AUBURN
Human Resources

Cybersecurity Eng-Central
Job Description

JOB INFORMATION

Job Code	MA40
Job Description Title	Cybersecurity Eng-Central
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:	11/15/2019 6:44:12 PM
Legacy Date Last Edited	11/10/2019

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

Under general supervision, responsible for the planning, engineering, developing, implementing, and compliance monitoring of organization-wide 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. (Employee must work in central IT unit. Exceptions require CIO prior approval.)

RESPONSIBILITIES

- Ensures information security policies and procedures are followed.
- 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.
- Assists with communication, reporting, and alerting on general information security issues as well as on specific assignments within Information Security tool sets.
- Develops scripts and tools to verify security platforms and automate security team operations.
- Implements new technology deployments and integration testing.
- Evaluates information security products, services, and procedures to enhance productivity and effectiveness.
- Maintains up-to-date understanding of best practices and security threats.
- Works with vendors to resolve security problems and develops infrastructure solutions.
- 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	No specified discipline. Degree in IT or a related field preferred.	And	5 years of	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber-attacks	Or
Associate's Degree	No specified discipline. Degree in IT or a related field preferred.	And	9 years of	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	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.	And
Must have team leadership skills, negotiation skills, and advanced client relation skills.	And
Ability to remain up-to-date with privacy and security regulations.	And
Ability to recognize, analyze, and solve a variety of problems.	And
Ability to effectively communicate technical concepts to a non-technical audience.	And
Strong technical aptitude and computer skills.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
None Required.				
Other	Industry recognized cybersecurity certification	within 180 Days	Required	And
CISSP Certified Information Systems Security Professional		within 180 Days	Required	Or
Certified Information Security Manager (CISM)		within 180 Days	Required	Or
Certified Information Systems Auditor (CISA)		within 180 Days	Required	Or
CompTIA Security+ Certification		within 180 Days	Required	Or
Certified Ethical Hacker (CEH)		within 180 Days	Required	Or
	Certified in Risk and Information Systems Control (CRISC)	within 180 Days	Required	Or
	Others as deemed appropriate by the CISO of Auburn University.	within 180 Days	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:

Ability to see information in print and/or electronically and distinguish colors.