UNIVERSITY OF CENTRAL FLORIDA	**IST, School of Modeling, Simulation & Training** **Controlling information posted or provided to publicly accessible information systems**		Policy Number: **IST-SMST-002**
Status: **Final**	Effective Date: **6/8/2020**	Revised Date:	Pages: **3**

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all IST, School of Modeling, Simulation, & Training (IST-SMST) students and employees who manage and maintain an IST-SMST publicly accessible information system or who post content to a publicly accessible system managed elsewhere. Improper use of the organization's proprietary information or information the organization is required to protect can damage the organization or other partnering agencies and sponsors. Everyone plays a role to ensure nonpublic information is not posted or processed on publicly accessible information systems.

POLICY STATEMENT:

In accordance with UCF Public Information and Media Relations, 6-002.1, the university's division of Communications & Marketing is responsible for disseminating information involving institutional policy or university-wide practice, or information that could impact the university's reputation. Any other information is at the discretion of the faculty research, department, or college to share, with exception to any information identified in the UCF Data Classification and Protection Policy, 4-008.1 as restricted or highly restricted, which includes information protected by contract.

To uphold university policies, federal laws, regulations and sponsored agreements governing the safeguarding of nonpublic information, the posting of nonpublic information on a publicly accessible information system or providing of nonpublic information to a publicly accessible system for processing, whether managed by IST-SMST or not (e.g., forums, LinkedIn, Facebook, Twitter) is strictly prohibited.

For publicly accessible sites managed by IST-SMST, the corresponding director, department/lab head or project lead (principal investigator), is responsible for:

a. Designating individuals authorized to post information onto the publicly accessible system;

b. Verifying authorized individuals complete training on how to ensure the publicly accessible system does not contain nonpublic information;

c. Ensuring a review is conducted of proposed content prior to posting onto the publicly accessible system to affirm nonpublic information is not included; and

d. Performing a review of the content on the publicly accessible system, minimally once a year, for nonpublic information, and remove such information, if discovered.

DEFINITIONS:

Nonpublic information. Any information that is strictly controlled, regulated, and/or protected by law, regulation, contract, or university policy is nonpublic information. Examples of nonpublic information:

- **Highly Restricted and Restricted Data.** See UCF Data Classification and Protection Policy, 4-008.1 which outlines information such as government identification numbers (SSN, driver's license, passport number, etc), privacy of student academic records (FERPA), Personal Identifiable Information (PII), individually-identifiable health information (HIPAA), business-sensitive information, proprietary intellectual property and other information protected by contract or federal or state law, rule, or regulation.

- **Federal Contract Information (FCI).** As outlined under 48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems, is information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but does not include information provided by the Government to the public (such as on public Web sites) or simple transactional information. Federal Contract Information for defense agencies, may include Covered Defense Information (CDI). CDI can be referred to as Controlled Technical Information (CTI) or Controlled Unclassified Information (CUI).

- **Controlled Technical Information (CTI).** CTI is information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. CTI is also a type of Controlled Unclassified Information.

- **Controlled Unclassified Information (CUI).** CUI is information that does not meet the threshold for classified data but does require safeguards from unauthorized access and release. Federal information systems, or information systems operated on behalf of a federal agency (per contractual requirement), must meet the safeguarding requirements detailed in NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, while non-federal information systems must meet the requirements of NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The different types of CUI are reflected in the National Archives and Records Administration (NARA) CUI rule (32 CFR 2002), and are maintained in the NARA CUI Registry. Examples of CUI range from data for critical infrastructure, export control, intelligence, law enforcement, privacy, and what defense agencies refer to as controlled technical information. Historically, documents from federal agencies may have been marked as 'For Official Use Only' or FOUO; or 'Sensitive, but Unclassified' or SBU. As revisions to older documents occur, the information is to be reviewed and markings for CUI (if applicable) are to be followed by all federal agencies. Until such time, documents previously marked confidential, FOUO, or SBU, while they may or may not be CUI, should still be considered nonpublic information.

Publicly accessible information system. An information system accessible to the public, typically without identification or authentication, such as a public facing website.

TECHNICAL IMPLEMENTATION:

By default, system administrators shall disable write and executable permissions for all users, within publicly accessible areas of an information system, except for those authorized to post.

PROCEDURE:

All personnel are to assess the contents of the information they are about to enter or provide to a publicly accessible site does not contain nonpublic information of the organization.

It is the responsibility of each corresponding director, department/lab head or project lead (principal investigator), to ensure internal procedures to achieve this policy are established for the publicly accessible system they manage. Procedures must minimally address:

- Maintaining a list of individuals authorized to post and reviewing the list with the respective system administrator of the publicly accessible site as personnel responsibilities or transfers occur.
- Ensuring training is performed and logged for individuals authorized to post.
- A process to review all content for nonpublic information prior to posting.
- Conducting and tracking when a full content review of the site has been conducted, which must minimally be performed annually, to ensure nonpublic information is not contained in the site; removing any nonpublic information upon discovery, and notifying IT Compliance and the information security office if data classified as highly restricted or restricted is, or is suspected to have been, lost or disclosed to unauthorized parties.

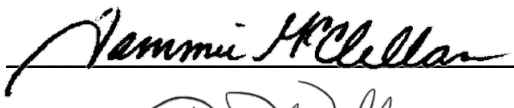
IT Compliance can facilitate enrollment in appropriate training modules for individuals authorized to post information to a publicly accessible system.

REFERENCES:

- UCF Use of Information Technologies and Resources, 4-002.2
- UCF Data Classification and Protection Policy, 4-008.1
- UCF Public Information and Media Relations, 6-002.1
- CMMC AC.1.004, SC.3.193
- FAR Clause 52.204-21 b.1.iv
- NIST SP 800-171 Rev 2 3.1.22
- NIST SP 800-53 Rev 4 AC-22

POLICY APPROVAL

Policy Number: IST-SMST-002

Initiated by:  **Date:** 05/28/2020

Director or Designee:  **Date:** 06/08/2020