AUBURN
Human Resources

Exec Dir/ChiefInfoSecurity Off

Job Description

JOB INFORMATION

Job Code	MA72
Job Description Title	Exec Dir/ChiefInfoSecurity Off
Pay Grade	CS10
Range Minimum	$135,200
33rd %	$180,260
Range Midpoint	$202,790
67th %	$225,330
Range Maximum	$270,390
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

The CISO reports to the Vice President for Information Technology and Chief Information Officer (CIO) and is responsible for the overall Auburn University Cybersecurity program (information security) and the development and delivery of a comprehensive information security strategy and programs to ensure university information assets are adequately protected. The CISO will provide senior level leadership and direction to the Cybersecurity organization. The CISO will oversee ongoing activities, programs, and projects that serve to protect data confidentiality, integrity and availability while providing secure and reliable access by team members, students, faculty, staff, researchers, affiliated providers, and vendors to systems and information. Auburn operates in a distributed IT model with a central Office of Information Technology (OIT), plus distributed IT (DIT) which includes 13 colleges, the library, research, and various administrative departments. Currently the CISO will supervise a Cybersecurity Manager and a Senior Engineer/Cybersecurity Architect. The cybersecurity department is comprised of the CISO, Cybersecurity Manager, Analyst, Engineers, and Senior Engineers/Architects.

The purposes of the Cybersecurity program include:

- Ensure that information created, acquired or maintained by the University and its authorized users is used in accordance with its intended purpose.
- Protect University information and its infrastructure from both external and internal threats.
- Ensure that the University complies with statutory and regulatory requirements.

This position will work collaboratively with Auburn executives, leaders of IT, industry security executives, Distributed IT, Research, Audit, Legal and Compliance on security initiatives for the university. This leader will be responsible for aligning Cybersecurity initiatives with university programs and business objectives, ensuring that information assets and technologies are adequately protected. In addition, the CISO is tasked with overseeing security operations and a security operations center, implementing a Cybersecurity Governance, Risk and Compliance program and Network Security (Firewalls, Data Flow, etc.) controls. Overall, the CISO will develop and lead effective Cybersecurity programs for Auburn's research, academic, business, and outreach, environments.

RESPONSIBILITIES

- Responsible for the strategic leadership of the University's Cybersecurity program.
- Provides guidance and counsel to the CIO and key members of the university leadership team, working closely with senior administration, academic leaders, and the campus community in defining objectives for Cybersecurity, while building relationships and goodwill.
- Leads cybersecurity planning processes to establish an inclusive and comprehensive information security program for the entire institution in support of academic, research, and administrative information systems and technology.

RESPONSIBILITIES

- Establishes annual and long-range security and compliance goals, define security strategies, metrics, reporting mechanisms and program services; and create maturity models and a roadmap for continual program improvements.
- Stays abreast of cybersecurity 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.
- Provides senior level leadership for the Cybersecurity Office to create a strong bridge between organizations, build respect for the contributions of all and bring groups together to share information and resources and create better decisions, policies, and practices for the campus.
- Mentors the Cybersecurity team members and implement professional development plans for all members of the team.
- Develops relationships with security peers at other universities through Higher Education Security Roundtable (HE-SRT), and with peer research institutions
  nationally through REN-ISAC and equivalent institutions.
- Governance, Risk and Compliance
  - Governance: Leads the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation. Develop and maintain enterprise-wide cyber security policies that promote responsible stewardship of information assets and provide practical, economical, and workable solutions to emerging policy questions. Serve as a resource for interpreting and establishing university polices with impact on IT operations and governance. Serve as Auburn's lead on cybersecurity focused legislation.
  - Risk Assessment and Incident Prevention: Develops and implements an ongoing risk program targeting cybersecurity matters; recommend methods for vulnerability detection and remediation, and oversee vulnerability testing.
  - Risk Management: Continually evaluate risks and act expeditiously in making mitigation decisions and recommendations, while considering the technology environment as well as the varying needs and viewpoints of the university community and its unique requirements. Maintain and report regularly on the university security risk tolerance levels. Develop security plans to support information protection needs across the complete system lifecycles from design and architecture to disaster recovery and potential system retirement. Lead efforts to internally assess, evaluate and make recommendations to management regarding the adequacy of the security controls for the University's information and technology systems.
  - Incident Response Management and Operations: Oversees and directs university wide technology incident management program to effectively defend the university brand from cyber, physical loss, and network-based threat sources. Use established incident response mechanisms and policies to advise university leadership in management actions in response to cybersecurity events and incidents. Assure team members are trained to effectively establish methods and best practices for use of security tools and services.
  - Strategy Development: Using the established security governance committees, develop and promulgate a strategic vision for security services and support of the university and Auburn's missions, notably through the respective strategic plans. Assures that security initiatives address all aspects of University information technology including academic, research, and administrative efforts.
  - Coordinates and track all information technology and cybersecurity related audits including scope of external penetration test, audits, colleges/units involved, timelines, auditing agencies and outcomes. Work with auditors as appropriate to keep audit focus in scope, maintain effective relationships with audit entities and provides a consistent perspective that continually puts the institution in its best light. Provide guidance, evaluation and advocacy on audit responses.
  - Coordinates efforts with the University Compliance Officer with respect to University, state and federal information security policies and regulations. Develop a strategy for dealing with increasing number of audits, compliance checks and external assessment processes for internal/external auditors. 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), and the Federal Information Security Management Act (FISMA). Assist and support efforts for compliance with European Union (EU) General Data Protection Act (GDPR), International Traffic in Arms Regulations (ITAR) and Cybersecurity Maturity Model Certification (CMMC).
- Incident Response
  - Keeps abreast of security incidents and act as primary control point during significant cybersecurity incidents. Chair and convene the Information Security Incident Response Team (ISIRT) as needed, or requested, in addressing and investigating security incidences that arise and provide leadership for breach response.
  - Chair the Information Security Incident Response Team (ISIRT). Develop and implement an Incident Reporting and Response System to address University security incidents (breaches and data exposures), respond to alleged policy violations, or complaints from external parties. Provide guidance on necessary host isolation, forensics and remediation. Serves as the official campus contact point for information security, and incidents.
  - Develops, implements and administers technical security standards, as well as a suite of security services and tools to address and mitigate security risk.

