SJECCD Human Resources Office

San Jose · Evergreen Community College District
Classified Job Description

Position: Information Security Analyst

Department: Information Technology Services & Support (ITSS)

Location: District Office

Date: December 13, 2023

POSITION PURPOSE

Reporting to Executive Director, ITSS or an assigned administrator, the Information Security Analyst performs complex work related to the District's information security program including testing, analysis and evaluation of the integrity and confidentiality of enterprise systems, network, assets and communication technology throughout the District. The position monitors security systems and conducts periodic risk assessments to identify, troubleshoot, diagnose, resolve and report security problems and breaches; assists in coordinating and conducting investigations involving District technology resources, and assists with security awareness training.

DISTINGUISHING CHARACTERISTICS

This position focuses on threat and vulnerability management with exposure and support on all aspects of the cybersecurity practice. Incumbent in this position should have advanced knowledge on risk identification, protection and compliance, threat detection, incident response plan development and annual review, and recovery services to achieve business resilience.

KEY DUTIES AND RESPONSIBILITIES:

1. Analyze, evaluate and implement security applications, policies, standards and procedures intended to prevent the unauthorized use, disclosure, modification, loss or destruction of data; work with the campus community and other staff to ensure the integrity and security of the information technology infrastructure.

2. Lead the development, testing and implementation of information security products and control techniques in all locations throughout the District.

3. Work with campus and district technology teams to ensure the security of all applications and assets.

4. Monitor and review security systems and logs. Identify, troubleshoot, diagnose, resolve, document and report security problems and incidents; help coordinate and conduct investigations of suspected breaches; respond to emergency information security situations.

5. Collaborate with application programming team and other IT staff to ensure production applications meet established security policies and standards.

6. Assist with training and education on information security and privacy awareness topics for District administrators, faculty and staff; assist in the development of appropriate security-incident notification procedures for District management.

7. Work with vendors to conduct vulnerability assessments to identify existing or potential electronic data and assets compromises and their sources; participate in investigative matters with appropriate law enforcement agencies.

8. Perform audits and periodic inspections of District information systems to ensure security measures are functioning and effectively utilized and recommend appropriate remedial measures to eliminate or mitigate future system compromises.

9. Review, evaluate, and recommend software products related to IT systems security, such as virus scanning and repair, encryption, firewalls, internet filtering and monitoring, intrusion detection, etc.

10. Monitor and maintain the District's security event information system (SEIM) and data loss prevention software.

11. Manage security systems and policies including but not limited to servers, firewalls, email security, and Microsoft 365 environment.

12. Recommend and implement security policies, protocols, practices and lead in creation of security training and guidance to staff.

13. Assist in the secure management and maintenance of the District's network authentication systems for wired and wireless network access.

14. Review security practices and controls of third-party service providers that handle District sensitive data, and review security controls and features of third-party software systems.

15. Ensure that maintenance, configuration, repair and patching of systems occurs on a scheduled and timely basis utilizing best practices in change management and consistent with policies and procedures.

16. Keep current with latest emerging security issues and threats through list servers, blogs, newsletters, conferences, user groups, and networking and collaboration with peers in other institutions.

17. Perform other duties reasonably related to the job classification.

EMPLOYMENT STANDARD

Knowledge of:

1. Compliance and industry cybersecurity standards frameworks such as NIST 800 and ISO standards.

2. Emerging technologies and the possible impact on existing information systems, instructional processes and business operations.

3. Incident response best practices and software license compliance laws.

4. Troubleshooting tools for computing hardware, servers and network equipment including but not limited to switches, routers, and firewalls.

5. Enterprise resource planning systems, Microsoft 365 and Active Directory and Azure Active Directory.

6. Principles of program design, coding, testing and implementation.

7. Advanced knowledge of desktop and server operating systems including Windows and Linux.

8. Disaster recovery and backup including business continuity planning.

9. Principles of training, support, and services to end-users.

10. General research techniques and data driven analytics.

11. Modern office administrative practices and use of tools including computers, websites and other applications related to this job.

Skills and Ability to:

1. Apply current NIST and ISO standards to current operations.

2. Respond to incidents and events in a timely manner.

3. Prepare clear and concise system documentation and reports.

4. Prioritize assigned tasks and projects.

5. Communicate complicated technical issues and the risks they pose to stakeholders and management.

6. Establish and maintain effective and cooperative working relationships with others.

7. Analyze situations accurately and adopt effective course of action.

8. Coordinate, develop, and implement projects.

9. Work with attention to detail and independently with minimum supervision.

Experience and Education:

1. A Bachelor's degree from an accredited institution with major course work in computer information systems, computer science, business administration, or related field.

2. Two years of experience performing information security duties, which may include implementing, overseeing, and/or managing information security technologies, process, or programs, including identification, protection, detection, response, and recovery activities.

3. Demonstrated sensitivity, knowledge, and understanding of the diverse academic, socioeconomic, gender identify, sexual orientation, cultural, disability, and ethnic backgrounds of the individuals we serve and sensitivity to and knowledge and understanding of groups historically underrepresented, and groups who may have experienced discrimination.

Certification:

1. Professional security or privacy certification, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or other similar credentials.

WORKINGS CONDITIONS

Physical Demands:

1. Must sit for long periods of time, use hands and fingers to operate an electronic keyboard, reach with hands and arms, and speak clearly and distinctly to ask questions and provide information, hear and understand voices over telephone and in person.

2. The physical demands described here are representative of those that must be met by an individual to successfully perform the essential functions of this job. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.

Board Approved: 12/12/2023
Salary Range: 150
EEO Category: 2B2 – Non-faculty/Other Professionals