UNIVERSITY OF CENTRAL FLORIDA	**IST, School of Modeling, Simulation & Training** **Use of removable storage devices or media**		Policy Number: **IST-SMST-003**
Status: **Final**	Effective Date: **6/25/2020**	Revised Date:	Pages: **3**

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all IST, School of Modeling, Simulation, & Training (IST-SMST) students, employees and others who use IST-SMST information systems.

POLICY STATEMENT:

Use of removable media introduces security risks to the system(s) the media is used, and the potential for loss and unauthorized access to data. The purpose of this policy is to ensure the use of removable storage devices and media is managed in a manner that permits data to be available or transferred where it is required, while protecting the integrity and confidentiality of the data and systems the media is used.

Labeling.

- IST-SMST devices (systems and storage devices) and removable media produced by IST-SMST personnel will minimally be labeled with an identifiable owner (e.g., employee, lab, or project), in accordance with the IST-SMST Media Marking standard, as applicable to the size and type of media used or produced. If the media contents is highly restricted, the label or marking must reflect *both* an identifiable owner and 'CONTROLLED' or 'CUI', to reflect presence of such data.

Use of Removable Storage Devices or Media in any IST-SMST System.

- The use of removable media ***without*** an identifiable owner, unknown or trusted by the user, is prohibited in any IST-SMST managed system. Media or devices found without an identifiable owner are to be brought to the IST-SMST Help Desk for review in a secured, sandboxed system.

Use of Removable Storage Devices or Writing/Burning Media in IST-SMST Controlled Systems.

- Use of removable storage devices on controlled systems is prohibited without management approval. Technical controls require authorization of the serial number of the device.
    - USB Flash/thumb drives cannot be read or written to without approval.
    - CD/DVDs can be read, but not written to without approval.
- Approved removable storage devices must be organizationally controlled and labeled according to the data contained, authorized per system and user(s) permitted to access, and stated purpose.
- Highly restricted data stored on removable media must be encrypted (FIPS 140-2 if Controlled Unclassified Information) unless otherwise protected by alternative physical safeguards.
- Personnel responsible for an approved device or media containing highly restricted data, must follow proper handling, physical protections, and custody procedures in accordance with all IST-SMST and university policies and procedures.
- Approval to use a removable storage device or write/burn media in an IST-SMST controlled system does ***not*** authorize the device or media to also be used in an external system. Use of approved storage devices or media containing highly restricted data that will be taken and used in an external information system, requires additional management approval and documentation of the external system usage and/or who the media is being provided to.

DEFINITIONS:

Controlled system. System authorized to process, store, or transmit 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.

Highly Restricted Data. Refer to UCF Data Classification and Protection Policy, 4-008.1. This university data category includes any federal data identified as Controlled Unclassified Information (CUI), which may also be referred to as Covered Defense Information (CDI) or Controlled Technical Information (CTI). Highly Restricted Data is protected by law or policy and requires the highest level of access control and security protection, both in storage and in transit.

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

External information system. A system the organization generally has no direct supervision and authority over the application of security controls. Typically, this is a system outside of the IST-SMST network, such as other university systems, personal systems, or one located at a partner (subcontractor) or research sponsor location. An external system may also be managed by IST-SMST, but is one ***not*** authorized to process Controlled Unclassified Information and is therefore outside of the protection boundary.

TECHNICAL IMPLEMENTATION:

Any device without an identifiable owner brought to the Helpdesk to identify a potential owner, shall be reviewed in a secured, sandboxed environment, with an immediate scan for threats performed on the device. The device shall be labeled, if an identified owner is determined and returned to owner. If no identification is feasible, the device shall be held for a reasonable period to see if a request is made and if not, destroyed according to the media sanitization policy.

For all IST-SMST controlled systems, all portable storage device/USB ports and hardware devices used to burn/write data to removable media are to be disabled by default. Ports may be activated for specific devices following authorization of the device and user's system under management approval and IT Compliance review. The ability to use removable media in any form containing highly restricted data, requires the device/media to be encrypted. Only in rare circumstances will a controlled system be authorized to burn/write to unencrypted media.

PROCEDURES:

All users: Only use, insert, plug-in media with an identifiable owner you trust.

Users of controlled systems, if applicable:

- Device ports to write/burn removable media (ie, CD/DVD) or for portable storage devices are disabled by default. The ability to write/burn a CD/DVD or to use a specific USB device may be authorized per user, lab/department, or group of controlled systems upon management approval.
  - Complete the Request for Removable Media/Device Allowance and External System Use.
  - Users of the systems/devices noted within the request must sign and accept the responsibilities and procedures highlighted within the form.
  - Submit the completed request to the corresponding director, department/lab head, or project lead (principal investigator) for approval. Have the completed and approved form sent to IT Compliance for review and authorization of the specific systems and devices.
  - All users of an approved device or who produce media containing highly restricted data must complete Security Awareness training that includes proper handling for highly restricted data before final authorization.
  - Requests must be re-authorized bi-annually.

REFERENCES:

- UCF Security of Mobile Computing, Data Storage, and Communication Devices, policy 4-007
- UCF Data Classification and Protection Policy, 4-008.1
- Safeguarding Media Policy, IST-SMST-004
- CMMC v1 AC.2.006, MP.2.121, MP.3.122, MP.3.123, MP.3.125
- NIST SP 800-171 Rev 2 3.1.21, 3.8.4, 3.8.6, 3.8.7, 3.8.8
- NIST SP 800-53 Rev 4 AC-20(2), MP-3, MP-7(1)

POLICY APPROVAL

Policy Number: IST-SMST-003

Initiated by: Tammie McClellan **Date:** 06/12/2020

Director or Designee: ____________ **Date:** 06/26/2020