

## 61.99.99.C0.04 Social Media Guidelines

Revised: May 11, 2020

Next Scheduled Review: May 11, 2025

[Revision History](#)



---

### Procedure Summary

---

The Division of Marketing and Communications (MARCOM) at Texas A&M University-Corpus Christi (TAMU-CC) is responsible for coordinating a consistent brand identity and overall management of university marketing and communication. MARCOM maintains the university's official social media accounts. As social media plays an increasingly larger role in the university's image to the public, social media sites created in affiliation with the university shall adhere to the standards outlined in this procedure in order to protect the university's reputation and brand.

---

### Procedure

---

1. General
  - 1.1. Social media is media based on the use of web and mobile technologies that allow for user-generated exchanges of information. With proper administration, social media can foster collaboration and communication as an interactive dialogue, enhancing the value of conversations across a global audience.
  - 1.2. Social media includes but is not limited to social networking sites, collaborative projects such as wikis, blogs and micro-blogs, content communities and virtual communities. Some commonly used social media platforms include: Facebook, Twitter, YouTube, TikTok, Flickr, SnapChat, LinkedIn, WordPress, and Tumblr.
  - 1.3. University social media accounts are separated into two (2) categories: official accounts (accounts for the university as a whole or an official division, department, departmental organization, or program) and affiliated accounts (accounts for student non-departmental organizations and university contracted vendors).
2. Responsibilities
  - 2.1. All units shall engage MARCOM when creating a new official social media account. Additionally, all official social media accounts must register with MARCOM.

- 2.2. MARCOM or a designee shall be granted the ability to login and make modifications to all official social media accounts.
  - 2.3. All official social media accounts must be monitored and updated on a weekly basis. Official social media accounts shall adhere to the best practices updated annually by MARCOM. Official social media accounts that are not updated regularly or do not adhere to best practices may be requested to be shut down. Affiliated social media accounts also should be monitored regularly and adhere to best practices.
  - 2.4. Upon notification from MARCOM units must bring the official social media account into compliance within five (5) days. Any expense shall be the responsibility of the unit. Social media communications that remain non-compliant shall be suspended immediately. Affiliate social media accounts not designated as official may not use the university's official marks or logos on their accounts.
3. Design and Style Guidelines
    - 3.1. Social media accounts must adhere to the university's design and style guides.
    - 3.2. Social media accounts must adhere to the copyright and intellectual property rights of others and of the university.
    - 3.3. Units must make reasonable efforts to ensure social media posts are accessible and usable by people with the widest range of capabilities possible. While some social media platforms have accommodations built in (e.g. closed captioning in YouTube; alternative text for images in Facebook, Instagram, and Twitter), others may require alternative methods of accommodation (e.g. providing links to transcripts, providing image descriptions within text). Guidelines and contact information on who can assist in making social media posts accessible will be provided on the Information Technology website.
4. Conduct and Ethics Guidelines
    - 4.1. It is imperative that all social media accounts maintain the same standards of conduct expected of all faculty and staff. Site content must be respectful, positive, helpful, and informative. Conversations on social media should enhance civic discussion. Profanity and language that is discriminatory must be removed from the site immediately.
    - 4.2. Units must protect confidential and proprietary information on their social media accounts. Units must not post any private, restricted, or sensitive information about the university and/or its students, staff, faculty, or alumni on their social media accounts. Types of private information include FERPA-protected student information, Social Security numbers, credit card numbers, and medical records.

- 4.3. Units must ensure the security of their social media accounts. A compromised account can lead to malicious entities posting inappropriate or even illegal material on the unit's behalf. This could lead to reputational risk to the university.
  - 4.4. Units must obey the terms of service of any social media platform employed.
  - 4.5. Units must adhere to guidelines set out by the Texas Department of Information Resources and the Texas A&M University System.
- 

## **Related Statutes, Policies, or Requirements**

---

[Texas Department of Information Resources Social Media Resource Guide](#)

University Rule [29.01.99.C1, Security of Electronic Information Resources](#)

University Procedure [09.02.99.C0.01, University Name and Indicia Usage](#)

University Procedure [09.02.99.C0.02, Branded Items](#)

University Procedure [29.01.04.C0.01, Electronic and Information Resources Accessibility](#)

University Procedure [61.99.99.C0.01, University Information](#)

University Procedure [61.99.99.C0.05, Marketing and External Communications](#)

---

## **Contact Office**

---

Contact for clarification and interpretation: Director of Web Services  
(361) 825-2419