UCF UNIVERSITY OF CENTRAL FLORIDA	**IST, School of Modeling, Simulation & Training** **Media Protection: Use, physical security, and disposal**		Policy Number: **IST-SMST-004**
Status: **Final**	Effective Date: **9/03/2020**	Revised Date:	Pages: **4**

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all IST, School of Modeling, Simulation, & Training (IST-SMST) students, employees and guests who use IST-SMST information in digital and non-digital form.

POLICY STATEMENT:

Safeguarding media is essential to preventing the theft of or unauthorized disclosure of information. It is the responsibility of everyone who handles information in its various forms and types to protect it.

Use.

- All workstations are to be locked when unattended and not actively in use.
- Collaborative computing devices must be configured to prevent remote activation and to provide notification when in use. Systems that cannot be configured this way, must disconnect, or disable such devices when not in use or seek an exception, with alternative, but similar mitigation procedures documented and approved by management and assessment by IT Compliance. This does not apply to dedicated video conferencing systems.
- Only authorized and organizationally managed information systems and removable media devices may be used to store, process, or transmit controlled unclassified information (CUI). Use of personal devices is prohibited to store, process, or transmit controlled unclassified information. Use of partnering agency systems are not authorized to store, process, or transmit IST-SMST received or produced CUI or connect to controlled IST-SMST systems without management approval and assessment by IT Compliance or partnering agency attestation.
- Highly restricted data must be encrypted when stored, processed and transmitted within systems and during transport, unless protected by an alternative physical barrier. Only approved Federal Information Processing Standard (FIPS) encryption methods may be used for controlled unclassified information (CUI).
- A chain of custody will be maintained for any media transported outside a controlled system.

Physical Security.

- Controlled unclassified information must be handled in a controlled environment or manner to prevent or detect the unauthorized access to, observation of, or overhearing discussions of CUI.
- Facility Coordinator(s) will ensure building security and areas designated as "restricted access" have the necessary physical barrier protections (e.g., locks, cameras, card readers, etc) to restrict access to only authorized individuals and will:
    - Maintain and operate equipment according to manufacturer recommended settings.
    - Review physical protections annually for continued suitability for physical protections.
    - Maintain inventory of and secure any keys, combinations, or other physical access devices.
    - Minimally review key and card access to restricted spaces once a year and re-evaluate continued requirement for access to spaces aside from direct office/lab of the employee.
    - Terminate card access, retrieve keys, or change locks when keys are lost, the combination is compromised, or individuals are transferred or terminated.

- When outside of a controlled environment, controlled unclassified information must be kept under direct control of the employee or protected by at least one physical barrier.
- The same requirements for work conducted on-premise in an employee's primary work location, applies to any alternate work site used to store, process or transmit controlled unclassified information, although different methods may be used to meet the requirements at the alternate site.

Disposal.
Prior to disposing, transferring or reusing media outside of IST-SMST, all systems (e.g., servers, workstations, copiers, printers, scanners), removable media, and paper must be erased or destroyed in accordance with university and IST-SMST media sanitization standards.

DEFINITIONS:

Chain of Custody. A chronological trail of when, how, and who transported and received media (digital and non-digital).

Collaborative computing devices. Such devices as networked white boards, cameras, and microphones must be configured to prevent remote activation. If this cannot be achieved through operating system settings, devices must be disconnected when not in use. When in use, notification is required, such as by an indicator light or text window that appears on screen or through manual means such as a posted sign.

Controlled environment. A controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) to protect CUI from unauthorized access or disclosure.

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.

Federal Information Processing Standards (FIPS) Encryption methods. An established set of standards, published by the National Institute of Standards and Technology (NIST), for the cryptographic modules which govern the processing and encryption algorithms used to safeguard information in accordance with the Federal Information Security Modernization Act and subsequent federal regulations requiring approved FIPS encryption to protect information from unauthorized access and release. The current standard is known as FIPS 140-2. FIPS approved encryption methods have been tested and validated through the NIST Cryptographic Algorithm Validation Program (CAVP) and are on the validation list maintained by the program.

