Confidential Research and Publications Policy

PUPPOSE

National Institute of Standards and Technology’s Special Publication 800-171 (NIST 800-171), is a Federal standard that standardizes security controls applied to Controlled Unclassified Information (CUI) and systems and processes involved with this data within federally funded environments. The University of Oklahoma is obligated to ensure that all systems and processes involved with CUI are compliant with NIST 800-171 to continue receiving Federal funds associated with the use of this data (either directly received from the government or indirectly through associated covered contracts and contractors). The purpose of the Confidential Research and Publications Policy is to establish the University of Oklahoma’s framework for providing adequate security of research and publication information designated as restricted, controlled, confidential, or sensitive.

The University of Oklahoma, through its research mission, is subject to laws, regulations and government wide policies that require certain types of information to be safeguarded. Some of the labels or legacy markings used to describe information subject to these laws, regulations and policies include, but are not limited to:

- For Official Use Only (FOUO)
- Controlled Unclassified Information (CUI)
- Sensitive But Unclassified (SBU)
- Limited Official Use (LOU)
- Sensitive Unclassified Information (SUI)
- Law Enforcement Sensitive
- DEA Sensitive
- Official Use Only (OUO)
- Department Of Defense (DoD) Technical Information
- Distribution Statements on Technical Documents
- Sensitive Security Information
- Protected Critical Infrastructure Information
- Unclassified Controlled Nuclear Information
- Export-Controlled Information

The University of Oklahoma shall use the term Controlled Unclassified Information (CUI) to describe the information types listed above.

SCOPE

This Policy applies to any offer or information OU or a sub-contractor of OU creates or possesses for or on behalf of the United States Government, which is required to be protected under law, regulation, or government-wide policy and is indicated in an executed contract or agreement where:

- Associated data is labeled as Controlled Unclassified Information;
- Contracts having DFARS 252.204-7012, or any other clause which invokes CUI requirements;
Confidential Research and Publications Policy

Examples of projects, which may include CUI.

- **Defense projects**
  - For defense projects, "covered defense information" can come in several forms. Generally, for aerospace manufacturing, noncommercial technical details are CUI. This may be called out in the contract, task order, or delivery order.
  - Technical information includes research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, datasets, studies and analyses, and computer software executable code and source code.

- **The following are specific DFARs that define the application of CUI:**
  - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
  - 252.227-7013 Rights in Technical Data-Noncommercial Items
  - 252.239-7010 Cloud Computing Services

  **Note:** These contract clauses denote that data must be handled appropriately.

- **CUI also applies to defense projects that include technical information with military or space application subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.**

- **Non-defense projects**
  - For non-defense federal projects, much depends on the specific contract. The definition is a bit open-ended in "52.204-21 Basic Safeguarding of Covered Contractor Information Systems," which states:

    Federal contract information means 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 not including information provided by the Government to the public such as the collection of PII or PHI.

**POLICY STATEMENT**

Controlled Unclassified Information (CUI) is unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or government-wide policy, as listed in the CUI Registry by the National Archives and Records Administration (NARA). This policy establishes a university-wide CUI Program and authorizes the Category D1 Confidential Research and Publications Information Protection Standard to define the handling, marking, protecting, sharing, destroying, and decontrolling of CUI in accordance with law, regulations, and government-wide policies.

Contracts having any clause which invokes CUI requirements, must be reviewed and assessed for CUI by the Associate VP for the Office of Research at OU.

**PR.AT Awareness and Training – CUI Training**

OU Faculty, Staff, and any other OU personnel including applicable contractors, storing, transmitting or processing CUI, must receive suitable CUI awareness training provided by the OU System Security Training, Education, and Awareness Team. Initial training must commence within 90 days of the identification of CUI requirements and at least once every 2 years after.

**PR.PT Protective Technology - Marking and Safeguarding**

All CUI documents must be protected according to applicable laws, regulations, and government-wide policies. Specific procedures for marking are outlined in the Category D1 Confidential Research and Publications Information Protection Standard. Authorized holders of CUI will be held accountable for knowing and following these procedures as described in the mandatory training and the Category D1 Confidential Research and Publications Information Protection Standard.
PR.IP Information Protection Procedures - NIST SP 800-171 Controls
All Information Systems or Information classified as Category D1 – Confidential Research and Publications Information, must comply fully with the Category D1 – Confidential Research and Publication Information Protection Standard (either directly or through compensating controls). In the event compensating controls are required, the OU System Security GRC Team, in collaboration with the Data Manager, must submit a written explanation of why a requirement is not applicable or how an alternative but equally effective security measure can compensate for the inability to satisfy a requirement. An authorized representative will adjudicate such requests prior to contract award.

Prior to disseminating CUI, authorized holders must properly label CUI. Prior to disseminating CUI to non-executive branch entities, OU employees should enter into a formal agreement that includes the requirement to comply with EO 13556 and the CUI Registry. At a minimum, the agreement must include the provisions of the DFARS 252.204-7012, or similar clause, statement.

ID.RA Risk Assessment - Proving Compliance
All Information Systems storing, processing, or transmitting CUI must undergo an annual Category D1 – Confidential Research and Publications Information Protection Standard compliance assessment by the OU System Security Governance, Risk, and Compliance Team before interacting with CUI. This assessment is to be completed on or before the execution and anniversary date of agreements imposing Category D1 protection requirements. These assessments will result in an attestation report that will be provided to the University of Oklahoma Vice President of Research, or designee as an attestation of the level of compliance with information protection requirements.

