CHAPTER 16

SOCIAL MEDIA

REVISED APRIL 2025

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 16

SOCIAL MEDIA

1. PURPOSE.

a. Government agencies are taking advantage of social media (e.g., Facebook, Instagram, and X [formerly Twitter]) to reach out to the public in an effort to inform and provide better service; along with these benefits comes certain risks. This chapter is aimed at addressing the risks associated with the use of social media and to define the requirements related to the use of social media.

2. DEFINITIONS.

a. Social Media. Social media, also referred to as Social Networking and Web 2.0 technologies, are applications which allow users to collaborate and share information over the Internet with a network of other social users or the community as a whole (e.g., Facebook, YouTube, X [formerly Twitter], Instagram, LinkedIn, etc.).

b. Agency. When capitalized, the term "Agency" refers to one of the state's super Agencies (e.g., Consumer Services Agency or the Health and Human Services Agency). When used in lower case, the term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this chapter, "agency" and "department" are used interchangeably.

3. SCOPE.

a. The use of social media falls within two fundamental categories:

(1) Obtaining information and performing research.

(2) Sharing or posting official agency information (a two-way flow of information).

b. The first category is covered in Chapter 18, Acceptable Use Policy, of this manual. The second category subjects the Department to possible exposure of confidential data, and is both a cyber security and business communication issue.

c. As with any Internet use, the Department must provide protection from cyber security risks associated with the use of social media. However, the specific risk associated with the use of social media technologies centers primarily around the unauthorized sharing or posting of official Department information.

4. POLICY.

a. Approval Process. The Community Outreach and Marketing Section (COMS) is the Office of Primary Interest for outreach activities including the use of social media. An official request to use social media must be made to COMS for approval. If approved by COMS, the request shall be routed to the Information Management Division (IMD) and reviewed by the Information Security Officer (ISO) for risks associated with the request. If approved by the ISO and IMD, the request will be implemented by Information Technology (IT) staff.

b. Requirements and Conditions. Pursuant to the State Information Management Manual (SIMM), Section 66B, Social Media Standard, the following requirements must be met:

(1) General Agency Management Requirements.

(a) Prior to authorizing and enabling Internet access to social media websites, agency management shall conduct a formal risk assessment of the proposed connections utilizing agency Risk Management processes. The assessment shall, at a minimum, include the analysis of the risks (including risk mitigation strategies) involved in providing users access to social media websites including:

1 Employee productivity.

2 Network bandwidth requirements and impacts.

3 Reputational risk to personnel, the agency, and the state.

4 Potential avenue for exposure or leakage of sensitive or protected information (e.g., copyrighted material, intellectual property, personally identifying information, etc.).

5 Potential avenue for malware introduction into the organization's IT environment.

6 Potential use of "other than government" sections of social media websites.

(b) State agencies shall document this risk analysis and retain it for a minimum of two years.

(2) Agency Information Technology Administrator Requirements.

(a) Agency IT Administrators shall limit Internet access to social media websites according to the agency's acceptable use policy, while allowing authorized users to reach content necessary to fulfill the business requirements. Limitations may include, but are not limited to:

1 Opening Internet access only to the government sub-domains on the social media websites.

2 Allowing Internet access to users who are specifically authorized.

3 Preventing unnecessary functionality within social media websites (e.g., instant messaging or file exchange).

4 Minimizing and/or eliminating the addition of web links to other websites (e.g., "friends") to minimize the risk of exposing a government user to a link that leads to inappropriate or unauthorized material.

(b) Enable technical risk mitigation controls to the extent possible. These controls may include:

1 Filtering and monitoring of all social media website content posted and/or viewed.

2 Scanning any and all files exchanged with the social media websites.

(3) User Requirements.

(a) Users shall connect to, and exchange information with, only those social media websites that have been authorized by agency management in accordance with the requirements within this and other agency and state policies.

(b) Users shall minimize their use of "other than government" sections of the social media websites.

(c) Users shall not post or release proprietary, confidential, sensitive, personally identifiable information, or other state government intellectual property on social media websites.

(d) Users who connect to social media websites through state information assets, who speak officially on behalf of the state agency or the state, or who may be perceived as speaking on behalf of an agency or the state; are subject to all agency and state requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.

(e) Users shall not speak in social media websites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency's Public Information Office. Users may not speak on behalf of the state unless specifically authorized by the Governor.

(f) Users who are authorized to speak on behalf of the agency or state shall identify themselves by full name, title, Agency, and contact information when posting or exchanging information on social media forums, and shall address issues only within the scope of their specific authorization.

(g) Users who are not authorized to speak on behalf of the agency or state shall clarify that the information is being presented on their own behalf and that it does not represent the position of the state or an agency.

(h) Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes or for other legitimate state purposes as defined in agency policy.

(i) Users shall avoid mixing their professional information with their personal information.

(j) Users shall not use their work password on social media websites.

NOTE: In addition to the above SIMM Section 66B requirements, the following Information Technology Policy Letter 10-02, Social Media, requirements must also be met:

1 Managers and users with access to social media websites are trained regarding their roles and responsibilities.

2 Assign the responsibility for management and monitoring of social media websites to the individual or entity responsible and authorized for outward-facing communications for the agency.