Security Engineer

Category: **Exempt**
Pay Grade: **E26**
Job Code: **14679**

To perform this job successfully, an individual must be able to perform the essential job functions satisfactorily. Reasonable accommodations may be made to enable individuals with disabilities to perform the primary job functions herein described. Since every duty associated with this position may not be described herein, employees may be required to perform duties not specifically spelled out in the job description, but which may be reasonably considered to be incidental in the performing of their duties just as though they were actually written out in this job description.

JOB SUMMARY

Performs professional strategic information technology work which requires an incumbent to produce expert analytical, technical, and administrative work products to protect the confidentiality and integrity of customer and employee data and ensures compliance with organization policies. The incumbent is required to develop a security strategy, maintain a supporting policy in line with IT Security best practice and governance, and define supporting cybersecurity tasks, methods and procedures involving reporting, auditing, disaster recovery/service continuity, and investigations. The incumbent identifies and resolves complex work problems of a nature that lower level employees are unable to solve or overcome. Work requires creative and original thinking and is performed under the general direction of the Cyber Security Manager with extensive latitude for individual and team initiative, judgment, and discretion in working with customers to determine hardware, software, and system functional requirements to maintain operations, productions, as well as achieve business objectives.

ESSENTIAL JOB FUNCTIONS (examples, not all inclusive)

- Demonstrates expert-level proficiency in two or more of the departmental section disciplines: Security Program Management, Vulnerability Management, Risk Management, Security Policy Management, Security Awareness, Incident Response, Enterprise Security Monitoring, Penetration Testing, Compliance and Auditing, Application Design, Network Design, Perimeter Defense Design, Enterprise Architecture, Configure and maintain all facets of the security infrastructure, Troubleshoot and resolve complex security issues;
- Demonstrates expert-level job knowledge, quality, dependability, judgment, communications and initiative, with demonstrated expert-level proficiency in meeting design specifications of computer systems, programs and operating systems, with the following core competencies: Analysis, Design, Business Process Improvement, Data Modeling, Development, Planning, Implementation, Test Script Development, Monitoring/Controls, Troubleshooting/Problem Solving, Documentation, and Service Motivation;
- Demonstrates leadership that fosters commitment, team spirit, pride and trust through coaching, mentoring, recognizing and guiding employees to achieve results through others. Uses interpersonal skills to influence and inspire others to follow. Facilitates and fosters open communication and cooperation within the organization and with customer groups to build an effective team environment. Acts as a catalyst for organizational change that fosters a quality of service essential to high performance. Has the ability to see things not as they are, but as they can be; and is able to motivate and influence others to translate vision into actions and meaningful contributions that drive performance to higher levels of effectiveness and productivity;
- Self-motivates, manages, and performs personal daily activities and multiple complex projects under the discipline of defined departmental business processes;
- Prepares and takes responsibility for project plans/schedules, and outlines requirements, tasks, work assignments, resources and critical milestones, with a demonstrated ability to prioritize tasks for both self and others;

- Identifies and analyzes complex problems; distinguishes between relevant and irrelevant information to make logical decisions; provides solutions to individual and organizational problems;
- Takes ownership of complex cross-sectional problems and leads a team to resolution with an appropriate sense of urgency;
- Communicates effectively, both verbally and in writing, to peers, management and customers at various levels of the organization. Prepares and delivers presentations regularly to various audiences using clear, concise and effective communication;
- Performs assessments and evaluations of employee performance as required;
- Performs other related job duties as assigned.

QUALIFICATIONS

Education and Experience:

Eight (8) years of technical and professional experience in information technology that includes customer service and two (2) years of professional team leadership or supervision in the assigned subject matter tasks; or; an Associate degree in information technology, computer science, computer technology, or related field and six (6) years of experience as described above; or a Bachelor's degree in information technology, computer science, computer technology, or related field and four (4) years of experience as described above; or; an equivalent combination of education, training, and/or experience.

Special Qualifications (May be required depending on area of assignment):

- CISSP: Certified Information Systems Security Professional
- CCRI: Command Cyber Readiness Inspection
- GSLC: GIAC Security Leadership Certification
- SSCP: ISC Systems Secured Certified Practitioner
- OSCP: Offensive Security Certified Professional
- Florida Driver's License or Florida Commercial Driver's License and endorsement, if any.
- Assignment to work a variety of work schedules including compulsory work periods in special, emergency, and/or disaster situations.
- Candidate to demonstrate competence and/or possess certifications in one or more specific IT functions.
- Acquire and maintain CJIS Certification.
- Other highly desirable knowledge, skills, abilities, and credentials relevant to a position.

Knowledge, Skills and Abilities:

- Knowledge of configuring and monitoring security technologies such as firewalls, intrusions detection, SIEM, honeypots;
- Knowledge of implementing vulnerability management and penetration testing tools;
- Knowledge of implementing anti-malware, anti-virus, web filtering, application control, and data leakage protection;
- Knowledge of application protection technologies and secure development concepts;
- Knowledge of performing risk assessments and IT audits;
- Knowledge of performing network and web application penetration testing;
- Knowledge of creating security policies and best practices;
- Knowledge of PCI, HIPAA and CJIS compliance requirements;
- Knowledge of confidentiality, integrity, and availability security principles;
- Knowledge in standard office practices, procedures, policies, personal computers, operating systems and related software applications. Recommends changes to improve operational efficiencies;
- Knowledge in managing personal daily activities and complex projects for self and others that may cross organizational boundaries;
- Knowledge in the use and application of reference materials to research and solve complex problems;
- Knowledge in the application of theory in resolving complex problems;
- Knowledge in applying new technologies, soft skills and procedures;
- Ability to mentor teammates, lead teams, and facilitate groups to achieve success through others;

- Ability to prepare and deliver effective presentations at various levels;
- Ability to use diplomacy in dealing with difficult customers and delivery of services;
- Ability to communicate effectively, both verbally and in writing, with peers and others;
- Ability to communicate with tact, patience and courtesy at all levels of the organization;
- Ability to assist lower level personnel with training of new technologies;
- Ability to establish and maintain effective work relationships, both inside and outside of the work section;
- Ability to self-develop relevant job-related skill(s) for current and future roles;
- Ability to understand, follow, and to provide specific instructions, priorities, policies and procedures;
- Ability to identify, to take ownership of, and to troubleshoot and solve complex problems.

PHYSICAL/MENTAL DEMANDS

The work is sedentary work which requires exerting up to 10 pounds of force occasionally and/or negligible amount of force frequently or constantly to lift, carry, push, pull, or otherwise move objects, including the human body. Additionally, the following physical abilities are required:

- Fingering: Picking, pinching, typing, or otherwise working, primarily with fingers rather than with the whole hand as in handling.
- Visual ability: Sufficient to effectively operate office equipment including copier, computer, etc.; and to read and write reports, correspondence, instructions, etc.
- Hearing ability: Sufficient to hold a conversation with other individuals both in person and over a telephone; and to hear recording on transcription device.
- Speaking ability: Sufficient to communicate effectively with other individuals in person and over a telephone.
- Mental acuity: Ability to make rational decisions through sound logic and deductive processes.
- Talking: Expressing or exchanging ideas by means of the spoken word including those activities in which they must convey detailed or important spoken instructions to other workers accurately, loudly, or quickly.
- Repetitive motion: Substantial movements (motions) of the wrist, hands, and/or fingers.
- Walking: Moving about on foot to accomplish tasks, particularly for long distances or moving from one work site to another.

WORKING CONDITIONS

Work is performed in a dynamic environment that requires sensitivity to change and responsiveness to changing goals, priorities, and needs.