Category: Information Technology **Applicable for:** CEAS Faculty, Staff, Students, and Affiliates	**COLLEGE OF ENGINEERING AND APPLIED SCIENCE** **Operating Policy** Controlled Unclassified Information (CUI) Media Protection **Effective Date:** July 15, 2021	**Document Owner:** CEAS Sr. Associate Dean **Responsible Office:** CEAS Dean

Purpose

This policy is intended to promote compliance with NIST 800-171 security controls. The intent of the Controlled Unclassified Information (CUI) Media Protection Policy is to ensure the protection of CUI until such time as the information is either released to the public via authorized dissemination (e.g. published research), or is purged or destroyed in accordance with applicable record retention rules. This policy may augment, or increase the standards, but shall not detract from any other UC and/or CEAS Security Policy standards.

Scope

This policy applies to any electronic or physical media maintained and managed by CEAS faculty, staff, students and its affiliates, containing CUI while being generated, stored, accessed or physically moved from a secure location from CEAS. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CUI outside the college's assigned physically secured area must be monitored and controlled.

Authorized CEAS personnel shall protect and control electronic and physical CUI at all times while at rest and in transit. CEAS researchers and staff will take appropriate safeguards for protecting CUI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CUI disclosure and/or use must be reported to the CEAS IT support staff and also in accordance with UC policy 9.1.8 Information Security Incident Management and Response.

Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CUI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CUI.

To protect CUI, CEAS researchers and personnel shall:

1. Securely store electronic and physical media within a physically secured or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed or digital media from CEAS secured areas.

4. Not use personally owned information system to access, process, store, or transmit CUI.
5. Not utilize publicly accessible computers to access, process, store, or transmit CUI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
6. Store all hardcopy CUI printouts maintained by the CEAS researchers in a secure area accessible to only those employees whose job function requires them to handle such documents.
7. Safeguard all CUI against possible misuse by complying with UC Policy 9.1.1 Data Governance and Classification Minimal Safeguards: https://www.uc.edu/content/dam/uc/infosec/docs/policies/Data_Governance_and_Classification_Policy_9.1.1.B.pdf .
8. Take appropriate action when in possession of CUI while not in a secure area:
    a. CUI must not leave the employee's immediate control. CUI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CUI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock and /or privacy screens. CUI shall not be left in plain public view. When CUI is electronically transmitted outside the boundary of the physically secured location, the data shall be immediately protected using FIPS-validated encryption.
        i. When CUI is at rest (i.e. stored electronically) outside the boundary of the physically secured location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CUI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
        ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
9. Lock or log off computer when not in immediate vicinity of work area to protect CUI. Not all personnel have same CUI access permissions and need to keep CUI protected on a need-to-know basis.
10. Adhere a CUI label to all media containing CUI to identify the media as containing sensitive data.
11. Prior to using any media from an external source on a machine with CUI, scan the media on a separate device for potential vulnerabilities using approved anti-virus and malware detection software.
12. Not use portable storage devices when such devices have no identifiable owner.

Media Transport

Controls shall be in place to protect electronic and physical media containing CUI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use.

Dissemination to another organization is authorized if:

1. The other organization is an Authorized Recipient of such information and is being serviced by the accessing organization.

The CEAS personnel and researchers shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The CEAS personnel and researchers will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CUI.
3. Following the least privilege and role-based rules for allowing access. Limit access to CUI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
    a. Storing CUI in a locked briefcase or lockbox.
    b. Only viewing or accessing the CUI electronically or document printouts in a physically secured location by authorized personnel.
    c. For hard copy printouts or CUI documents:
        i. Package hard copy printouts in such a way as to not have any CUI information viewable.
        ii. That are mailed or shipped, must only be released to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CUI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.
5. Not taking CUI home or when traveling unless authorized.
6. Documenting transport activities in a log to maintain accountability of transporting CUI outside of controlled spaces.

Electronic Media Sanitization and Disposal

Physically protect CUI until media end of life. End of life CUI is destroyed or sanitized using approved equipment, techniques and procedures.

The CEAS personnel and researchers shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to the Electronic Media Sanitization Standard: https://www.uc.edu/content/dam/uc/infosec/docs/Standards/Electronic_Media_Sanitization_Standard.pdf

Breach Notification and Incident Reporting

The CEAS personnel and researchers shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems and media shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. For UC's incident response policy, refer to UC policy 9.1.8 Information Security Incident Management and Response: https://www.uc.edu/content/dam/uc/infosec/docs/policies/Information_Security_Incident_Management_and_Response_Policy_9.1.8.pdf

Related Document

NIST Computer Security Resource Center for 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Contacts

CEAS Office of College Computing – CEAS-USERHELP@listserv.uc.edu

IT@UC – (513) 556-4357, or https://ituc.service-now.com/sp