ASU Knowledge Enterprise Development ARIZONA STATE UNIVERSITY		**Page 1 of 2**
	PREPARED BY: Office of Research Compliance, Research Advancement Services, KE Research Technology Office	**EFFECTIVE DATE:** March 16,2026
DOCUMENT TITLE: CUI Handling Process		

Purpose:

This document outlines the standard process for managing Controlled Unclassified Information (CUI) in compliance with federal requirements.

Scope:

This document applies to all personnel involved in the handling, processing, or management of CUI within the context of research activities at Arizona State University

Definitions:

Authorized Personnel (CUI Handlers): Individuals who have been formally approved to access, handle, store, transmit, or dispose of Controlled Unclassified Information in connection with a sponsored project. Authorized Personnel must meet all applicable eligibility and dissemination requirements, complete required training, have a legitimate need to know, and comply with institutional policies, safeguarding standards, and sponsor-specific requirements governing CUI.

Controlled Defense Information (CDI): Refers to unclassified information that requires protection due to its relevance to military operations and defense-related activities. CDI is a subset of Controlled Unclassified Information (CUI) tied to defense contracts and activities. It includes CDI data such as technical drawings, software code, and specifications.

Controlled Technical Information (CTI): means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled Unclassified Information (CUI): is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI ASU Resource

Cybersecurity Maturity Model Certification (CMMC): which requires federal contractors to adhere to specific cybersecurity controls when working with Controlled Unclassified Information (CUI). CMMC ASU Resource

Export: A release of items (including technology and/or software) subject to export control regulations to a foreign national outside and inside the United States. A "deemed" export is an export within the US to the home country of the foreign national.

Foreign National: Any individual who is not a citizen of the country they are residing in. Refer to the specific federal sponsored project award terms for this definition.

Fundamental Research: means basic and applied research in science and engineering, where the resulting information is shared broadly within the scientific community.

HIPAA: for the Health Insurance Portability and Accountability Act of 1996, a U.S. federal law designed to protect sensitive patient health information from being disclosed without consent. It mandates security standards to guard electronic protected health information (ePHI) and privacy rules for medical records, applying to healthcare providers, insurers, and clearinghouses. HIPAA ASU Resource

Knowledge Enterprise Research Technology Office: is the institutional unit responsible for assessing, advising on, and supporting research cybersecurity and information technology requirements associated with sponsored projects. This office reviews contractual and proposal-level cybersecurity obligations (including those related to Controlled Unclassified Information (CUI)), evaluates institutional capabilities to meet those requirements, provides guidance on approved secure systems and tools, and supports budgeting and pricing related to cybersecurity compliance and staffing.

Office of Research Compliance: is the institutional authority responsible for ensuring compliance with applicable laws, regulations, and sponsor requirements governing research activities. This office provides oversight and guidance on export controls, foreign national participation, Controlled Unclassified Information (CUI), and other regulatory requirements. The Office of Research Compliance determines whether CUI is export-controlled, confirms dissemination and access restrictions, facilitates the development of Technology Control Plans (TCPs), and approves the handling, sharing, and safeguarding of regulated research information.

National Archives and Records Administration: is an independent agency of the U.S. government responsible for preserving, documenting, and managing the permanent, historically valuable records of the federal government. https://www.archives.gov/

NIST 800-171: is a National Institute of Standards and Technology publication that defines security requirements for protecting the confidentiality of CUI in non-federal systems.

Principal Investigator (PI): Is the lead researcher responsible for the overall management, conduct, and scientific direction of a sponsored research project. The PI assumes primary responsibility for project leadership, fiscal oversight, and ensuring compliance with university and sponsor policies and regulations.

Project Leadership: Include the Principal Investigator (PI), Co-Investigators, senior institutional leadership (as applicable), and project or program management personnel responsible for the overall direction, execution, and oversight of a sponsored project. Project Leadership is responsible for ensuring compliance with sponsor requirements, determining personnel access needs, implementing access controls and mitigation measures, coordinating with institutional compliance offices, and ensuring ongoing adherence to CUI, cybersecurity, export control, and dissemination requirements throughout the project lifecycle.

Recipient: Any individual, organization, or system that is authorized to receive, access, or handle CUI in order to perform official duties or a lawful government-related function.

Research Administrator: An individual who works with investigators to identify funding opportunities, develop proposals, and/or manage sponsored funds.