RESPONSIBILITIES

	- Provides leadership, direction and guidance in assessing and evaluating cybersecurity risks and monitor compliance with security standards and appropriate policies. - Examines impacts of new technologies on the Institution's overall cybersecurity. Establish processes to review implementation of new technologies to ensure security compliance.
•	Outreach, Education and Training - Works closely with IT leaders, technical experts, deans and administrative leaders across campus on a wide variety of security issues that require an in-depth understanding of the IT environment and risks in their units, as well as the research landscape and federal regulations that pertain to their unit's research areas. - Coordinates the development and delivery of an education and training program on cybersecurity matters for employees, other authorized users, and students. - Champions education and awareness programs and advice operating units at all levels on security issues, best practices, and vulnerabilities. - Works with campus groups such as Cybersecurity Liaisons, SGA, Compliance to build awareness and a sense of common purpose around security. - Pursues student security initiatives to address unique needs in protecting identity theft, mobile social media security, and online reputation program.
•	Performs special projects as assigned.

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	Supervises others with full supervisory responsibility.

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	Bachelor’s Degree from an accredited institution, with a major in Computer Science, Management of Information Systems Technology, Information Technology or other directly related information technology major. Master’s Degree in information technology or directly relevant discipline preferred.	and	10 years of	Ten years of progressively increasing professional responsibility across a cybersecurity organization within a large, complex university environment. Eight of the ten years must be at a management level with direct supervision of fulltime employees that includes project planning, budgeting, and developing and implementing tiered cybersecurity strategies.	And

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Extensive background and knowledge derived from experience in core cybersecurity and information technology concepts, and skills required at the most senior level.	
Work experience should include leading a large, cross-functional work group with knowledge of security technologies, standards, and networking architectures.	
Experience in managing incident response and security operations is required.	
Experience working in an organization with matrix reporting relationships and integrated, cross-functional work teams is necessary.	
Demonstrated effectiveness in a systems development environment with concurrent tasks and changing priorities and resources.	
Some knowledge of University policies, practices, and procedures is preferable.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Advanced written and verbal communication skills and the ability to present effectively to small and large audiences of varying technical and operational backgrounds.	
Strong interpersonal skills and the ability to build effective professional relationships with a wide range of constituencies in a culturally and intellectually diverse organization.	
Ability to interact with colleagues, supervisors, and customers face to face.	
Demonstrated knowledge of security concepts including malware, intrusion detection, risk analysis, threat/vulnerability management, system hardening, and business continuity.	
Demonstrated mastery and experience with cybersecurity risk assessment and management processes and standards.	
Ability to perform deep level technical assessment of vulnerabilities to support incident investigations and system assessments.	
Demonstrated ability to mentor and lead cybersecurity managers.	
Demonstrated ability to identity problems, analyze courses of action, and propose solutions.	
Demonstrated ability to successfully handle sensitive discussions with discretion, strong personal ethics commitment, and demonstrated sound judgment.	
Consistently models high standards of honesty, openness, and respect for the individual.	
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 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).	
Knowledge of data forensics and collection technologies, disk imaging, chain of custody records, handling sensitive information preferred.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
Certified Information Security Manager (CISM)	This position requires industry-standard Information Assurance certifications appropriate to the position (Certified Information Security Manager (CISM),	Upon Hire	Required	And
CISSP Certified Information Systems Security Professional	Certified Information Systems Security Professional (CISSP) or equivalent).	Upon Hire	Required	And
Certified Information Systems Auditor (CISA)	Certified Information Systems Auditor (CISA) preferred.	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				

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
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.