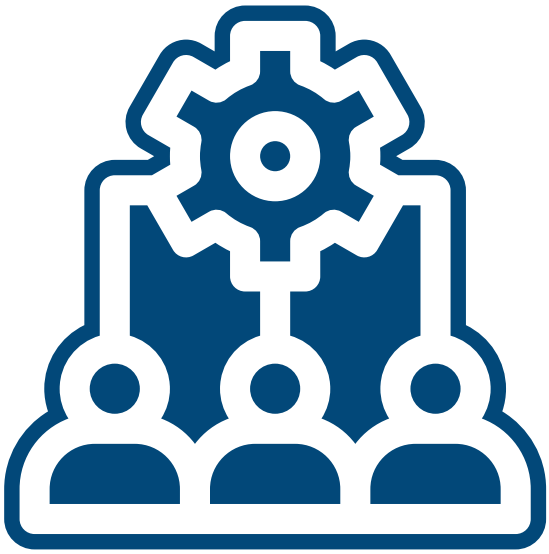
Social Media for Local Governments

Social media plays an important role in expanding traditional channels of resident engagement. When used strategically, social media can give agencies the ability to grow online communities and leverage social content as a service. Through sharing real-time updates for your programs and services, disseminating information during times of crisis, and giving followers a thoughtful behind-the-scenes look at your operations, the use of social media can help humanize and enhance transparency for your agency, build trust with your community, and strengthen your workforce talent attraction and retention efforts.

The Michigan Department of Technology, Management & Budget (DTMB) recommends the following security and governance best practices when establishing or reviewing your organization's social media policies and use.



Centralizing Social Media Program Governance Controls

- Have an information technology (IT) acceptable use and social media policy for official agency accounts.
- Identify who should be using social media for business purposes and how they should use it.
- Implement a social media training and onboarding process for newly authorized account authors.
- Consider creating an authorized users list and have users sign off on use.
- Establish a process for requesting, reviewing, creating, and managing accounts.
- Have engagement guidelines for staff as they manage accounts.
- Avoid blocking, banning, and muting users.
- Have a plan and practice in place for content moderation.
- Identify and implement social media best practices for reaching your business goals.

Account Security

- Use official agency IT devices to manage authorized accounts.
- Connect using a virtual private network (VPN) when possible.
- Avoid using public WiFi to manage accounts. If public WiFi is used, consider installing a mobile security app, like Michigan Secure at Michigan.gov/MichiganSecureApp.
- Enable multifactor authentication (MFA) or two-factor authentication (2FA) for official accounts.
- Limit third-party applications, tools, and services from accessing your social media accounts.
- Ensure account privacy settings are reviewed regularly and are carefully managed.
- Consider issuing devices that are "off your network" (isolated) if you have security concerns for specific platforms.

DTMB
Technology, Management & Budget

Social Media for Local Governments

Organizational IT Considerations

- Implement a security awareness training program for staff. Consider adding information around social media use and general tips for staying safe online. Related to training, KnowBe4, the world's largest integrated platform for security awareness training is now part of the State of Michigan's extended purchasing program, MiDEAL, which allows Michigan cities, townships, villages, counties, school districts, universities, colleges, and nonprofit hospitals to buy goods and services from state contracts. Learn more at Michigan.gov/MiDeal.
- Consider the use of cloud security technology or a whitelisting service to allow/disallow certain sites from being accessed on your network.
- Install firewalls, virus protection, and/or end-point protection product on laptops and desktops.
- Have a process to ensure all devices have the latest upgrades, security patches, etc.
- Install a mobile security app on mobile devices.
- If your account or device is compromised, call the Michigan Cyber Command Center (MC3) at 1-877-MI-CYBER (1-877-642-9237).

Michigan Secure

- Michigan Secure alerts you to unsecure Wi-Fi networks, unsafe apps in Android, system tampering, and more.
- It helps protect your mobile device or Chromebook without requiring any personal, private information.
- It costs $0 to download, $0 to use, no in-app purchases, and no ads.
- It gives you the tools to determine the best action to help protect yourself.
- It helps you determine whether a link sent to you through email, text, a messaging app, or social media is safe or a possible phishing attempt.
- Don't leave your device unprotected, learn more at Michigan.gov/MichiganSecureApp.

Download on the App Store

GET IT ON Google Play

For additional social media and cybersecurity practices from the State of Michigan, visit DTMB's Cybersecurity Resource Hub at Michigan.gov/CyberSecurity and Michigan.gov/SocialMedia.

DTMB Technology, Management & Budget