Any items of non-compliance found during the assessment must be remediated before any interaction with CUI is allowed.

In support of the offer and when required, the OU System Security Governance, Risk, and Compliance (GRC) team in collaboration with the Data Manager, must develop, document and maintain:
- All CUI self-assessment documentation;
- A Systems Security Plan;
- A Plan of Action and Milestones to monitor and manage security controls not yet implemented, but scheduled to be implemented, and controls not scheduled to be implemented; and
- University risk decisions supporting any decisions to not implement required security controls;

If designated by offer or award language, offers and agreements which require the system that is storing or processing CUI to obtain Authority to Operation (ATO), OU System Security GRC team must coordinate the activities required to receive an ATO, which is granted by an Authorizing Official (AO) once an Information System has been assessed and authorized to be in compliance. The AO is the senior official/executive with the authority to assume responsibility for operating an Information System at an acceptable level of risk; the AO is typically employed by the government agency/funding sponsor.

ID.GV Governance - Misuse of CUI
Misuse of CUI may be subject to penalties established in applicable laws, regulations, or government-wide policies, or result in loss of funding. University Personnel responsible for submitting, reviewing, and/or signing federally funded proposals, solicitations, or contracts must identify and report to OU System Security GRC when CUI

RESPONSIBILITIES

Below are the responsibilities of the CUI-specific roles established to implement the University of Oklahoma CUI program.

A. Information System or Data Owner
The University of Oklahoma, in support of its Research mission, has elected the Office of Research (VPR) for the Norman and Health Sciences Center campuses, to serve as the Confidential Research Information System or Data Owner who will be responsible to:

- Establish and oversee the CUI Program at OU;
- Ensure OU has implemented CUI policies and plans;
- Provide updates on CUI implementation efforts to the GRC Team for CUI Compliance;
- Notify authorized recipients, of any waivers granted by the contracting office including a description of all waivers in the Security Management Plan; and
- Interact directly and officially with the Executive Agent on CUI matters including submission of required reports.

B. OU System Security GRC Team
- Develop and implement OU’s CUI self-assessment compliance methodology;
- Present at least annually, and more often as necessary, a Category D1 Confidential Research and Publications Cybersecurity Assessment Report;
- Establish a process to accept and manage challenges to CUI status (including improper or absence of marking), in accordance with existing processes based in laws, regulations, and Government-wide policies;
- Establish processes and criteria for reporting and investigating improper handling of CUI;
- Ensure OU compliance with laws, regulations and OU policy in collaboration with OU’s Official for Privacy;
- Establish processes for handling CUI control requests;
- Oversee the compliance activities and responsibilities of the CUI System Administrator; and
- Coordinate CUI policy development and updates.

C. OU System Security Training, Education, and Awareness Team
- Implement the Information Security CUI Education and Training Program and ensure identified and or pertinent OU Faculty, Staff, or any other OU personnel including applicable contractors, receive suitable CUI Awareness Training;

C. Category D1 - Information System or Data Administrator
- Manage the day-to-day operations of the OU CUI program as directed by the VPR and/or GRC Team CUI Compliance Team;
- Carry out the responsibilities of the CUI controls; and
- Upload evidence for periodic review of CUI controls to the GRC compliance assessment repository.

REFERENCES
- NIST Cybersecurity Framework
- NIST SP 800-171-Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Executive Order 13556 Controlled Unclassified Information (CUI)
- NARA’s CUI webpage

ENFORCEMENT AND COMPLIANCE
Failure to comply with this policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, University policies, and applicable laws. This policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.
Confidential Research and Publications Policy

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this standard. Such instances must call the Information Protection Policy exception process. Each exception request is carefully considered by the Information Owner, Information System Owner, OU IT Security Advisory Council and the CIO. See OU IT Information Protection Policy Exception Standard.

Table 1 Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version</th>
<th>Revised By</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/14/2019</td>
<td>0.1</td>
<td>April Dickson, GRC</td>
<td>Initial Draft</td>
</tr>
<tr>
<td>10/21/2019</td>
<td>0.1</td>
<td>April Dickson, GRC</td>
<td>Revised Title of Policy from Controlled Unclassified (CUI) Policy to Confidential Research and Publications Policy in order to better align with University mission. Added Rows 18-31 to better define how CUI can be identified.</td>
</tr>
<tr>
<td>02/13/2020</td>
<td>0.2</td>
<td>April Dickson, GRC</td>
<td>Modified row 148, and added language to reflect the named Information System or Data Owner for OU Confidential Research information: “The University of Oklahoma, in support of its Research mission, has elected the Office of Research (VPR) for the Norman and Health Sciences Center campuses, to serve as the Confidential Research Information System or Data Owner who will be responsible to?”</td>
</tr>
<tr>
<td>03/10/2020</td>
<td>0.2</td>
<td>April Dickson, GRC</td>
<td>Elevated version 0.2 to the official 1.0 version being presented to the President for final approval and publication after receiving Governance board approval.</td>
</tr>
</tbody>
</table>

Table 2 Approval History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Approved by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>04/27/2020</td>
<td>Interim President, Joseph Harroz</td>
</tr>
</tbody>
</table>

Table 3 Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Review Date</th>
<th>Reviewed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>03/10/2020</td>
<td>Information Security Review Board (ISRB)</td>
</tr>
<tr>
<td>1.0</td>
<td>03/10/2020</td>
<td>Security Governance Advisory Council (SGAC)</td>
</tr>
</tbody>
</table>