JOB DESCRIPTION
The UNIVERSITY of OKLAHOMA

Controlled Unclassified Information (CUI) Manager

Job Code: 8264

Salary Grade: S12

FLSA Status: Exempt

The following statements are designed to outline the general functions and typical responsibility levels associated with positions in this classification. They are not intended to serve as an exhaustive list of specific duties or requirements for individual positions assigned to this classification.

Duties and Responsibilities

Responsible for leading and coordinating efforts to support compliance with Controlled Unclassi¿ed Information (CUI) regulations, including NIST 800-171, 32 CFR Part 2002, CMMC, and other federal mandates related to federally funded research. Works collaboratively with research, IT, and administrative partners to implement and maintain processes, controls, and training that support the secure handling of CUI across research and operational environments..

- Serves as the primary point of contact for all CUI-related matters, providing expert guidance and support to internal teams and external partners.
- Assess existing CUI research programs, policies, and IT infrastructure, collaborating with stakeholders to identify needs and gaps.
- Collaborates with IT and other partners to define requirements and support the development and maintenance of CUI-compliant environments (e.g. secure enclaves).
- Coordinates with the O¿ce of Research Services, Office of the Vice President for Research and Partnerships, and the Office of Export Controls to identify and address CUI requirements in proposals and projects.
- Works directly with researchers and project teams to support implementation of CUI requirements, including developing project-specific plans and monitoring approaches.
- Develops, implements, and maintains operational processes, procedures, and guidance to support consistent and compliant handling of CUI.
- Delivers training and educational resources to faculty, staff, and students to promote awareness and understanding of CUI responsibilities.
- Applies federal regulations and institutional policies to support compliance in U.S. Government-funded research programs, escalating complex or high-risk issues as appropriate.
- Conducts routine assessments, monitoring activities, and internal reviews to evaluate compliance and identify potential risks or areas for improvement.
- Supports incident response activities in coordination with IT and appropriate offices, including documentation and follow-up actions related to CUI-related concerns.
- Maintains accurate documentation of CUI activities, compliance efforts, and identified risks; assists in preparing reports for leadership and regulatory requirements.
- Participates in internal committees and external professional groups to stay informed on evolving CUI requirements and best practices.
- Supports user access management processes and helps ensure appropriate system configurations and permissions for CUI environments in coordination with IT.
- Provides day-to-day guidance and work direction to assigned staff, supporting task prioritization, training, and professional development.
- Performs other duties as assigned to support the successful implementation and ongoing management of CUI-related activities.

Minimum Qualifications

Education:

- Bachelor's degree in cybersecurity, information technology, or a related discipline
- Or 60 months of comparable job experience.

Experience:

- 5 years of experience in research security, cybersecurity compliance, information security or related ¿eld

Certifications or Licenses:

- Certi¿ed Information Systems Security Professional (CISSP), Certi¿ed Information Security Manager (CISM), or Cybersecurity Maturity Model Certi¿cation (CMMC Assessor)
- Ability to obtain and maintain a security clearance

Verification of education and licensure (if applicable) will be required if selected for hire.

Knowledge, Skills, and Abilities

- Strong knowledge of NIST SP 800-171, CMMC, and federal Controlled Unclassi¿ed Information (CUI) handling regulations

- Familiarity with federal policies on handling, safeguarding, and disseminating CUI within government and contractor environments
- Strong ability to develop, implement, and maintain CUI policies, procedures, and training programs that ensure compliance and mitigate risk
- Pro¿cient in conducting security assessments, audits, and monitoring activities related to CUI handling
- Understanding of information security frameworks, risk management principles, and compliance standards relevant to CUI protection
- Committed to delivering high-quality work while upholding professional standards
- Excellent organizational and document management skills
- Strong verbal and written communication with the ability to conveys complex information clearly and concisely to diverse audiences through reports, presentations, and interpersonal interactions
- Ability to apply critical thinking to identify issues, evaluate options, and implement e¿ective solutions that enhance processes and outcomes
- Ability to manages multiple deadlines and competing priorities through careful planning and adaptability, consistently meeting project goals and organizational expectations
- Stay current with evolving CUI regulations and adjust organizational practices accordingly

Working Conditions

- Occasional evening or weekend work required for audits, incident response, or compliance deadlines
- Must be able to sit or stand for extended periods and use standard o¿ce equipment such as computers, phones, printers, etc.
- Travel is required to support audits, training, conferences, site assessments, or coordination with external partners

Printed Date: 10/29/2026