

---

## Auburn University Job Description

Job Title: **Mgr, Cyber - Research**

Job Family: No Family

Job Code: **MA74**

Grade CS05: \$98,200 - \$157,200

FLSA status: Exempt

---

### Job Summary

As a member of the Office of the Vice President for Research & Economic Development (OVPRED), and working closely with the University's Cybersecurity team (Office of the CIO/CISO) as well as Office of Information Technology (OIT) and Research Security Compliance, this position is responsible for providing cybersecurity management of multiple 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).

Directs security specialists within the OVPRED, as well as collaborates with University CISO and Cybersecurity personnel that provide cybersecurity operations including a Security Operations Center (SOC); systems and network security monitoring; penetration testing; firewall and related infrastructure management; network traffic analysis; and cybersecurity consulting for the University community. Assists with Governance, Risks and Compliance (GRC) requirements specifically for research. Consults with leadership on security matters such as security frameworks policies/procedures.

### Essential Functions

1. Mentors the Research Cybersecurity team members, researchers, and contract specialists, as well as implements professional development plans for all members of the team.
  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; and 4) preparing and maintaining system security plans (SSPs) for various research projects on campus.
  3. Provides assistance and guidance for the Research Security Enclave, to include network security and 1) maintaining cybersecurity firewall and web application firewalls for on-premise network and cloud environments that support research; 2) directing security monitoring systems for network server, firewall, and network anomalies within the Research Security Enclave; 3) creating infrastructure designs of current and future network designs and incorporating appropriate mitigation of existing and emerging threats; and 4) identifying security design gaps in existing and proposed network architecture and recommending changes and enhancements.
  4. Collaborates with the Auburn Office of Cybersecurity security operations ensuring the Security Operations Center (SOC) is monitoring appropriate Research Cybersecurity events and providing appropriate alerting to the Research Cybersecurity Group, and provides guidance and strategic planning for Security Incident Event Management (SIEM), both in the cloud and on-premise.
  5. Collaborates with campus groups to build awareness and a sense of common purpose around research security. Stays fully informed of current security information and issues, as well as regulatory changes affecting higher education at the state and national level. Participates in national policy and practice discussions, and communicates results with the entire campus. Engages in professional development to maintain continual growth in professional skills and knowledge essential to the position.
  6. Performs special projects and other duties as assigned.
-

---

## **Auburn University Job Description**

### **Supervisory Responsibility**

Full supervisory responsibility for other employees is a major responsibility and includes training, evaluating, and making or recommending pay, promotion or other employment decisions.

*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>
<b>Education</b>	Four-year college degree	Entry into the applicant pool requires a Bachelor's degree from an accredited institution in Business Administration, Management, Computer Engineering, Computer Science, Information Systems, or a related field. Master's Degree in information technology or directly relevant discipline is preferred.
<b>Experience (yrs.)</b>	8	Demonstrated successful experience in information technology that includes a minimum of 8 years of progressively responsible experience in information security. Must possess full or advanced proficiency and understanding of Security Operations, Security Operations Center (SOC) processes, Network Security, and Cybersecurity Governance, Risks and Compliance. Experience as a manager preferred. Experience leading projects involving multiple team members can be considered as management experience.

#### **Substitutions allowed for Education:**

Indicated education is required; no substitutions allowed.

#### **Substitutions allowed for Experience:**

Indicated experience is required; no substitutions allowed.

#### **Minimum Required Knowledge**

Demonstrated knowledge of various security and regulatory compliance standards, such as understanding and experience with the Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA); Federal Information Security Management Act (FISMA); Cybersecurity Maturity Model Certification (CMMC); NIST 800-171; and NIST 800-53. Knowledge of data forensics and collection technologies, disk imaging, chain of custody records, handling sensitive information preferred.

Must be able to convey goals and objectives clearly and in a compelling manner; listen effectively and clarify information as needed; produce clear status reports; and communicate tactfully and candidly. Demonstrated ability to mentor and lead cybersecurity personnel. Demonstrated ability to identify problems, analyze courses of action, and propose solutions. Ability to maintain industry security certification(s).

#### **Certification or Licensure Requirements**

This position requires industry-standard Information Assurance certifications appropriate to the position (Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or equivalent). Certified Information Systems Auditor (CISA) will also be considered.

United States Government Security Clearance desired, but not required.

---

---

---

## **Auburn University Job Description**

### **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 and revised beyond one's control; interruptions influence priorities; difficult to anticipate nature or volume of work with certainty beyond a few days; meeting of deadlines and coordination of unrelated activities are key to position; may involve conflict-resolution or similar interactions involving emotional issues or stress on a regular basis.

Job frequently requires standing, walking, sitting, talking, hearing, handling objects with hands, and lifting up to 10 pounds.

Job occasionally requires reaching, stooping/kneeling/crouching/crawling, and lifting up to 25 pounds.

Requires the ability to view and interpret information on a computer monitor for large portions of the day.

Date: 2/12/2021

---