resulting from the sharing of passwords and accounts, making social media security infrastructure stronger and more cost efficient.

In fact, small teams can meet social media security and management requirements for less than the cost of the average agency's monthly printing supply expenses.

Hootsuite maintains a high level of security standards as described in our Trust Center. Our security controls are verified with an annual SOC 2 Type II audit conducted by an independent internationally recognized accounting firm.

ADDITIONAL RESOURCE

The Social Government Benchmark Report

ABOUT HOOTSUITE

Hootsuite is the most widely used social media management platform. Our battle-tested technology, extensive ecosystem, and social DNA help government agencies understand, inform, and engage citizens through a centralized, secure, and scalable social media platform. More organizations trust our technology than anyone else: We have over 16 million users, including over 2,500 government customers and employees at more than 800 of the Fortune 1000.

Hootsuite®

ABOUT CARAHSOFT

Carahsoft is the public sector partner for Hootsuite products and services supporting customers through needs analysis, configuration support, simplified ordering and special Government pricing. Through this partnership, we provide public sector organizations with easy access to the Hootsuite platform through the following contracts GSA, SEWP V, CMAS, National IPA, VASCUPP, MD COTS, COSTARS, City of Seattle, New Mexico, Ohio STS, and NCPA. Carahsoft is The Trusted Government IT Solutions Provider®, with a proven history of helping government agencies select and implement the best possible technology solution at the best possible value.

carahsoft.

For more information on enacting the best practices presented in this action plan through Hootsuite, contact Carahsoft at (703) 581–6599 or Hootsuite@carahsoft.com