EL CAMINO COMMUNITY COLLEGE DISTRICT

CLASS TITLE: INFORMATION SECURITY SPECIALIST

BASIC FUNCTION:

Under the direction of a designated supervisor, manager or Director, incumbents assigned to this classification ensure the secure operation of the in-house computer systems, servers, and network connections. Information Security Specialist will assist in detecting, investigating, and defending against information security incidents targeting the College's IT systems and data. This includes checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting. The incumbent will also analyze and resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user activity audits where required.

REPRESENTATIVE DUTIES:

Acts as Project Manager on information security projects.

Evaluates new systems and products for security monitoring and response.

Assesses the need for security reconfigurations (minor or significant) and executes them as required.

Monitors and maintains current knowledge of emerging security alerts, issues, threats and trends.

Conducts research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.

Builds and maintains tolls, flags and triggers in order to proactively monitor and respond to emerging threats.

Conducts technical assessments of information security incidents, including malware analysis, packet level analysis, and system level forensic analysis.

Coordinate and provide technical updates to management throughout incident management cycles.

Develops and conduct Security Awareness training for staff and faculty.

Deploys and maintains security systems and corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems and antivirus software.

Recommend, schedule and apply fixes, security patches, disaster recovery procedures, and any other measures required in order to address security breaches.

Develops and implements enforcement policies, procedures and associated plans for system security administration and user system access based on industry-standard best practices.

Designs, implements, and reports on IT Security performance results, audits, and recommendations and end user activity audits.

Performs other related duties as assigned.

KNOWLEDGE AND ABILITIES:

KNOWLEDGE OF:

Design, development, and implementation of software systems, applications, and related products.

Systems planning, security principles, functional shell code fundamentals, and general software management best practices.

Current software protocols, and Internet standards, including TCP/IP, HTML, AJAX, JavaScript, and XML, Regular Expressions, Wiki Markup, SQL, Linus, IOS, Perl, Python, Bash, and PHP programming languages.

Software troubleshooting experience.

Testing, flowcharting, and data mapping tools and procedures.

Demonstrated knowledge of applicable practices and laws relating to data privacy and protections.

Well versed in multiple security technologies such as SIEM; Intrusion Detection Systems; End-point security; Web Proxy/Content Filtering; Active Directory, PKI, Radius, Log Analysis, etc.

Broad knowledge of business-impacting security scenarios and viable methods to detect these scenarios.

ABILITY TO:

Conduct research into security issues and products as required.

Analyze, conceptualize, and problem solve.

Participate in ongoing training and certification to maintain and develop technical skills.

Understand the District’s goals and objectives.

Communicate effectively, both orally and in writing.

Apply strong interpersonal and consultative skills.

Prioritize and execute tasks in a high-pressure environment.

Work in a team-oriented, collaborative environment.

Respond to common inquiries or complaints from District staff, regulatory agencies, or members of the business community.

Present information to senior and executive management, public groups, and or board of trustees.

EDUCATION AND EXPERIENCE:

Bachelor's degree in Computer Science, Computer Engineering, IT, or other related field and 3 years of IT security related work experience or additional work experience equivalency as noted below.

Additional related work experience in lieu of education requirement:

Three (3) years related work experience **PLUS** an additional two (2) years for every one year of related college education requirement noted above.

Example: No related college degree = 3 yrs. related work experience **PLUS** another 8 years in lieu of 4-year degree requirement.

LICENSES AND CERTIFICATIONS:

Current valid California Driver's License

WORKING CONDITIONS:

Typical office environment.
Extensive computer work.
Long periods of standing and sitting.
Move from one location to another as needed.
Lift and carry up to 25 pounds.

Classified Salary Range: 49
Board Approved: March 21, 2016