AUBURN
Human Resources

Mgr, Cybersecurity
Job Description

JOB INFORMATION

Job Code	MA73
Job Description Title	Mgr, Cybersecurity
Pay Grade	CS08
Range Minimum	$104,030
33rd %	$138,710
Range Midpoint	$156,040
67th %	$173,380
Range Maximum	$208,060
Exemption Status	Exempt
Approved Date:	1/1/1900 12:00:00 AM
Legacy Date Last Edited	9/30/2022

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

Under the direction of the Chief Information Security Officer (CISO), the Cybersecurity (Information Security) Manager assists with the development and delivery of an information security program at Auburn University. The scope of this program is university-wide, and the purpose is to protect University information and its infrastructure from threats; ensure the confidentiality, integrity, and availability of University data; and that the University complies with statutory and regulatory requirements.

Oversees and manages a team of security specialists that provide cybersecurity operations including a Security Operations Center (SOC), systems and network security monitoring, penetration testing, firewall and related infrastructure management, network traffic analysis, and cybersecurity consulting for the University community. Mentor security staff within the group. Assists with Governance, Risks and Compliance (GRC). Consults with leadership on security matters such as security frameworks, policies/procedures, and strategic planning.

RESPONSIBILITIES

- Mentors the Cybersecurity team members and implement professional development plans for all members of the team.
- The Cybersecurity Manager will provide assistance and provide guidance with Network Security to include:
  * Cybersecurity firewalls and Web Application Firewalls for on premise network and cloud environments.
  * Design and configuration of security systems including firewalls, IDS/IPS, and remote access.
  * Oversee monitoring systems for network server/firewall/network anomalies.
  * Creating infrastructure designs of current and future network designs and incorporates appropriate mitigation of existing and emerging threats.
  * Identifies security design gaps in existing and proposed network architecture and recommends changes/enhancements.
- The Cybersecurity Manager will assist with cybersecurity operations to include:
  * Lead the Security Operations Center (SOC) and ensuring continuous monitoring of Cybersecurity events.
  * Provide guidance and lead Auburn's Data Loss Prevention (DLP) Strategies and processes. Provide guidance and lead Cybersecurity awareness and training to include Phishing campaigns.
  * Provide guidance and strategic planning for Security Incident Event Management (SIEM), both in the cloud and on premise.
  * Provide and lead education and awareness programs and advise operating units at all levels on security issues, best practices, and vulnerabilities.
  * Work with campus groups such as Information Security Liaisons to build awareness and a sense of common purpose around security.
- The Cybersecurity Manager will provide assistance with Governance, Risks and Compliance by:

RESPONSIBILITIES

	* Coordinating the development of University information security technical standards, guidelines and procedures based on a recognized framework of best practices and in support of Auburn University Policies and regulations such as FERPA, CMMC, and GLBA. * Assisting with Risk Analysis and Risk Management. * Assisting with Security and Compliance reviews. * Assisting with the creation of System Security Plans (SSPs).
•	Stays fully informed of current information security issues and regulatory changes affecting higher education at the state and national level, participate in national policy and practice discussions, and communicate to campus on a regular basis about those topics. Engage in professional development to maintain continual growth in professional skills and knowledge essential to the position.

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	Full supervisory responsibility for other employees is a major responsibility and includes training, evaluating, and making or recommending pay, promotion or other employment decisions.

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	Entry into the applicant pool requires a Bachelor's degree from an accredited institution in Business Administration, Management, Computer Engineering, Computer Science, Information Systems, or a related field. Master’s Degree in information technology or directly relevant discipline preferred.	and	8 years of	Demonstrated successful experience in information technology that includes a minimum of 8 years of progressively responsible experience in information security. Must possess full or advanced proficiency and understanding of Security Operations, Security Operations Center (SOC) processes, Network Security, and Cybersecurity Governance, Risks and Compliance. Experience as a manager preferred. Experience leading projects involving multiple team members can be considered as management experience.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Demonstrated knowledge of various security and regulatory compliance standards, such as Understanding and experience with, the Family Educational Rights and Privacy Act (FERPA), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Cybersecurity Maturity Model Certification(CMMC).	
Extensive background and knowledge derived from experience in core cybersecurity and information technology concepts, and skills required at the most senior level.	
Experience in managing a cybersecurity department (preferred), technical knowledge of information technology, and cybersecurity practices and advanced degrees.	
Knowledge of project and operations management to include team leadership skills including motivating team member and group processes, team collaboration, empowering, coaching, mentoring, training, ethical integrity, championing diversity and inclusiveness, and supervising staff.	
Ability to translate specific strategic information into operational programs.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Demonstrated knowledge of cybersecurity concepts including malware, intrusion detection, risk analysis, threat/vulnerability management, system hardening, and business continuity.	
Understanding of Cybersecurity Frameworks.	
Must be able to convey goals and objectives clearly and in a compelling manner; listen effectively and clarify information as needed; produce clear status reports; communicate tactfully and candidly.	
Demonstrated ability to mentor and lead cybersecurity managers.	
Demonstrated ability to identity problems, analyze courses of action, and propose solutions.	
Knowledge of data forensics and collection technologies, disk imaging, chain of custody records, handling sensitive information preferred.	
United States Government Security Clearance desired, but not required.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
Certified Information Security Manager (CISM)		Upon Hire	Required	And
CISSP Certified Information Systems Security Professional		Upon Hire	Required	And
Certified Information Systems Auditor (CISA)		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			
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.