Sponsored Projects: refers to the institutional offices responsible for proposal submission, award negotiation and acceptance, and post-award administration of externally funded research and sponsored activities. These offices review proposals, awards, and related documents for terms, conditions, and compliance requirements, including those related to CUI, cybersecurity standards, and dissemination restrictions. Sponsored Projects coordinates with Project Leadership, Research Compliance, and Research Technology to ensure sponsor requirements are identified, communicated, and implemented.

Sponsors / Prime Awardees: External entities that issue solicitations, provide funding, or otherwise sponsor research or sponsored activities. This includes federal agencies, state or local governments, non-profit organizations, and private entities. Sponsors and Prime Awardees are responsible for identifying and marking CUI, specifying applicable CUI categories, dissemination controls, cybersecurity requirements, and any additional contractual or regulatory obligations associated with the award.

Subawardees: A third-party organization that receives funding support from ASU to collaborate in carrying out the performance of an externally sponsored project. The subrecipient plays an integral role in the project and is responsible for programmatic decision-making. Suitable means of verification Includes but is not limited to: first-hand observations of the work being performed, written confirmation from the individual, physically verifiable information, notebooks, and/or sign-in sheets.

Technology Control Plan: a formal compliance document used to manage and protect controlled technologies, data, or information that are subject to U.S. export control laws.

Third Parties: Any external individuals or organizations that are not part of the covered organization and are not employees or internal users, but who may access, receive, process, store, transmit, or support systems containing CUI.

Responsibilities:

Sponsored Projects / Research Administration (RA)

- Review proposals, awards, and related sponsor documents to determine whether:

    - Controlled Unclassified Information (CUI), NIST SP 800-171, DFARS 252.204-7012/7020, Cybersecurity Maturity Model Certification (CMMC), or other cybersecurity requirements are referenced.
    - Information is marked as CUI (overarching term), CTI (Controlled Technical Information), or CDI (Controlled Defense Information).
- Identify whether the proposal or award includes pricing, budget line items, or cost assumptions related to CUI handling, cybersecurity compliance, or cybersecurity staffing.
- Coordinate with Project Leadership and Research Technology Office when CUI is identified, anticipated, or requires pricing.
- Verify that authorized recipients meet dissemination controls and mandatory training requirements prior to distribution.
- Coordinate controlled distribution of CUI documents, ensuring access is limited to individuals with a valid need to know.

Office of Research Compliance (Export Controls)

- Provide authoritative determination on whether CUI is export-controlled under U.S. export control regulations.
- Confirm required dissemination controls for export-controlled CUI.
- Advise on foreign national access restrictions and permissible participation.
- Facilitate development and approval of a Technology Control Plan (TCP), when required.
- Approve any sharing, forwarding, or handling of export-controlled CUI.
- Serve as the primary contact for export-controlled CUI inquiries (export.control@asu.edu).

Knowledge Enterprise Research Technology Office

- Review cybersecurity requirements associated with CUI in proposals and awards.
- Advise on institutional capabilities and compliant secure environments for storing, processing, and transmitting CUI.
- Support pricing and budgeting considerations related to cybersecurity controls and staffing.
- Provide guidance on approved tools and systems for handling digital CUI.
- Accept and manage ServiceNow tickets related to research cybersecurity requirements.

Project Leadership *(Principal Investigator, Co-Investigators, C-suite leadership, Project/Program Management)*

- Review proposal and award documents for indications of CUI, cybersecurity requirements, or dissemination restrictions.
- Identify the type or category of CUI (e.g., export control, privacy, financial) or request clarification from the Sponsor when unclear.
- Identify individuals who require access to CUI and confirm they:
    - Are authorized based on dissemination controls.
    - Have a legitimate need to know.

- Ensure foreign nationals do not access CUI unless explicitly authorized by the U.S. Government and approved by Export Controls.
- Distinguish fundamental research activities from CUI-restricted work and ensure foreign nationals participate only in permissible portions.
- Implement supervision, access controls, and mitigation measures identified in the TCP or other compliance requirements.
- Ensure ongoing monitoring and adherence to access limitations.
- Ensure access to project systems and CUI (including SWAPHub or similar platforms) is promptly removed when personnel leave the project.
- Ensure physical and digital safeguarding requirements are followed in day-to-day operations.

