AUBURN
Human Resources

Cybersecurity Analyst-Central

Job Description

JOB INFORMATION

Job Code	MA39
Job Description Title	Cybersecurity Analyst-Central
Pay Grade	CS02
Range Minimum	$60,150
33rd %	$76,190
Range Midpoint	$84,210
67th %	$92,230
Range Maximum	$108,270
Exemption Status	Exempt
Approved Date:	11/15/2019 6:45:00 PM
Legacy Date Last Edited	11/10/2019

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

Under general direction and supervision, utilizes information gathering, analytics aptitude, and problem solving skills to minimize and/or neutralize information and cybersecurity risks within the University network. Monitors the environment and security tools for signs of trouble. Serves as the first point of contact when a high-risk alert is issued or a suspected attack begins to affect business operations. (Employee must work in central IT unit. Exceptions require CIO prior approval.)

RESPONSIBILITIES

- Assists in enforcing and auditing information security policies and procedures such as access, breach escalation, use of firewalls, and encryption routines.
- Assists in updating, maintaining, and documenting security controls. Provides direction and support to clients and internal IT groups for information security-related issues.
- Performs administration duties of varied server technologies, enterprise systems and peripheral devices, network and security devices, and all desktop computer systems and peripherals within the last five years on market.
- Assists in performing high-level analysis of complex and disparate computing systems, networks, and data architectures to identify, rectify, and prevent technical and information security vulnerabilities.
- Performs work on critical automated processes, computer systems, networks, databases, information systems, telecommunication systems, and computer policies, procedures, and practices.
- Demonstrates high-level technical skills in the areas of information security, networking and computer systems, and excellent capacity for grasping relevant details and complex systems analysis.

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 specific discipline. Degree in IT or related field preferred.	and	3 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 specific discipline. Degree in IT or related field preferred.	and	7 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	/GED General education	and	11 years of	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber attacks.	Or

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 intermediate troubleshooting, client relations, and cybersecurity principles.	And
Ability to implement a plan to address and mitigate security vulnerabilities.	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.				And
Other	Industry recognized cybersecurity certification	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					

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
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.