AUBURN
Human Resources

Dir, Cybersecurity-RSC

Job Description

JOB INFORMATION

Job Code	MA79
Job Description Title	Dir, Cybersecurity-RSC
Pay Grade	CS09
Range Minimum	$118,590
33rd %	$158,120
Range Midpoint	$177,890
67th %	$197,660
Range Maximum	$237,190
Exemption Status	Exempt
Approved Date:	9/23/2024 2:55:23 PM

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

Reporting to the Chief Research Security Officer Director of Cybersecurity for Research Security oversees cybersecurity and IT activities within the Office of the Senior Vice President for Research & Economic Development (OSVPRED), the Auburn University Research and Innovation Campus, and the university's research security compliance office. Ensures the safeguarding of both controlled unclassified research networks and classified information systems, the confidentiality, integrity, and availability of research data. Leads a team of cybersecurity professionals, manage security and IT operations, serves as the Information Systems Security Manager (ISSM), and ensures compliance with federal and institutional security standards.

RESPONSIBILITIES

- Provides strategic direction and leadership to the Research cybersecurity teams, mentoring managers responsible for Cybersecurity Maturity Model Certification (CMMC)and classified systems, and fostering a culture of cybersecurity awareness across all campuses.
- Oversees Research cybersecurity for research programs, including the protection of classified and unclassified data, managing risk assessments, and developing a robust risk management framework.
- Develops and implements a comprehensive cybersecurity strategy, ensuring compliance with federal regulations such as CMMC, National Institute of Standards and Technology (NIST), Defense Federal Acquisition Regulation Supplement (DFARS), and National Industrial Security Program Operating Manual (NISPOM), while maintaining security policies, procedures, and guidelines.
- Collaborates with internal and external stakeholders to build a shared commitment to research security, develop and deliver cybersecurity training programs, and stay informed on regulatory changes.
- Leads incident response efforts for OSVPRED and maintains continuous monitoring programs, ensuring rapid threat detection and effective mitigation strategies.
- Oversees the deployment, management, and evaluation of cybersecurity tools, processes, and software across research networks. Ensure that all information systems and software acquisitions meet cybersecurity standards, supporting the integrity of research activities through regular audits, vulnerability assessments, and secure software deployment.
- Ensures Cybersecurity efforts align with Auburn University's Information Technology priorities.
- Performs special projects as assigned.

The responsibilities listed above show the typical duties for jobs in this classification. Actual tasks may differ depending on the department's needs. Other similar duties may be assigned with discretion of the supervisor. Not every duty will apply to every position, and the amount of time spent on each task can change based on department needs.

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	Business Administration, Management, Computer Engineering, Computer Science, Information Systems, or a related field.	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 desired. Experience leading projects involving multiple team members can be considered as management experience.	

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 desired.	
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)	(Certified Information Security Manager (CISM)	Upon Hire	Required	And
CISSP Certified Information Systems Security Professional	Certified Information Systems Security Professional (CISSP) or equivalent)	Upon Hire	Required	And
Certified Information Systems Auditor (CISA)	Certified Information Systems Auditor (CISA) will also be considered.	Upon Hire	Required	And
	United States Government Security Clearance desired, but not required.	Upon Hire	Required	

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.