I. INTRODUCTION

A. Purpose: This instruction establishes the Los Angeles County Fire Department (Department) policy on the management, administration, and oversight of its official social media accounts.

B. Background: Social media is a valuable means of assisting the Department in meeting its responsibilities of community outreach, public information, and education. Social media enhances the Department's ability to communicate information in a timely manner to the public.

C. Scope: This policy applies to all employees to include: permanent, temporary, recurrent, and temporary agency employees.

1. If any portion of this policy is found to conflict with State or federal law, only that portion shall be superseded by the law, and all remaining portions of this policy shall remain in effect.

D. Author: The Fire Chief, through the Executive Support Division (ESD) manager, shall be responsible for the content, revision, and review of this policy.

E. Authority: The Department has been given the authority to publish this policy by the Board of Supervisors Policy Manual 6.105 Internet Usage Policy.

F. Definitions: See Appendix I

II. RESPONSIBILITY

A. The ESD and the Employee Services Section, through the Public Information Office (PIO), shall approve and oversee official Department social media accounts.

1. Social Media Administrators (SMAs) shall post, review replies, and interact with the public on sites within their division in collaboration with the ESD, PIO, or Fire Chief.

a. Business Operations matters will be referred to the ESD.

b. Emergency Operations matters will be referred to the PIO.

2. The ESD and PIO shall have administrative rights and access to all official Department social media accounts.

B. The Department's Information Security Officer (DISO) shall provide oversight on any security issues with Department social media accounts. A Los Angeles County Computer Security Incident Report (CSIR) will be submitted by the DISO for all security incidents involving Department social media accounts.

1. SMAs shall report all actual or suspected security incidents that include, but are not limited to, unauthorized content to the ESD and PIO as soon as possible and;

2. SMAs shall report all actual or suspected security incidents (e.g., hacking) affecting Department social media accounts to the DISO (IMDInfoSec@fire.lacounty.gov) by the next business day.

III. POLICY

A. Department Social Media Accounts

1. All official Department social media accounts shall:

   a. State that if there is an emergency, 911 should be called.

   b. State they are not monitored 24/7.

   c. Clearly indicate they are maintained by the Department and have the Department logo and contact information displayed.

   d. Display a uniform design that includes the Department logo and its respective division or section name.

   e. Link to the Department's official website.

      1) If space permits, link to or mention the Department's respective main social media account (e.g., a division's Facebook account shall link or mention the Department's main Facebook account; a division's Twitter account shall link or mention the Department's main Twitter account).

   f. If space permits, state that the opinions expressed by visitors to the page(s) may not reflect the opinions of the County of Los Angeles or the Department.

g. Reserve the right to remove obscenities; off-topic comments; personal attacks; discriminatory content; sexual content or links to sexual content; solicitations of commerce; conduct or encouragement of illegal activity; information that may compromise the safety or security of the public or public systems; copyright infringement; or any other content the SMAs deem inappropriate. The ESD and PIO reserve the final authority to remove any content deemed inappropriate.

h. Only post content that adheres to all applicable Departmental policies and procedures, including information technology (Information Technology Acceptable Use Agreement, V8-C1-F45) and records management (Department policies under V3-C9 Written Communication and Records).

i. Be regularly monitored by the ESD or PIO.

j. Not use the image or likeness of the Fire Chief or any Department member as an account's profile image without their written consent or approval.

2. New SMAs and social media accounts shall be approved by the ESD and PIO before activation.

3. Fire stations, sections, units, or any other Departmental subgroups shall submit social media content to their jurisdictional assistant fire chief or division manager and to the SMA for posting on behalf of the Department, and not create, manage, or operate any form of social media accounts on their own behalf.

4. Only SMAs shall operate approved and active Department social media accounts (see Manual A, Subject H).

5. SMAs shall:

a. Conduct themselves at all times as representatives of the Department and shall adhere to the Department's Standards of Behavior policy (V2-C1-S4).

b. Attempt to use a Department-issued device to manage the Department's social media activities.

c. Not disseminate or transmit personal viewpoints.

d. Use caution when applying scheduled or timed post options.

e. Not post pictures depicting patients. This is strictly prohibited.

IV. PROCEDURES

A. Posting emergency incident information, images, and/or electronic media on social media accounts.

The PIO shall be the primary contact in posting emergency incident information, images, and/or electronic media on social media accounts.

1. If the PIO is on-scene at an emergency incident, SMAs may post (or repost) emergency incident information, images, and/or electronic media on social media accounts disseminated by the PIO with the approval of the Incident Commander (IC).

2. If the PIO is not on-scene at an emergency incident, SMAs may post emergency incident information, images, and/or electronic media on social media accounts with the approval of the IC.

B. Posting non-emergency information, images, and/or electronic media on social media accounts.

1. SMAs may post (or repost) Division-related information, images and/or electronic media on social media accounts (e.g., announcement of CERT and CPR Anytime classes, public safety themes, city/community events and related programs, information, and activities, etc.).

2. SMAs may post (or repost) County and Department-related information, images, and/or electronic media on social media accounts in collaboration with the ESD (e.g., Ready! Set! Go!, Firefighter Memorial, recruitment events, upcoming exams, Explorer Program events, Los Angeles County Charitable Giving Campaigns, etc.).

C. Reporting violations:

1. SMAs shall report non-approved posts and unauthorized content to the ESD and PIO (info@fire.lacounty.gov) as soon as possible.

2. SMAs shall report all actual or suspected security incidents affecting Department social media accounts. Incidents shall be reported to the DISO (IMDInfoSec@fire.lacounty.gov) by the next business day.

3. A Los Angeles County CSIR will be submitted by the DISO for all security incidents involving Department social media accounts.

APPENDIX I

Blog: A self-published diary or commentary on a particular topic or several related topics that may allow visitors to post responses, reactions, or comments.

Electronic Media: Any communication, recording, or transmission of electronic messages, files, data, and all forms of digital and film imagery or other electronic information.

Official Department Social Media Accounts: Social media accounts approved and managed by authorized Department personnel.

Post: Content an individual shares on a social media site or the act of publishing content on a site.

Profile: Information that a user provides about themselves on a social networking site.

Profile Image: An image a user provides to represent themselves on a social networking site.

Security Incident: Any malicious act or suspicious event that compromises or attempts to compromise a computer account, system, or application.

Social Media: A form of electronic communications where users are encouraged to participate and interact by creating and sharing ideas, information, personal messages, videos, pictures, audio, etc. through websites, pages, and/or applications. This includes, but is not limited to, social networking sites (e.g., Facebook, Facebook Live), microblogging sites (e.g., Twitter, Nixle), photo- and video-sharing sites (e.g., Periscope, Instagram, Snapchat, YouTube), wikis (e.g., Wikipedia), blogs, LinkedIn, and other sites.

Social Media Administrator (SMA): A designated Department user authorized to create, post, moderate, delete, and otherwise manage content and/or other settings on the Department's official social media sites and pages. SMAs are the Communications Section of the Executive Support Division (ESD), the Public Information Office (PIO), deputy fire chiefs, assistant fire chiefs and division managers or their designees (e.g., community service liaisons), as well as the Fire Chief.

Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

Speech: The intentional or unintentional expression or communication of thoughts or opinions in spoken words, writing, expressive content, symbolism, photographs, digital video/audio, or related forms of communication.