SOUTHWESTERN COMMUNITY COLLEGE DISTRICT

CLASS TITLE: IT SECURITY ANALYST/PROJECT COORDINATOR

SUMMARY DESCRIPTION

Under general direction, provide technical advice, coordination, and planning in support of technology projects and initiatives of considerable scope and complexity; design, develop, test, install, monitor, and maintain information technology security systems for the District; and provide advanced guidance to technologists and systems users in system security best practices.

DISTINGUISHING CHARACTERISTICS

This class is distinguished by its regular and ongoing responsibility for providing advanced guidance to technologists and systems users in system security best practices as well as managing projects of considerable scope and complexity while ensuring established security requirements are met. Incumbents within this classification have strong experience that enables the ability to exercise project management skills, work independently with minimal direction, perform complex analyses, establish and follow industry best practices, and implement appropriate solutions.

REPRESENTATIVE DUTIES

The following duties are typical for this classification. Incumbents may not perform all of the listed duties and/or may be required to perform additional or different duties from those set forth below to address business needs and changing business practices.

1. Initiate, coordinate, and enforce policies and procedures in support of best practices for systems infrastructure security and change management; maintain quality service by establishing and enforcing organization standards. ***E***

2. Ensure satisfactory information technology project results by communicating project expectations, coordinating resources and timetables, planning, monitoring, and appraising results; ensure systems security is carefully maintained through all project implementations. ***E***

3. Maintain organizational effectiveness and efficiency by defining, delivering, and supporting strategic, operational, and security plans related to information technologies. ***E***

4. Coordinate troubleshooting and resolution of technology security related incidents in a timely manner; coordinate team efforts to research, select, plan, implement, and support effective technology security controls, monitors, and practices to reduce or eliminate security-related incidents. ***E***

5. Define and deliver audits for information technologies and related data sources; recommend information technology strategies, policies, and procedures by evaluating organization outcomes, identifying problems, evaluating trends, and anticipating requirements; recommend procedural changes to enhance systems and data security and integrity. ***E***

6. Preserve assets by implementing disaster recovery and back-up procedures as well as information security and control structures. ***E***

7. Maintain professional and technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks, benchmarking state-of-the-art practices, and participating in professional societies. ***E***

8. Contribute to team effort by accomplishing related results as needed; develop project plans; guide, plan, educate, and review the assignments of staff responsible for implementing technology projects. ***E***

9. Develop, implement, audit, and guide on security systems in support of a secure technology infrastructure; maintain vendor contacts, partnerships, and relationships in support of the secure infrastructure. ***E***

10. Perform related duties and responsibilities as required.

KNOWLEDGE AND ABILITIES

Knowledge of:

Project management body of knowledge (PMBOK) including processes, best practices, terminologies, and guidelines.
Multiple operating systems including recent desktop and server versions of Microsoft Windows, Mac OS, and distributions of Linux.
IT architecture including data centers, cloud deployment, containers, network distribution points, and wireless technologies.
Networking concepts including routing and switching concepts, Ethernet, wireless networking, TCP/IP, and NetBIOS.
Programming or scripting in at least one language such as Python, PHP or Powershell.
Security protocols including WPA/WPA2, Kerberos/AD, IPSEC, SSL/TLS, and SSH.
Security assessment and scanning tools such as Nessus, Nmap, oclHashCat, Kali.
Detection and monitoring tools including network-based IDS/IPS software and appliances as well as endpoint detection and response software.
Computer forensics and incident response tools and procedures.
Security standards and frameworks such as NIST, PCI-DSS, OWASP, or CIS Critical Security Controls.
"Network of Things" concepts.
Methods and techniques of research, analysis, and decision-making.
Principles of process documentation.
Oral and written communication skills.
Customer service principles and practices.
Basic principles and practices of providing work guidance to staff.

Ability to:

Effectively interact and negotiate with vendors.
Assess and remedy system performance problems.
Troubleshoot and resolve complex hardware and software problems.
Perform complex analyses, establish and follow industry best practices, and implement appropriate solutions.
Research, compile, assemble, analyze, and interpret data from diverse sources.
Exercise leadership skills.
Plan, organize, implement, and complete complex IT security projects.
Prepare and follow work plans and timelines for projects and tasks.
Work independently with little direction.
Adapt to changing technology and quickly learn functionality of new applications and systems.
Work with and exhibit sensitivity to and understanding of the diverse racial, ethnic, disabled, sexual orientation, and cultural populations of community college students.

Communicate clearly and concisely, both orally and in writing.
Establish and maintain effective working relationships with those contacted in the course of work.

EDUCATION AND EXPERIENCE

Any combination equivalent to: A Bachelor's degree in computer science, information technology, or a related field and three years of experience in a system administration, IT security, or a project management role, **OR** at least two years of college level course work in computer science, information technology or a related field and five years of experience in a system administration, IT security, or a project management role.

DESIRABLE QUALIFICATIONS

One or more relevant technical security certifications such as the CCNA: Security, Offensive Security Certified Professional (OSCP), or a SANS certification. At least two years of experience in an IT security role.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential job functions.

Environment: Work is performed primarily in a standard office setting with frequent interruptions and distractions; extended periods of time viewing computer monitor; possible exposure to dissatisfied individuals.

Physical: Primary functions require sufficient physical ability and mobility to work in an office setting; to stand or sit for prolonged periods of time; to occasionally stoop, bend, kneel, crouch, reach, and twist; to lift, carry, push, and/or pull light to moderate amounts of weight; to operate office equipment requiring repetitive hand movement and fine coordination including use of a computer keyboard; and to verbally communicate to exchange information.

Vision: See in the normal visual range with or without correction.

Hearing: Hear in the normal audio range with or without correction.

Created: July, 2019
Forsberg Consulting Services