Sam Houston State University Human Resources

Staff Classification Description – Cybersecurity Analyst III

Skill Category: Professional
Position (Employee) Class: 3N447 (E1)
Grade: 22
Date: 5/2018

Department: Information Security

Educational & Experience Requirement: Bachelor's degree from an accredited four-year college or university with major coursework in cybersecurity, information technology security, computer engineering, computer information systems, computer science, management information systems, or a related field. Four years of experience in cybersecurity analysis, information security analysis, or digital forensics plus two additional years of relevant experience. A combination of education, experience, and training that would produce the required knowledge and abilities could be considered.

Nature & Purpose of Position: Performs highly advanced and/or supervisory (senior-level) cybersecurity analysis work. Work involves protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services.

Supervision Given & Received: Works under minimum direction, with extensive latitude for the use of initiative and independent judgment. May plan, assign, and/or supervise the work of others.

Primary Responsibilities: Monitors and analyzes cybersecurity alerts from cybersecurity tools, network devices, and information systems. Monitors and maintains cybersecurity infrastructure and/or policies and procedures to protect information systems from unauthorized use. Performs vulnerability scans of networks and applications to assess effectiveness and identify weaknesses. Performs forensic analysis of information systems and portable devices and forensic recovery of data using assessment tools. Evaluates network and system security configuration for best practices and risk-based access controls. Evaluates cybersecurity and privacy legislation, regulations, advisories, alerts, and vulnerabilities. Reviews, develops, and delivers cybersecurity awareness training. Researches and implements new security risk and mitigation strategies, tools, techniques, and solutions for the prevention, detection, containment, and correction of data security breaches. Identifies and evaluates new cybersecurity technologies to remediate vulnerabilities. Advises management and users regarding security procedures. Recommends and manages implementation of corrective actions. Performs other related duties as assigned.

Other Specifications: Requires a demonstrated ability to establish congenial work relationships and to communicate effectively within department or work-group, throughout the university with professional or managerial staff, and with outside vendors. Interprets and implements complex policies, laws, and standards relating to information security affecting the department or university level. Knowledge of the limitations and capabilities of computer systems and technology; of operational support of networks, operating systems, Internet technologies, databases, and security infrastructure; of cybersecurity and information security controls, practices, procedures, and regulations; and of incident response program practices and procedures. Skill in the use of a computer and applicable software; and in configuring, deploying, and monitoring security infrastructure. Ability to resolve complex security issues in

diverse and decentralized environments; to plan, develop, monitor, and maintain cybersecurity and information technology security processes and controls; to communicate effectively; and to plan, assign, and/or supervise the work of others. During emergencies, operational failures, and peak use periods, employee may be called in when off shift to work an extended shift. Special procedures sometimes require extended hours. Some travel is required.

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. This position is security-sensitive and thereby subject to the provisions of the Texas Education Code §51.215, which authorizes the employer to obtain criminal history record information. 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.