Cybersecurity Analyst-Central

Job Description

JOB INFORMATION

Job Title:	Cybersecurity Analyst-Central
Auburn Title:	Analyst, Cybersecurity - Central
Job Code:	MA39
FLSA Classification:	Exempt
Salary Grade:	CS02 $57,500 - $103,500
Organizational use restricted to the following divisions:	*155 - Office of Info Technology*

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

Family Description

This job family manages or performs work associated with analysis, design, implementation, operation, deployment, and support of the organization's information technology resources (including computer hardware, operating systems, communications, software applications, data processing and security), telecommunication systems, and software/database products by internal staff, outsourcing staff, or consultants. Activities include developing information technology strategies, polices and plans; maintenance and use of information technology resources; training and supporting technology users; telecommunications network planning, operations and site acquisition; programming software/database products for sale to external customers; developing PC, online, and mobile games; and internet product management & operations.

Function Description

Responsible for managing or performing work associated with developing, communicating, implementing, enforcing and monitoring security controls to protect the organization's technology assets from intentional or inadvertent modification, disclosure or destruction including: Designing, testing, and implementing secure operating systems, networks, and databases; Password auditing, network based and Web application based vulnerability scanning, virus management and intrusion detection; Conducting risk audits and assessments, providing recommendations for application design; Monitoring and analyzing system access logs Planning for security backup and system disaster recovery.

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.)

KEY RESPONSIBILITIES

		% TIME
•	Assists in enforcing and auditing information security policies and procedures such as access, breach escalation, use of firewalls, and encryption routines.	25%
•	Assists in updating, maintaining, and documenting security controls. Provides direction and support to clients and internal IT groups for information security-related issues.	20%

•	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.	15%
•	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.	10%
•	Performs work on critical automated processes, computer systems, networks, databases, information systems, telecommunication systems, and computer policies, procedures, and practices.	10%
•	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.	10%
•	Performs other related duties as assigned by the supervisor.	10%

The above key responsibilities are representative of major duties of positions in this job classification. Specific duties and responsibilities may vary based upon departmental needs. Other duties may be assigned similar to the above consistent with the knowledge, skills and abilities required for the job. Not all of the duties may be assigned to a position and the percent of time spent on each duty varies based on department needs.

MINIMUM QUALIFICATIONS

To perform this job successfully, an individual must be able to perform the minimum requirements listed below. The requirements listed below are representative of the skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the key responisibilities.

Minimum Education and Experience

Education Level	*Field of Study*		*Years of Experience*	*Area of Experience*	
Bachelor's Degree	No specific discipline. Degree in IT or related field preferred.	And	3	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	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	Relevant IT experience in administering security measures to monitor and protect sensitive data and systems from infiltration and cyber attacks.	

Minimum Skills and Abilities

Description	*Proficiency*	
Knowledge of intermediate troubleshooting, client relations, and cybersecurity principles.	Intermediate	And
Ability to implement a plan to address and mitigate security vulnerabilities.	Intermediate	And
Ability to recognize, analyze, and solve a variety of problems.	Intermediate	And
Ability to effectively communicate technical concepts to a non-technical audience.	Intermediate	

Minimum Technology

Technology	*Technology Details*	
Strong technical aptitude and computer skills.		

Minimum Licenses and Certifications

Licenses/Certifications	*Licenses/Certification Details*	*Time Frame*	
None Required.	Industry recognized cybersecurity certification preferred.	Upon Hire	

Approved Date:	11/10/2019