
Auburn University Job Description

Job Title: **Cybersecurity Eng- Research**

Job Family: No Family

Job Code: **MA76**

CS03: \$74,200 - \$118,700

FLSA status: Exempt

Job Summary

Under general supervision of the Cybersecurity Research manager, responsible for the planning, engineering, developing, implementing, and compliance monitoring of organization-wide research programs including, but not limited to, Controlled Unclassified Information (CUI) management; Cybersecurity Maturity Model Certification (CMMC); Research Electronic Data Capture System (REDCap); and Electronic Research Administration (ERA). Performs analysis to ensure security controls are consistently implemented, integrating new technology with IT research security standards; developing and executing plans for monitoring, assessing, and verifying security controls across all major information systems; and developing, evaluating, and exercising IT survivability and contingency plans to protect the University's information assets.

Essential Functions

1. Monitors real-time data, discovers security events, analyzes qualified incidents, executes documented resolutions for common incidents, recommends remediation steps for new incidents, and escalates major security incidents for the Research Security Enclave.
 2. Provides assistance with governance, risks, and compliance by 1) coordinating the development of University Research information security technical standards, guidelines, and procedures, based on a recognized framework of best practices and in support of Auburn University policies and regulations, such as Cybersecurity Maturity Model Certification (CMMC), NIST 800-171, and NIST 800-53; 2) assisting with risk analysis and risk management; 3) assisting with security and compliance reviews; 4) preparing and maintaining system security plans (SSPs) for various research projects on campus; 5) creates and manages standard operating procedures (SOPs) for various projects.
 3. Assists with communication, reporting, and alerting on general information security issues as well as on specific assignments within Information Security tool sets of the Research Security Enclave.
 4. Develops scripts and tooling to verify security platforms and automate security team operations.
 5. Implements and evaluates new technology deployments, integration testing, information security products, services, and procedures to enhance productivity and effectiveness while maintaining compliance.
 6. Provides assistance for the Research Security Enclave, to include network security and 1) maintaining cybersecurity firewalls and web application firewalls for on-premise network and cloud environments that support research; 2) managing security monitoring systems for network server, firewall, and network anomalies within the Research Security Enclave; 3) maintaining infrastructure designs of current and future network designs and incorporating appropriate mitigation of existing and emerging threats; and 4) assisting with identifying security design gaps in existing and proposed network architecture and recommending changes and enhancements.
 7. Stays fully informed of current security information and issues, as well as regulatory changes affecting industry research and higher education at the state and national level. Engages in professional development to maintain continual growth in professional skills and knowledge essential to the position.
 8. Performs other related duties as assigned by the supervisor.
-

Auburn University Job Description

Supervisory Responsibility

May be responsible for training, assisting or assigning tasks to others. May provide input to performance reviews of other employees.

The above essential functions are representative of major duties of positions in this job classification. Specific duties and responsibilities may vary based upon departmental needs. Other duties may be assigned similar to the above consistent with the knowledge, skills and abilities required for the job. Not all of the duties may be assigned to a position.



Auburn University Job Description

Minimum Required Education and Experience

	<u>Minimum</u>	<u>Focus of Education/Experience</u>
Education	Four-year college degree	Degree in Computer Science, Engineering, Computer Information Systems, or related field. See experience for substitutions.
Experience (yrs.)	5	Demonstrated Cybersecurity experience, Governance, Risk and Compliance (GRC). Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber-attacks. <ul style="list-style-type: none">• High School Diploma - 13 yrs.• Associate's Degree - 9 yrs.• Bachelor's degree - 5 yrs.

Substitutions allowed for Education:

When a candidate has the required experience, but lacks the required education, they may normally apply additional relevant experience toward the education requirement, at a rate of two (2) years relevant experience per year of required education.

Substitutions allowed for Experience:

Indicated experience is required; no substitutions allowed.

Minimum Required Knowledge

- Knowledge of generally accepted information/cyber security principles and practices with the ability to apply that knowledge to perform complex and non-routine specialized information technology (IT) security analysis functions such as troubleshooting, advanced analysis, research, and problem-solving.
- Deep understanding of NIST 800-53 and NIST 800-171 framework and controls.
- Knowledge of Cybersecurity Maturity Model Certification framework.
- Must have team leadership skills, negotiation skills, and advanced client relation skills.
- Ability to remain up-to-date with privacy and security regulations.
- Ability to recognize, analyze, and solve a variety of problems.
- Ability to effectively communicate technical concepts to a non-technical audience.

Certification or Licensure Requirements

- None required.
- Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) or CompTIA Advanced Security Practitioner (CASP) is desired. Other certifications from recognized vendors (EC-Council, GIAC, etc.) will be considered.
- United States Government Security Clearance is desired, but not required.

Physical Requirements/ADA

No unusual physical requirements. Requires no heavy lifting, and nearly all work is performed in a comfortable indoor facility.

Externally imposed deadlines; set or revised on short notice; frequent shifts in priority; numerous interruptions requiring immediate attention; unusual pressure on a daily basis due to accountability for success for major projects or areas of operation.

Auburn University Job Description

Job occasionally requires standing, walking, sitting, reaching, climbing or balancing, stooping/kneeling/crouching/crawling, talking, hearing, handling objects with hands, and lifting up to 50 pounds.

Date: 10/22/2021