Authorized Project Personnel (CUI Handlers)

- Complete all required training prior to accessing CUI, including:
    - Controlled Unclassified Information (CUI) Training
    - Insider Threat Awareness
    - Initial Orientation and Awareness Training
    - Cybersecurity Awareness
    - HIPAA-required training when handling HIPAA-designated CUI
- Access, store, transmit, and dispose of CUI only in accordance with institutional policies, training, and approved systems.
- Maintain physical security of hardcopy CUI and prevent unauthorized viewing or disclosure.
- Follow labeling, safeguarding, and disposal requirements at all times.
- Immediately report suspected incidents, unauthorized access, or compliance concerns to Project Leadership and Research Compliance.

Sponsors / Prime Awardees

- Identify and mark CUI in solicitations, proposals, and awards when applicable.
- Specify applicable CUI categories, dissemination controls, and cybersecurity requirements.
- Provide clarification when CUI type or restrictions are unclear.

Requirements / Steps

Process Phases:

This process spans multiple stages:

- Pre-Award Phase: Steps 1 -4
- Pre- or Post-Award Phase: Step 5
- Post-Award Phase: Steps 6-9

Step 0: Locate and Request Access to FOAs Containing CUI *(Applies prior to Step 1 and during opportunity identification)*

FOAs that contain Controlled Unclassified Information (CUI) are not publicly posted and may not be freely shared. These FOAs are typically distributed directly by the Sponsor or Program Manager (PM) to eligible institutions or investigators.

- If a PI becomes aware of a restricted FOA through:
    - a Program Manager,
    - prior sponsor communications,
    - a colleague, or
    - a notice indicating the FOA is available "upon request," the PI must engage their Unit RA, and the RA will contact RAhelp@asu.edu before requesting or distributing the FOA.

- ORSPA Pre-Award Services leadership will coordinate with the Sponsor or Prime to:
    - confirm institutional eligibility,
    - determine whether a request form or nondisclosure is required,
    - verify that the FOA is appropriately designated as CUI,
    - identify the correct institutional delivery method (secure electronic or hard copy), and
    - ensure the FOA is received and stored in compliance with CUI requirements.

Important restrictions:

- FOAs containing CUI may not be forwarded, copied, or shared until reviewed and approved by ORSPA and the Knowledge Enterprise Office of Research Compliance.
- If a PI receives an FOA directly from a Sponsor or PM and is informed it cannot be shared, this indicates CUI restrictions are in place. The PI must immediately notify ORSPA for guidance.
- FOAs containing CUI should be sent to the institutional office designated by ORSPA, not to departments or individuals, unless explicitly authorized.

Once the FOA is received and reviewed, proceed to **Step 1: Determine whether CUI is involved**.

Step 1: Determine whether CUI is involved *(This step applies once the FOA or related sponsor materials have been received through the approved ORSPA process described in Step 0.)*

Determine whether the material/information contains Controlled Unclassified Information (CUI), whether CUI may be included in the resulting award, and whether the proposal includes pricing or cost considerations related to CUI compliance.

- Sponsored Projects/RA to review the proposal, award, or related documents to determine whether:
    - CUI, NIST SP 800-171, DFARS 252.240-7997 (previously 252.204-7020), CMMC, or other cybersecurity requirements are referenced;
    - The information is marked as CUI* (overarching term used); and/or
    - The information is marked as CTI* (Controlled Technical Information) or CDI* (Controlled Defense Information). Both of these are subsets of CUI.

      *Do not share the material or forward-related emails without the Knowledge Enterprise Office of Research Compliance approval, contact export.control@asu.edu
    - The proposal will include pricing, budget line items, or cost assumptions related to CUI, cybersecurity compliance and/or cybersecurity staffing, see Step 3 below.

Step 2: Determine CUI type and controls

- Sponsored Projects/RA/Project Leadership to identify the category of CUI (e.g., export control, privacy, financial) or request clarification from the Sponsor on category of CUI.
    - Resource: https://www.archives.gov/cui/registry/category-list
- Sponsored Projects/RA/Project Leadership to check for dissemination controls or restrictions that apply to the CUI. These are controls to limit CUI access to individuals or organizations and have a valid need to know.
- Sponsored Projects/RA/Project Leadership to contact Office of Research Compliance if CUI is export-controlled at export.control@asu.edu to confirm required specific dissemination controls under U.S. export control regulations. Do not share the material or forward-related emails without the Office of Research Compliance approval. CUI Guidance

Step 3: Contact KE Research Technology Office

- Sponsored Projects/RA/Project Leadership: If CUI is identified, anticipated, or needs to be priced, submit a ticket.
    - Contact KE Research Technology Office at Service Now Review Research Cybersecurity Requirements in Contracts/Proposals.

