CSID-OPERATED SOCIAL MEDIA POLICY

I. PURPOSE

The Coral Springs Improvement District (CSID) recognizes the need and value of the use of social media to enhance public communication, collaboration and information exchange. Social media is used to further CSID's strategic goals, promote its values and provide customer service.

To ensure the proper use of CSID's social networking sites and to enhance communication, streamline processes and foster productivity, this policy establishes CSID's position on the use and management of social media and provides guidance on its management, administration and oversight.

This policy provides rules and guidelines regarding the use of CSID-operated social media accounts and shall not be construed or interpreted in any way to infringe upon a person's right to free speech under the Florida or United States Constitution.

II. DEFINITIONS

Social Media, as defined by the U.S. government, is the various activities that integrate technology, social interaction, and content creation. Through social media, individuals or groups can create, organize, edit or comment, combine and share content. Social media uses many technologies and forms, including social-networking, blogs, wikis, photo–sharing, video–sharing, podcast, social bookmarking, mashups, widgets, virtual worlds, microblogs, Really Simple Syndication (RSS) and more.

Social Networks use online technology to communicate, share information and encourage user engagement. Social media platforms have been identified as "limited public forums" where speech by "certain group(s)" or "discussion of certain subject(s)" is held.

Social Media Account means any registration, login credential, tool, forum, platform, website or network that is created or maintained by a department or contracted service for the purpose of establishing or perpetuating a social media presence. Not all forms of social media may be appropriate for use by CSID departments, contracted services or programs and all accounts must obtain Director of Operations' approval.

Social Media Content includes any materials, documents, photographs, videos, graphics and other information that is created, posted, distributed or transmitted using social media internet sites or social media tools.

Post is considered speech whether in a written message, picture, graphic, advertisement, notification, feed, stream, transmission, broadcast, podcast, video, instant message, text message, blog, microblog, status update, wall post, comment, and any and all other forms, means or attempts at collaboration or communication that is uploaded, posted to, or otherwise displayed on or transmitted by, any social media account or network.

Profile is the identification of the agency or person that manages or operates a social media account.

Hashtags (#) are words or phrases used within a message to identify a keyword or topic of interest and facilitate a search for it. Hashtags are preceded by the pound sign (#) and can be a word or a short phrase.

Tag or Tagging someone or some business or organization means a link is created to that person's or organization's profile. The person/organization that is tagged in a post will be notified and the post may be added to the person's/organization's timeline or newsfeed.

III. SCOPE

The scope of this policy includes the use of social media platforms operated by CSID as a communication platform and the acceptable use of social media by authorized employees or contractors of CSID when conducting CSID business.

IV. ROLES & RESPONSIBILITIES

A. Roles

Authorized social media users include CSID personnel responsible for the use, administration, management, monitoring and/or retention of social media, social media tools or websites and/or social media content in the name of, or on behalf, of CSID. These administrators include the Director of Operations and their designee(s).

B. Responsibility of Administrator

1. The primary social media point of contact for CSID and accountable for the effective oversight, coordination and management of information for assigned social media.

2. Control access and maintain security for the account (secure password maintenance and deactivate account access due to change in staffing).

3. Assign and regulate access to pages for other assigned administrators and editors; limit social media account access to those with a clear business purpose, including,

but not limited to, those authorized to post content on CSID social media accounts on behalf of CSID.

4. Ensure that a Social Media Strategy Plan is submitted before any new account for a department, program, service or individual is considered for the Director of Operations' approval. Respond to all inquiries related to such requests for new social media accounts or current social media accounts.

5. Manage social media, such as adding content and responding to inquiries within 24 hours during normal business hours. Informing the Director of Operations of concerns when appropriate.

6. Review account activity daily during normal business hours for exploitation or misuse.

7. Consolidate or delete social media accounts that are inactive or infrequently updated.

8. Monitor and measure social media, analyzing effectiveness and facilitating continuous improvements.

9. Attend available training and/or meetings regarding government social media.

10. Employ best practices for social media use for government.

11. Collaborate with records management to ensure that CSID is adhering to all applicable federal, state, county and city laws and regulations.

V. POLICY

A. General

1. All social media is considered an extension of CSID's information networks and shall comply with all CSID-related policies.

2. All use of social media shall comply with all applicable federal, state, and county laws, regulations and policies. This includes adherence to established laws and policies regarding copyright, records retention, Freedom of Information Act (FOIA), Florida Sunshine, First Amendment, Americans with Disabilities Act (ADA), Health Insurance Portability and Accountability Act (HIPAA), privacy laws, and others as they apply to digital media. This also includes CSID design and branding standards;

policies relating to Information Technology and other relevant policies established by CSID; and norms of professional business communication.

3. All use of social media shall directly support CSID's strategic goals.

4. Any individual with access to CSID's social media accounts shall:

    a. Not use social media account for personal use, to promote or reply to personal contacts or to provide personal information or opinions.

    b. Keep all communication on social media professional and follow established policies regarding workplace professionalism.

    c. Not place any CSID technology at risk due to use of social media.

    d. Individuals with access to CSID's social media accounts do not have an expectation of privacy regarding their use of CSID social media.

