AUBURN
Human Resources

Mgr, Cyber-Research

Job Description

JOB INFORMATION

Job Code	MA74
Job Description Title	Mgr, Cyber-Research
Pay Grade	CS08
Range Minimum	$104,030
33rd %	$138,710
Range Midpoint	$156,040
67th %	$173,380
Range Maximum	$208,060
Exemption Status	Exempt
Approved Date:	1/1/1900 12:00:00 AM
Legacy Date Last Edited	9/30/2022

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

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.

RESPONSIBILITIES

- Mentors the Research Cybersecurity team members, researchers, and contract specialists, as well as implements professional development plans for all members of the team.
- 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.
- 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.
- 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.

RESPONSIBILITIES

- 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.
- Performs special projects and other duties as assigned.

SUPERVISORY RESPONSIBILITIES

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.

MINIMUM QUALIFICATIONS

To be eligible, an individual must meet all minimum requirements which are representative of the knowledge, skills, and abilities typically expected to be successful in the role. For education and experience, minimum requirements are listed on the top row below. If substitutions are available, they will be listed on subsequent rows and may only to be utilized when the candidate does not meet the minimum requirements.

MINIMUM EDUCATION & EXPERIENCE

Education Level	Focus of Education		Years of Experience	Focus of Experience	
Bachelor's 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.	And	8 years of	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.	Or

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

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 identity problems, analyze courses of action, and propose solutions.	
Ability to maintain industry security certification(s).	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
Certified Information Security Manager (CISM)		Upon Hire	Required	And

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
CISSP Certified Information Systems Security Professional		Upon Hire	Required	And
Certified Information Systems Auditor (CISA)		Upon Hire	Required	And
	United States Government Security Clearance	Upon Hire	Desired	

PHYSICAL DEMANDS & WORKING CONDITIONS

Physical Demands Category:	Other

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
Standing				X		
Walking				X		
Sitting				X		
Lifting				X		
Climbing	X					
Stooping/ Kneeling/ Crouching	X					
Reaching	X					
Talking				X		
Hearing				X		
Repetitive Motions				X		
Eye/Hand/Foot Coordination				X		

WORKING ENVIRONMENT

Working Condition	Never	Rarely	Occasionally	Frequently	Constantly
Extreme cold		X			
Extreme heat		X			
Humidity		X			
Wet		X			
Noise		X			
Hazards		X			
Temperature Change		X			
Atmospheric Conditions		X			
Vibration		X			

Vision Requirements:

Requires performing and/or viewing work on a computer screen for the majority of the day. Ability to view and interpret information on a computer screen for long periods of time.