Social Media Policy: City of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **PURPOSE AND APPLICATION**

a. The purpose of this policy is to establish City of \_\_\_\_\_\_\_\_\_\_\_\_\_ (city) general standards and responsibilities for the acceptable use of social media. This policy governs the use, administration, management, monitoring, and retention of social media and social media content, consistent with state, federal and city laws and regulations.

b. This policy is applicable to employees of the city, including part-time and full-time employees, who create or contribute to social media.

c. In addition to this policy, all social media activity shall comply with any and every other applicable city policy including but not limited to: (ADD OR DELETE POLICIES AS APPLICABLE)

 i. Open Records Policy

ii. Internet Use Policy

iii. IT Use, Security and Accessibility Policy

iv. Ethics/Conflict of Interest Policy

v. Public Records and Record Retention Policy

2. **DEFINITIONS**

a. Social Media Channels: Any online communication channel dedicated to community-based input, interaction, content-sharing and collaboration including websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation and wikis. Social media can take many forms, including but not limited to text, images and video. Examples covered include, but are not limited to, Facebook, Twitter, LinkedIn, YouTube, and Google+.

b. Authorized Employee: An employee who has been authorized to post social media content on behalf of the city, including but not limited to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

c. Mobile Apps: Technologies that can be downloaded to smartphones and tablets and accessed on the go; provides publishing abilities to authorized employees who work at a city worksite or offsite.

3. **USE OF SOCIAL MEDIA**

**Official Use of Social Media on Behalf of the City**

a. Only authorized employees may post content to social media channels on behalf of the city.

b. Authorized employees should not disclose confidential or proprietary information acquired by way of their official position with the city. This restriction applies whether the information is disclosed on professional or personal social media channels, or by any other method.

c. All official use of social media must be through authorized official social media accounts. Authorized employees using social media for official purposes are prohibited from using personal social media accounts for those purposes. This is to facilitate compliance with public records law and protect information on personal accounts from public disclosure.

d. Authorized employees should always consider whether it’s appropriate to post an opinion, commit the city to a course of action, or discuss areas outside the employee’s expertise online.

e. Authorized employees posting content on behalf of the city may not include profanity or obscenity.

f. Authorized employees posting content on behalf of the city must respect the intellectual property rights of others and shall comply at all times with intellectual property laws including the Copyright Act and the Lanham Act. Authorized employees should seek legal counsel before posting any content subject to trademark or copyright protection to ensure compliance with the law.

g. Authorized employees should conduct themselves in a professional manner at all times while utilizing or posting to city social media channels. Authorized employees are prohibited from engaging in disagreements or arguments with members of the public who may be critical of the city on social media channels.

g. Authorized employees must comply with the Terms of Service of social media channels utilized on behalf of the city.

h. The city reserves the right to delete posts that are objectionable or offensive in nature, not relevant or off-topic, inaccurate, and those which violate a social media channel’s Terms of Service.

i. \_\_\_(mayor/manager/communications director)\_\_\_\_\_\_\_\_\_\_\_\_\_\_ shall have final authority to edit or remove content from any of the city’s social media channels.

j. Hourly employees should not work on social media for official city purposes after hours without prior approval. This is considered overtime, and failure to obtain prior authorization may be cause for corrective action.

**Personal Use of Social Media**

a. Employees may access personal social media accounts at work for limited personal communications, but only as long as it does not interfere with work responsibilities and does not violate the city’s IT access and use policy or any other personnel policies or Code of Conduct for a particular department.

b. Employees may not use a city email address when using social media channels for personal use.

c. An employee may not characterize him or herself as representing the city, directly or indirectly, in any social media channel posting or account. The use of a city e-mail address, job title, official city name, seal or logo shall be deemed an attempt to represent the city in an official capacity and is prohibited on personal use of social media. Other communications leading an average viewer to conclude that a posting was made in an official capacity shall also be deemed an attempt to represent the city in an official capacity and is prohibited.

**Desktop Applications:**

In order to prevent accidental posting of personal information on or from city social media channels, authorized employees should not use professional and personal social media channels in the same system for managing social media channels (e.g. the same dashboard). If employees use desktop applications to manage city social media channels, they must use their city email address and a password that’s unique to the application (i.e. not the same as their city email password). Employees should use a personal email address to access a separate dashboard used for personal social media use.

**Mobile Apps:**

Authorized employees should use different mobile apps for professional and personal use of social media channels. If an employee uses Twitter’s mobile app to manage a city Twitter account, for example, they should not use that same mobile app to send personal tweets. It is recommended that authorized employees with smartphones download social media mobile apps such as the Facebook Page Manager mobile app to post information to city social media channels. Mobile apps should be set up to allow authorized employees to post to a city social media channel without accessing the employee’s personal social media accounts.

4. **EMPLOYEE RIGHTS**

Nothing in this policy will be interpreted or applied in a manner that interferes with employee rights to organize, form, join, or assist labor organizations, to bargain collectively through representatives of their choosing to the extent allowed by law, or to engage in other concerted activities for the purpose of addressing the terms and conditions of employment. Further, nothing in this policy is meant to prevent an employee from exercising his or her right to make a complaint of discrimination or other workplace misconduct. This policy does not prohibit employees from publicly expressing an opinion on a matter of public concern that does not unduly disrupt city operations.

**5. DISCLOSURE AND PRIVACY**

Employees have no expectation of privacy when using city owned equipment. The city has the right to access and monitor its computers, equipment and systems without warning or any specific notice to employees.

4. **DISCIPLINARY ACTION**

Inappropriate use of social media can be grounds for corrective action, including disciplinary action.

**DISCLAMER**

NOTE:  This document is being provided to you from our AMIC/MWCF Loss Control Division and it is not intended to be legal advice.  It does not identify all the issues surrounding the topic. Laws and “Best Practices” change and policies must be continually reviewed to updated as needed.  Public agencies are encouraged to review their procedures with an expert or an attorney who is knowledgeable about the topic. Reliance on this information is at the sole risk of the user.