Physical barrier. Sealed envelope, area equipped with electronic locks, or locked: Door, Overhead bin, Drawer, File cabinet

Removable media. Includes any portable storage device or media that can be removed from a system while operating normally. Removable media provides an easy means to transport information and requires proper labeling, handling, and encryption requirements based on the classification of the data contained therein. Examples of removable media are:

- Floppy disks;
- Compact/digital video disks (CDs/DVDs);
- USB connectable small hard drive;
- USB Flash/thumb drives;
- Flash memory cards / drives that contain nonvolatile memory

PROCEDURES:

- System settings will be configured to prevent remote activation of collaborative computing devices, such as microphone and camera, and settings will be implemented to provide automatic notification when use occurs (namely Windows 10 domain connected systems). Where a system cannot be configured this way, users will:
  - Disconnect microphones or otherwise disable when not in use
  - Disconnect cameras when not in use or cover camera lens to prevent visual access and use
  - Post signs of microphone and camera use to inform users entering a space with such activity
- For controlled environments, such as spaces designated for data center, telecom, and network operations or as "restricted access", must:
  - Have signage indicating "Restricted Area – Authorized Personnel Only"
  - Limit physical access to only authorized individuals
  - Maintain audit logs of physical access
  - Escort visitors and monitor visitor activity (by review of visitor access log)
- For office and lab workstations handling controlled unclassified information, physical access must be limited to authorized organizational personnel (e.g., employees).
  - Offices with lockable doors should be locked when unattended.
  - Open areas to the public (e.g., no other physical barrier restriction that only allows authorized organization personnel), should employ other protections as appropriate for the equipment (e.g., equipment lock, keyboard lock).
- A visitor access log to a controlled environment is to include visitor name, organization, date/time of entry and departure, purpose, and name of the escort.
- Controlled information is not to be left unattended at a work area/desk; it must be securely stored.
- File cabinets containing controlled information are to be closed and locked when not in use or when unattended.
- All controlled information in hardcopy or electronic form must be properly marked at all times with a cover sheet, label, and/or applicable markings. See IST-SMST Media Marking Standard.
- Ensure keys used to access controlled/restricted information are not left at an unattended desk.
- Building/Room access card and Common Access Card must be under the control of the individual it was issued to at all times.
- Facilities Coordinator and supervisors shall annually review key and card access

- Output devices (e.g., monitors, printers, copiers, scanners) are to be placed in areas where their use does not expose controlled information to unauthorized individuals. Monitors should be turned to prevent unauthorized viewing and output of devices of controlled information must be under the direct control of the authorized data handler. Dedicated printers and scanners may be needed in some cases to prevent unauthorized access to controlled information.

REFERENCES:

- UCF Use of Information Technologies and Resources Policy, 4-002.2
- UCF Security of Mobile Computing, Data Storage, and Communication Devices, 4-007
- IST-SMST Media Sanitization Standard, IST-SMST-STD-002
- FAR Clause 52.204-21 b.1.iii and vii, viii, partial v.1.ix
- CMMC v1 AC.1.003, AC.2.016, MP.1.118, MA.3.115, MP.3.124, MP.3.125, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, PE.3.136, SC.2.178
- NIST SP 800-171 Rev 2 3.1.3, 3.1.20, 3.7.3, 3.8.3, 3.8.5, 3.8.6, 3.10.1, 3.10.2, 3.10.3, 3.10.4, 3.10.5, 3.10.6, 3.13.12
- NIST SP 800-53 Rev 4 AC-20, AC-20(1), AC-4, MP-6, MA-2, MP-5, MP-5(4), PE-2, PE-3, PE-6, PE-17, SC-15

POLICY APPROVAL

Policy Number: IST-SMST-004

Initiated by: Tammi McClellan **Date:** 09/03/2020

Director or Designee: **Date:** 09/03/2020