Step 4: Confirm Recipient Eligibility

- Project Leadership to identify individuals who need access. Confirm that:
    - They are authorized to receive CUI based on dissemination controls (U.S. citizens, permanent residents, government employees, or contractors as applicable). If CUI is

export-controlled, promptly contact Office of Research Compliance export controls at export.control@asu.edu to confirm required specific dissemination controls under U.S. export control regulations.

  - They have a valid need to know. Under the CUI program governed by the National Archives and Records Administration, access to CUI must be limited to individuals who:

    - Are authorized (e.g., trained, vetted, contractually covered), and

    - Have a legitimate need-to-know to perform their duties

- Project Leadership responsibility: Foreign nationals typically cannot access CUI. If CUI is export-controlled, access to foreign nationals may be permissible with U.S. Government authorization. Contact the Office of Research Compliance export controls at export.control@asu.edu

  - If part of the work qualifies as fundamental research and is unclassified, foreign nationals may participate in that portion only. They would not have a reason to view the CUI.

Step 5: Mandatory Training

- In addition to ASU required annual cybersecurity training, all personnel handling CUI must complete:

  1. Controlled Unclassified Information (CUI) Training
  2. Insider Threat Awareness
  3. Initial Orientation and Awareness Training
  4. Cybersecurity Awareness

- Researchers handling HIPAA data marked as CUI are also required to take

  1. HIPAA for ASU Researchers
  2. HIPAA for ASU Covered Entity Employees

- Project Leadership to confirm that training is completed before accessing any CUI documents.

Step 6: Coordinate Distribution

- Project Leadership provides a list of authorized recipients to the RA.

- RA verifies recipients meet all dissemination controls and completed training.

- Until ASU has a compliant secure environment to meet CUI. CUI documents can only be in the form of hardcopy and will need to be picked up in person from a designated location. *Note: Distribution only to those who need to know.*

- If CUI is export-controlled, as determined by the Office of Research Compliance Export Controls, the controls and dissemination will be described in the Technology Control Plan (TCP).

The Office of Research Compliance will facilitate the development of the TCP with the Project Leadership.

Step 7: Safeguard CUI

- Only store and access digital CUI in regulatory compliant systems, using the Research Data Solution Tool.
- Only transfer digital CUI using regulatory compliant tools.
- Store physical documents in a locked file cabinet or drawer only to the designated/authorized recipient of the CUI..
- Only authorized individuals with a need to know may review the documents.
- Review physical documents only in controlled settings (out of sight of non-approved viewers, covered windows, see here for physical security details)
- Label the information as "CUI" and include the CUI category when it is known or specified.
- If CUI is export-controlled, safeguarding will be in accordance with the approved TCP.

Step 8: Disposal of CUI

- Once no longer needed, destroy CUI according to CUI standards outlined in the training, Controlled Unclassified Information (CUI) Training.
- If CUI is export-controlled, disposal will be in accordance with the approved TCP.

Step 9: Special Considerations

- **Foreign Nationals**: Non-US persons are usually restricted from having access to CUI. Dissemination controls may indicate further limitation to access. CUI will include NOFORN markings to indicate that foreign nationals, permanent residents, and green card holders cannot have access to said materials.
- **Fundamental Research Exception:** If the work is unclassified and fundamental research, foreign nationals may participate in that portion. No CUI, publication, or export control restrictions can be applied to any resulting award.
- **Solicitation Compliance:** Always review the award or proposal for additional restrictions, export control, or nondisclosure requirements.
- **Third Parties:** Are not authorized to receive CUI directly from ASU. Any request for CUI must be submitted directly to the Sponsor or Prime awardee, unless the applicable agreement explicitly permits ASU to share CUI with the Third Party.
- **Subawards:** ASU subawardees may not share CUI directly with ASU or the Sponsor unless the subcontract or sponsor explicitly authorizes direct submission.