AUBURN
Human Resources

Cybersecurity Eng-ISSO

Job Description

JOB INFORMATION

Job Code	MA77
Job Description Title	Cybersecurity Eng-ISSO
Pay Grade	CS05
Range Minimum	$78,840
33rd %	$102,490
Range Midpoint	$114,310
67th %	$126,140
Range Maximum	$149,790
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 Information System Security Manager (ISSM), serves as the Information System Security Officer (ISSO) for the Office of Research Security Compliance. Responsible for the planning, engineering, developing, implementing, and compliance monitoring of research information security programs. Performs analysis to ensure security controls are consistently implemented, integrating new technology with IT 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

- Ensures research information systems are operated, maintained, and disposed of in accordance with security policies and procedures as outlined in the security plan.
- Verifies the implementation of delegated aspects of the system security program.
- Ensures all proper account management documentation is completed prior to adding and deleting system accounts and verifying all security documentation is current and accessible.
- Conducts periodic assessments of authorized systems and providing corrective actions for all identified findings and vulnerabilities.
- Ensures audit records are collected and analyzed in accordance with the security plan.
- Monitors system recovery processes to ensure security features and procedures are properly restored and functioning correctly.
- Monitors changes to systems that could affect authorization.
- Ensures user activity monitoring data is analyzed, stored, and protected.
- Executes the continuous monitoring strategy.

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	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	No specified discipline. Degree in IT or related field preferred.	and	5 years of	Progressively responsible experience with Cybersecurity, as well as Governance, Risk and Compliance (GRC).	Or
Associate's Degree	No specified discipline. Degree in IT or related field preferred.	and	9 years of	Progressively responsible experience with Cybersecurity, as well as Governance, Risk and Compliance (GRC).	Or
High School Diploma or GED		and	13 years of	Progressively responsible experience with Cybersecurity, as well as Governance, Risk and Compliance (GRC).	Or

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 nonroutine specialized information technology (IT) security analysis functions such as troubleshooting, advanced analysis, research, and problem solving.	
Demonstrated team leadership skills, negotiation skills, and advanced client relation skills.	
Demonstrated ability to remain uptodate with privacy and security regulations.	
Demonstrated ability to recognize, analyze, and solve a variety of problems.	
Demonstrated to effectively communicate technical concepts to a nontechnical audience.	
Understanding of NIST 80053 framework and controls.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
	Industry recognized cybersecurity certification required within six (6) months of hire date.	within 180 Days	Required	And
CISSP Certified Information Systems Security Professional		Upon Hire	Required	Or
CISM - Certified Information Security Manager		Upon Hire	Required	Or
Certified Information Systems Auditor (CISA)		Upon Hire	Required	Or
CompTIA Security+ Certification		Upon Hire	Required	Or
Certified Ethical Hacker (CEH)		Upon Hire	Required	Or
	Certified in Risk and Information Systems Control (CRISC) and others as deemed appropriate by the CISO of Auburn University.	Upon Hire	Required	Or
	Current government clearance at the Secret level is	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.