Cybersecurity Eng-Central

Job Description

JOB INFORMATION

Job Title:	Cybersecurity Eng-Central
Auburn Title:	Cybersecurity Engineer - Central
Job Code:	MA40
FLSA Classification:	Exempt
Salary grade:	CS05 $74,400 - $133,900
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 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.)

KEY RESPONSIBILITIES

		% TIME
•	Ensures information security policies and procedures are followed.	15%
•	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.	15%

•	Assists with communication, reporting, and alerting on general information security issues as well as on specific assignments within Information Security tool sets.	10%
•	Develops scripts and tools to verify security platforms and automate security team operations.	10%
•	Implements new technology deployments and integration testing.	10%
•	Evaluates information security products, services, and procedures to enhance productivity and effectiveness.	10%
•	Maintains up-to-date understanding of best practices and security threats.	10%
•	Works with vendors to resolve security problems and develops infrastructure solutions.	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 specified discipline. Degree in IT or related field preferred.	And	5	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 related field preferred.	And	9	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	13	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 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.	Intermediate	And
Must have team leadership skills, negotiation skills, and advanced client relation skills.	Intermediate	And
Ability to remain up-to-date with privacy and security regulations.	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 required within six (6) months of hire date. Recognized certifications include the Certified Information Systems Security Professiona (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), CompTIA Security +, Certified Ethical Hacker (CEH), Certified in Risk and Information Systems Control (CRISC) and others as deemed appropriat by the CISO of Auburn University.	180 Days	

Approved Date: 11/10/2019