Sam Houston State University

Sam Houston State University Human Resources

Staff Classification Description – Associate Vice President - Chief Information Security Officer & Chief Technology Officer

Skill Category: Executive/Administrative
Position (Employee) Class: 1M130
Grade: NC
Date: 12/2024

Department: Division of Information Technology

Educational & Experience Requirement: Master's degree in computer science, information systems, or an information technology-related field, seven years related experience. In-depth knowledge of cybersecurity principles, practices, technologies, and standards, with a proven track record in developing and implementing security strategies preferred. Strong understanding of risk management frameworks, regulatory requirements, and compliance standards relevant to the organization's industry preferred. Professional certifications such as CISSP, CISM, or CISA are highly desirable. A combination of education, experience, and training that would produce the required knowledge and abilities could be considered.

Nature & Purpose of Position: Serves as the university's strategic leader for cybersecurity, compliance, and technology infrastructure. This role integrates the oversight of information security, business technology solutions, systems, and networking, driving the evolution of the university's digital ecosystem to ensure it is secure, reliable, and scalable. The AVP-CISO/CTO oversees the Office of Information Security & Compliance, Business Technology Solutions, Systems Administration, and Networking, ensuring alignment with the university's academic, research, and administrative goals.

Supervision Given & Received: Reports to and receives direction from the Sr. Vice President for Strategic Enrollment and Innovation & the University President. Provides direct supervision to the Director of Systems, the Director of Networking, Director of Business Technology Solutions, and the Director of Cybersecurity, and other full-time technical and administrative staff. Collaborates with executive leadership and key stakeholders across the institution to ensure operational excellence, security, and innovation in technology and compliance.

Primary Responsibilities: Develops and executes a unified strategy for information security and technology, ensuring alignment with university priorities and goals. Leads governance frameworks, policies, and processes to ensure robust security, compliance, and operational efficiency. Advises executive leadership on cybersecurity and technology matters, integrating these considerations into institutional decision-making. Stays at the forefront of industry trends, emerging technologies, and regulatory requirements to anticipate risks and identify opportunities. Oversees the implementation of a comprehensive cybersecurity program to protect university assets and sensitive data. Leads the identification, assessment, and mitigation of cybersecurity risks, ensuring compliance with legal and regulatory requirements (e.g., FERPA, TPIA, GLBA, COPPA, HIPAA, PCI-DSS). Oversees incident response and disaster recovery efforts, ensuring readiness to address security breaches and operational disruptions. Promotes a culture of cybersecurity awareness across the university community through training and communication. Directs the design, deployment, and maintenance of scalable, secure systems and networking infrastructure. Guides the Director of Systems in managing server environments, cloud strategies, and hybrid solutions; the Director of Networking in developing and optimizing local and wide area networks, wireless systems, telephony, and other critical infrastructure; the Director of Cybersecurity in managing cybersecurity operations and incident response; the Director of Business Technology Solutions in business analysis initiatives and technology solutions to meet strategic priorities. Ensures integration of systems and networking operations to deliver seamless technology services across the institution. Establishes and monitors performance metrics for technology operations, identifying opportunities for optimization and growth. Oversees major technology and security initiatives, from project inception to completion, ensuring on-time delivery and alignment with strategic goals. Cultivates strong vendor and partner relationships to enhance service delivery and ensure compliance with contractual obligations. Conducts regular evaluations of the university's technology environment, recommending enhancements and identifying cost-saving opportunities. Leads and mentors cross-functional teams in security, business technology solutions, systems, and networking, fostering a culture of accountability, collaboration, and innovation. Provides professional development opportunities to team members to ensure they remain current with technology and cybersecurity advancements. Works closely with university stakeholders to align technology services with institutional needs, ensuring transparency and collaboration.

Other Specifications: Deep knowledge of cybersecurity principles, compliance frameworks, and risk management strategies. Proven experience with systems administration, cloud infrastructure, and networking technologies. Familiarity with hybrid IT environments, including on-premises and cloud-based solutions. Exceptional leadership abilities with a proven track record of managing diverse teams and driving organizational change. Strong analytical and problem-solving skills, with the ability to make sound decisions under pressure. Excellent communication skills, capable of translating complex technical concepts for a variety of audiences. Ability to anticipate future technology trends and align them with university objectives. Skilled in fostering partnerships across organizational boundaries. Expertise in designing and implementing robust systems to ensure continuity of operations. Ability to leverage emerging technologies to enhance university operations.

This position may be designated as a Campus Security Authority (CSA).

This is a classification description with the complete list of job duties being maintained at the departmental level. Other job duties necessary for the effective operation of the University are expected to be performed. Any qualifications to be considered as equivalents in lieu of stated minimums require the prior approval of Human Resources.

Sam Houston State University is an at will employer and drug free/smoke free workplace. All positions at Sam Houston State University are considered security sensitive requiring background checks in accordance with education code 51.215, and drug testing as required by D.O.T. for safety sensitive positions. The pay grade range is inclusive of social security benefit replacement pay.

Sam Houston State University is Committed to Equal Opportunity in Employment and Education.