AUBURN
Human Resources

Cybersecurity Eng-Research

Job Description

JOB INFORMATION

Job Code	MA76
Job Description Title	Cybersecurity Eng-Research
Pay Grade	CS05
Range Minimum	$74,320
33rd %	$96,610
Range Midpoint	$107,760
67th %	$118,910
Range Maximum	$141,200
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

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.

RESPONSIBILITIES

- 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.
- 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.
- Assists with communication, reporting, and ale1iing on general information security issues as well as on specific assignments within Inf01mation Security tool sets of the Research Security Enclave.
- Develops scripts and tooling to verify security platforms and automate security team operations.
- Implements and evaluates new technology deployments, integration testing, information security products, services, and procedures to enhance productivity and effectiveness while maintaining compliance.
- 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.

RESPONSIBILITIES

- 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.
- Performs other related duties as assigned by the supervisor.

SUPERVISORY RESPONSIBILITIES

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

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	Degree in Computer Science, Engineering, Computer Information Systems, or related field.	And	5 years of	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.	Or
Associate's Degree	Degree in Computer Science, Engineering, Computer Information Systems, or related field.	And	9 years of	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.	Or
High School		And	13 years of	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.	

Substitutions Allowed for Education	Yes

Substitution 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.

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

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.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
CISSP Certified Information Systems Security Professional		Upon Hire	Desired	Or
Certified Information Systems Auditor (CISA)		Upon Hire	Desired	Or
CompTIA Advanced Security Practitioner (CASP)		Upon Hire	Desired	Or
	Other certifications from recognized vendors (EC-Council, GIAC, etc.) will be considered.	Upon Hire	Required	Or
	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:

Ability to see information in print and/or electronically.