



Social Media Used to Disseminate University Content Policy #1705.027

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 19, 2025	December 19, 2025	Marketing and Strategic Communications

POLICY STATEMENT

All FIU social media accounts created to disseminate University content must be approved by and registered with the Division of Marketing and Strategic Communications (MarComm). Unapproved accounts will be deemed unauthorized and must be closed or will be reported to the social media provider as unauthorized. Unauthorized accounts will be subject to the Use of Social Media for Non-University Purposes Policy#1710.026.

All social media accounts must be registered with a departmental shared cellular phone for 2-Factor authentication and business continuity, ensuring account access when employees transition. The departmental shared phone is not required for posting or management of the account and can be used by a team or multiple individuals.

All social media accounts created to disseminate university content must be registered using an official FIU employee email address. Student employees must use their student employee email. Personal or non-university email addresses should not be used. When an employee separates from the university, ownership and administrative access to all social media accounts created to disseminate university content must be transferred to the employee’s supervisor or designated departmental representative prior to departure.

All social media accounts must use platform-supported two-factor authentication, and a department-issued shared mobile phone must be associated with the account for continuity and access recovery purposes.

SCOPE

This policy applies to all employees who use social media to disseminate FIU university content. This includes, but is not limited to, faculty, staff, students employed by the university,



third-party vendors, volunteers, and appointees. It also extends to all FIU colleges, schools, departments, auxiliaries, research programs, teams, events, and governing bodies.

For third-party vendors, contractors, or partners engaged to manage or support university social media activities, the responsibility for ensuring compliance with this policy rests with the FIU employee or entity that hires and manages the vendor. The hiring unit or employee is accountable for oversight, compliance, and enforcement when third parties are acting on behalf of the university.

REASON FOR POLICY

The purpose of this policy is to govern the creation, registration, and management of all FIU social media accounts established to disseminate university content. This ensures that university-affiliated accounts are managed professionally, remain secure, and are maintained under the oversight of FIU employees. By requiring registration with Marketing and Strategic Communications (MarComm), the use of official FIU email addresses, and departmental shared phones for authentication, the university safeguards account continuity, preserves institutional integrity, and ensures that ownership and access remain with FIU during employee transitions or turnover.

The use of social media to disseminate university content on behalf of the University is subject to state and federal law and regulations as well as all University policies and procedures. By posting on or with FIU social media sites, users agree to follow the terms of use of the site, Florida, and federal laws, and FIU regulations and policies.

DEFINITIONS

TERM	DEFINITIONS
Social Media	Social media are computer-mediated technologies that allow the creating and sharing of information and ideas via virtual communities and networks.
Unit level Designee	Specifically identified and registered communicators tasked with running official FIU social media accounts.
Emergency	A serious, unexpected, and/or threatening situation as deemed by FIU’s Department of Emergency Management and/or FIU Police requiring immediate action.



Departmental shared cellular phone	A department-issued mobile phone that is officially requested with the university using the cell phone allowance and purchased request form (section 3 found in the Procedures) and linked to the social media account for business continuity, two-factor authentication, and access recovery. The registered phone is not required to actively manage the account but must remain in the department’s possession and accessible to authorized staff at all times.
Unit	Refers to a college, division, department or office at the university.
MarComm	The Division of Marketing and Strategic Communications.

ROLES AND RESPONSIBILITIES

The Division of Marketing and Strategic Communications (MarComm) is charged with increasing public awareness of FIU through effective marketing and communication strategies that enhance the university’s image and present a consistent, unified message. Given this mission, MarComm has the authority to regulate the use of social media to disseminate university content.

During any emergency, MarComm will take the lead for all communication via social media in coordination with the Department of Emergency Management Services and FIU Police Department. All accounts must defer the posting of information to the unit handling the incident unless otherwise approved by MarComm.

RELATED RESOURCES

New Account Request
Go.fiu.edu/socialrequest

Registering Existing Accounts
Go.fiu.edu/socialform

Brand Standards and Social Guidelines
brand.fiu.edu

Use of Social Media for Non-University Purposes #1705.026



CONTACTS

Division of Marketing and Strategic Communications
Florida International University
11200 S.W. 8th Street - PC 519
Miami, Florida 33199
Telephone: (305) 348-7235

HISTORY

Initial Effective Date: December 19, 2025

Review Dates (*review performed, no updates*): n/a

Revision Dates (*updates made to document*): December 19, 2025



**Social Media Used to Disseminate University Content Policy
#1705.027a**

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 19, 2025	December 19, 2025	Marketing and Strategic Communications

PROCEDURE STATEMENT

1. Account Creation and Approval (New Accounts)

- All new social media accounts created to disseminate FIU content must be approved in advance in writing by Marketing and Strategic Communications (MarComm).
- Units or employees seeking to establish a new account must submit the **Social Media Account Request Form** at go.fiu.edu/socialrequest.
- Unauthorized accounts created without MarComm approval will be reported to the platform provider and/or will be asked to be closed.

2. Account Registration and Review (Existing Accounts)

- As of the effective date of this policy, all existing social media accounts created to disseminate FIU content must be registered using the **Social Media Account Registration Form** at go.fiu.edu/socialform.
- Existing accounts will undergo a review process to ensure compliance with university standards, branding, accessibility, and security requirements.
- Accounts that fail to register or do not meet requirements may be reported as unauthorized and reported to the platform provider and/or will be asked to be closed.

3. Account Registration Standards

- All social media accounts must be registered using an official FIU employee email address.
- Student employees must use their official student employee email.
- Personal or non-FIU email addresses are not permitted for account registration or

management.

4. Authentication and Security

- All FIU social media accounts must use two-factor authentication.
- The mobile number associated with authentication must be a departmental shared cellular phone, issued for business continuity.
- The departmental shared phone is required for authentication purposes but is not required for posting or content management.
- Each Unit and Designee must securely store the usernames and passwords for their social media accounts in a safe and reliable location. Access should be limited to authorized personnel only, ensuring the security and confidentiality of account credentials.
- Unit level Designees shall provide all contact information for the person posting and the supervisor approving of their designated account(s) to MarComm. MarComm may ask the Designee to suspend or terminate such accounts at any time for improper use.

5. Continuity and Oversight

- The departmental shared phone ensures secure account access during employee transitions or turnover.
- The FIU employee or entity that hires or manages third-party vendors is responsible for ensuring those vendors comply with this policy.
- Ultimate oversight and enforcement authority rests with Marketing and Strategic Communications (MarComm).
- MarComm reserves the right to conduct periodic reviews of all registered social media accounts created to disseminate university content to ensure information accuracy, compliance, and alignment with university standards. Units must promptly remove or update any outdated, inaccurate, or non-compliant content as directed by MarComm.

Departments that use social media are responsible for complying with applicable federal, state, and county laws, regulations, and University policies. This includes adherence to laws and policies regarding copyright, use of photographs, records retention, personnel privacy, public records, First Amendment, FERPA (Family Educational Rights Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), the Americans with Disabilities Act (Facebook and Twitter have ADA settings), and information security policies established by MarComm.