AUBURN
Human Resources

Sr Cybersecurity Eng-Central

Job Description

JOB INFORMATION

Job Code	MA41
Job Description Title	Sr Cybersecurity Eng-Central
Pay Grade	CS06
Range Minimum	$85,790
33rd %	$111,530
Range Midpoint	$124,400
67th %	$137,270
Range Maximum	$163,000
Exemption Status	Exempt
Approved Date:	11/15/2019 6:44:43 PM
Legacy Date Last Edited	11/10/2019

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

Under minimal supervision, serves as technical lead for information technology (IT) security analysis projects and services. Responsible for overseeing and improving the function of the suite of IT security tools utilized by the University to protect the institution's informational assets. Participates in active troubleshooting of data flows as well as evaluates and collaborates on the implementation of new security tools. Functions as the technical and engineering subject matter expert for specific cybersecurity technology areas and is a primary interface to the University's IT community. (Employee must work in central IT unit. Exceptions require CIO prior approval.)

RESPONSIBILITIES

- Serves as the subject matter expert in operating systems, network devices and protocols, security technologies, cloud technologies, and security data sharing work flows. Leads small projects when necessary.
- Assists and, at times, leads efforts for incident response activities. Works with vendors to define mitigation strategies when incidents are identified and responded to.
- Validates and tests information security architecture and design solutions to produce detailed engineering specifications with recommended vendor technologies. Integrates large amounts of intelligence information on threats into context in order to draw insights about the possible implications.
- Compiles relevant data and integrates data into a coherent whole. Considers the information's reliability, validity, relevance, and time sensitivity.
- Works with stakeholders to identify strategies to mitigate and remediate vulnerabilities as they are identified.
- Provides peer level review to work performed by other team members in order to mentor and elevate the team's overall effectiveness.
- Aides in identifying and evaluating assets, trends, and patterns of threat actors. Performs tailored analysis to develop comprehensive target definition for far-reaching strategic threats to support operational planning and to identify opportunities for neutralizing or degrading activities of threat actors.
- Trains other team members on new information security solutions and transitions ownership, where possible, upon successful implementation.
- May serve as a lead within the team, coordinating the work of others and serving as the primary contact.

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 a related field. Master's Degree in a related field preferred.	and	8 years of	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber-attacks.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

In-depth knowledge of IT architecture, project management, basic vendor relations, proposal writing, business acumen, and quality assurance methodologies.	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	
Certified Information Systems Security Professional (CISSP) Certification 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:
Ability to see information in print and/or electronically and distinguish colors.