B. Use

1. The Director of Operations will administer CSID's official social media accounts. CSID's official social media accounts will be used for purposes of connecting, engaging and informing the community in an effort to raise awareness of policy information, CSID business, accomplishments, events, programs, services, news and updates, conduct community outreach and engagement, and disseminate time-sensitive and emergency alerts.

2. CSID's official social media pages will not be used as a political, charitable, religious or fundraising platform including, campaigns and fundraising for election to public or private office or public or private ballot issues; general advertising/promotion of third-party businesses; or for lobbying. Pages are not to be used by the public to report criminal activity or emergencies.

3. As a limited public forum, speech and opinions expressed on CSID's social media platforms will be monitored during business hours and CSID will only participate in conversations as appropriate. Hiding and deleting posts may violate rights to free speech. Any post edited, hidden, removed or otherwise moderated will be treated as a public record. Removal of content will cite the violation of policy or standard in writing and be logged.

C. Content

1. *Official CSID Posts / Content Made by Authorized Users*
   These accounts will be used to post general information to increase public awareness of CSID's policies, programs, services, news/updates, and the like, as well as serve as an immediate form of communication in emergency situations. All material posted shall be consistent with CSID's mission, vision and values.

   a. Types of acceptable posts made by an official account of CSID, in a text, image or video format include, but are not limited to, information about a CSID-sponsored or endorsed program, service or event, policy decision/outcome, agenda summaries, general information or history about CSID, public safety prevention and information, and alerts and/or notifications made on behalf of CSID.

   b. Unacceptable content includes information on litigation or claims that could be brought against CSID; non-public information; personal, sensitive or confidential information of any kind; and medical information that violates a persons' Health Insurance Portability and Accountability Act (HIPAA) protections.

   c. Display CSID branding to include official CSID logo/seal on the account.

   d. Display official website and an official email account in the contact information.

   e. Comply with accessibility requirements.

   f. Content should be strategically crafted and mindful of those with mobile devices.

   g. Enhance the image of CSID, while being professional and user-friendly.

2. *Comments and Responses*

   a. Comments and replies on CSID's posts from the public are allowed and will be monitored by the aforementioned administrator or their designee for unacceptable content including defaming, harassing, threatening or otherwise violating the legal rights of others, including their privacy; misrepresenting one's person, background or character; posting any defamatory, infringing, obscene, false or unlawful material; selling, advertising or exchanging any goods or services unless expressly allowed; statement / threats or calls for violence or attacks of sexual assault or sexual exploitation, including derogatory terms related to sexual activity; calling for

self-injury suicide or harm of a specific person or group of people; posting any copyrighted material; and/or spam or bot-generated content; and those listed in Section V, C4.

b. Responses from CSID to comments/replies from the public will be warranted and provided when a specific question is asked about a CSID-related policy, program, service or event and there is specific response, or respond to correct an inaccuracy in a discussion and there is misinformation about a CSID policy, program, service or event.

c. CSID reserves the right to hide a comment or content in violation of unacceptable practices without prior notification (see also Section VIII, A).

3. *Sharing, Liking and Following*

a. CSID reserves the right to like, share, retweet or re-post content from another social media account. A like, share or re-tweet of content does not imply or denote an endorsement of that account or content.

b. CSID social media accounts may like or follow official public local, county, state and federal government agencies and/or businesses or non-profit agencies contracted to do business on behalf of and in conjunction with CSID, or as approved by the Director of Operations.

4. *Disclaimer of Guidelines*

CSID social media accounts, where possible, as well as CSID's website, will have the following disclaimer of guidelines posted or provide a link to them:

Comments expressed on this page do not necessarily reflect the opinions and position of CSID, its Board of Supervisors, administration, officers, employees or contractors.

CSID's use of social media is intended to be used for informational purposes only. If you wish to contact CSID or to request CSID's services, please visit CSID's official website at CSIDfl.org.

Under Florida law, this is a public record. If you do not want your name, profile, comment and/or post released in response to a public-records request, do not post to this page.

CSID's accounts are maintained and moderated by the Director of Operations or designee(s) during normal business hours to ensure that posted comments are constructive and suitable for all readers while respecting a range of opinions and points of view.

Anyone posting comments contrary to the platform's Terms of Use may be prohibited from future participation. By participating, users agree to send and receive messages that are both proper and related to the posting, discussion or forum topic.

The following actions are unacceptable practices: defaming, harassing, threatening, or otherwise violating the legal rights of others, including their privacy; misrepresenting one's person, background, or character; posting any defamatory, infringing, obscene, false, or unlawful material; selling, advertising, or exchanging any goods or services unless expressly allowed; statements / threats or calls for violence or attacks of sexual assault or sexual exploitation, including derogatory terms related to sexual activity; calling for self-injury or suicide of a specific person or group of people; posting any copyrighted material; and/or spam or bot-generated content.

CSID does not endorse any content, viewpoint, product or service linked from its social media sites and shall not be held liable for any losses caused by reliance on the accuracy, reliability or timeliness of shared information. CSID reserves the right to hide a comment or content in violation of unacceptable practices without prior notification.

5. *Security*

    a. Authorized users should employ strong passwords that cannot be easily compromised.

    b. Account passwords should periodically change and, in the event of a change, should be communicated with the other authorized users of the account.

    c. Authorized users of accounts should not share access with anyone other than an authorized user.

    d. Third-party applications may be used if it serves an appropriate and valid business purpose, adds to the user experience and originates from a trusted source. A third-party application may be removed at any time if CSID

determines it causes or potentially contributes to a security breach, the spread of viruses or is otherwise deemed inappropriate.

D. Employee Guidance for Participating in Social Networking

CSID understands that social networking and internet services have become a common form of communication in the workplace and among stakeholders and citizens. Employees who choose to participate in social networks are doing so voluntarily and as a CSID employee should adhere to current employee policies including:

- Employee Handbook
- Human Resources
- Information Technology

VI. EMERGENCIES AND EMERGING INCIDENTS

During emergencies or emerging incidents, all social media content and posting must be coordinated with the Director of Operations as part of its emergency support function. Pre-scheduled social media content should be unscheduled or removed. Depending on the incident, the Director of Operations or their designee(s) may be directed to point to specific social media accounts that will serve as the main source(s) of information. As incidents evolve over time, CSID may need to change how social media assets are used from strategic to tactical perspectives. Close coordination for all communications, including social media, is required.

VII. PROCEDURE

Account Establishment, Management and Administration

A. Establishment of an Additional Account on an Existing Social Media Platform

1. With the Director of Operations' approval, they or their designee(s) can create additional account(s) and/or merge or delete existing social media platform currently utilized by CSID, as deemed necessary.

B. Establishment of a Social Media Account on a New Platform

1. Each year, the Director of Operations and authorized users will review its social media needs. The Director of Operations and authorized users will determine if and when the addition or deletion of a social media platform is necessary based on

perceived potential value, function, opportunity and relation to the communication strategy and approved by CSID.

2. Only a CSID (CSIDfl.org) email address will be associated with the account and profile.

C. Profile

1. Where possible, the social media account profile should include a hyperlink back to www.CSIDfl.org for the purpose of providing additional information, resources, documents and other information pertaining to CSID to the public.

2. Where possible, the profile should clearly indicate that all posts are subject to public records laws.

3. Where possible, the profile should also include the disclaimer language listed previously in Section V, C4.

D. Required Training

Upon creation of a newly created social media account, the Director of Operations or designee(s) will provide training, if requested, to the new user(s) on how to access the account, best practices for use and suggested "dos and don'ts."

VIII. PUBLIC RECORDS AND ARCHIVING

A. Preservation of Social Media Records

When CSID uses social media to conduct CSID business, it must preserve social media public records, as it would any other public record. This includes preserving posts and comments made by the public on official posts.

1. Comments deemed inappropriate may be hidden, but not deleted, and only when in violation of social media conduct guidelines. See Section V. C2c.

2. Archive/maintain social media content (e.g., comments, posts, images and videos) in compliance with Florida's Public Records and Sunshine laws and applicable CSID policies.

3. Accounts that are archived.

a. All official CSID social media accounts are archived. Future accounts may be added at any time.

b. Social media accounts are, by definition, searchable history feeds, but archiving is necessary to maintain records of removed content, edited content and direct messages.

4. Accounts that are not archived:

   a. Campaign accounts of those running for office or campaign account(s) of incumbents.

   b. Personal accounts of elected officials, employees, contractors and officers.

   c. Public pages and profiles that are followed or linked by official CSID accounts.

5. Requests for public records related to content on CSID's social media accounts shall be made to Inframark:
Sandra Demarco
210 N. University Drive, Suite 702 Coral Springs, FL 33071
(O) 954.603.0033, Ext. 40532
Email: Sandra.demarco@inframark.com

IX. SECURITY OF SOCIAL NETWORK

The following strategies can minimize the risk of a hacker breaking into a site.

A. Protection Strategies
   1. Follow CSID's IT password guidelines when setting passwords for social media platforms.
   2. Never leave computer unattended or unlocked when logged on to a social media account.
   3. Only the Director of Operations, or designee(s), and moderator should know login and password to social media account(s).
   4. At least two people should have the password.
   5. If users/moderator(s) change, login and password should also change.

Even with these measures, sites are not immune from attacks by tenacious criminals. One sign of intrusion is defacement, in which your web page is replaced with the attacker's

message. Another indicator might be complaints of emails containing a virus or a fraudulent message coming from a CSID social media account.

B. Network Attack Protocol - If security of account has been compromised:
   1. Call IT Help Desk as soon as you notice a problem.
   2. Change login and password information immediately.
   3. Acknowledge security breach to social media followers. The Director of Operations and/or designee can help you develop a communications strategy.
   4. Look for signs of damage, make necessary corrections.
   5. Report incident to the Director of Operations and IT Security Officer.