SAN MATEO COUNTY COMMUNITY COLLEGE DISTRICT

Cañada College ◆ College of San Mateo ◆ Skyline College

GENERIC POSITION DESCRIPTION

INFORMATION SECURITY OFFICER

A Classified Supervisory Position (Exempt Status)
Grade 193E – Salary Schedule 35

A. Who We Are

The San Mateo County Community College District is committed to achieving educational equity for all students. As outlined in the District's Strategic Plan, "success, equity, and social justice for our students are longstanding goals." The District's "Students First" Strategic Plan is focused on "Student Success, Equity and Social Justice." We provide students with a rich and dynamic learning experience that embraces differences — emphasizing collaboration and engaging students in and out of the classroom, encouraging them to realize their goals, and to become global citizens and socially responsible leaders. When you join our team at San Mateo County Community College District, you can expect to be part of an inclusive, innovative and equity-focused community that approaches higher education as a matter of social justice that requires broad collaboration among faculty, classified staff, administration, students and community partners.

B. The College and the District

The San Mateo County Community College District is home to Cañada College, College of San Mateo, and Skyline College. All three of our colleges are designated as Hispanic Serving Institutions enrolling approximately 33,000 students each academic year. San Mateo County Community College District has a diverse student population that is a reflection of the communities that it serves. Detailed information about the student population, including data related to student success, can be found on the San Mateo County Community College District's Educational Services & Planning website.

C. Who We Want

We value the ability to serve students from a broad range of cultural heritages, socioeconomic backgrounds, genders, abilities and orientations. Therefore, we prioritize applicants who demonstrate they understand the benefits diversity brings to a professional educational community. The successful candidate will be an equity-minded individual committed to collaborating with faculty, classified staff, administration, students and community partners who are also committed to closing equity gaps. The San Mateo County Community College District seeks employees who value mentorship and working in a collegial, collaborative environment, guided by a commitment to helping all students achieve their educational goals.

D. The Position

Under general direction of the Chief Technology Officer, the Information Security Officer is responsible for the coordination of the development, implementation and evaluation of information technology (IT) security standards, best practices, architecture and systems for the district to ensure the integrity and security of the district's IT infrastructure and the protection, integrity and confidentiality of information assets spanning the entire enterprise; and perform related duties as assigned. Public contact is extensive and involves staff at all levels within the organization, other educational institutions, governmental, business and community agencies, students and the

general public for the purpose of exchanging technical and other information related to security. A high degree of independent judgment and creativity is required to resolve a variety of minor and potentially major problems that occur. Consequences of errors in judgment can be costly in employee time, public relations and/or institution funding.

E. Duties & Responsibilities

The duties below are representative of the duties of the classification and are not intended to cover all of the duties performed by the incumbent(s) of any particular position. The omission of specific statements of duties does not exclude them from the position if the scope of work is similar, related to, or a logical assignment to this classification.

1. Develop and implement security applications, policies, standards and procedures intended to prevent the unauthorized use, disclosure, modification, loss or destruction of data; works with the Infrastructure Systems Engineer, System Administrators, Managers, Directors, campus community and other staff to ensure the integrity and security of the department's IT infrastructure; reviews the development, testing and implementation of IT security products and control techniques in all locations and departments throughout the district.

2. Monitor & review security systems, logs. Identify manager, troubleshoot, diagnose, resolve and report IT security problems and incidents; help coordinate and conduct investigations of suspected breaches in IT Security; respond to emergency IT security situations.

3. Consult with application developers and other Academic Information Services staff to ensure production applications meet established IT security policies and standards.

4. Promote and coordinate the development of training and education on IT security and privacy awareness topics for district administrators, faculty and staff; develop appropriate security-incident notification procedures for district management.

5. Conduct vulnerability assessments to identify existing or potential electronic data and information system compromises and their sources; coordinate IT investigative matters with appropriate law enforcement agencies.

6. 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.

7. 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.

8. Good understanding of cloud systems & architecture such as Azure, OCI & AWS. Should have the ability to conduct vulnerability scanning & log analysis, etc.

9. Maintain up-to-date technical knowledge by attending educational workshops, reviewing professional publications, establishing personal networks and participating in professional associations.

10. May participate in the review of IT facility acquisition, construction and remodeling projects to ensure conformity to established security policies and guidelines.

11. May serve as a witness or subject-matter expert for the department in legal matters concerning IT systems security.

12. Perform other duties as assigned by the Chief Technology Officer

F. Minimum Qualifications

- A combination of education and experience equivalent to a Bachelor's degree from an accredited institution in computer science, information technology, systems engineering or a closely related field
- Five years of increasingly responsible experience involving applications and/or IT infrastructure systems, including three or more years of IT security-related experience involving risk identification and mitigation, security architecture development and compliance; or an equivalent combination of training and experience.
- Demonstrated cultural competence, sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty, and staff
- Experience in a public agency is preferred
- Certifications such as CISSP, CISM, GIAC is preferred

G. Physical/Other Requirements

This classification requires sitting and standing for periods of time, oral and written communication, keyboarding for significant portions of the workday, pushing, pulling, bending, stooping, reaching, patience and tact in order to perform the essential functions.

F. Knowledge, Skills & Abilities

1. Knowledge of current trends and advancements in enterprise-wide technology security management, including IT security risk identification and mitigation.
2. Knowledge of information systems security architecture and compliance.
3. Knowledge of disaster recovery planning and testing, auditing, risk analysis and business continuity planning.
4. Knowledge of advanced IT security and IT audit concepts and techniques.
5. Knowledge of enterprise operating systems.
6. Knowledge of information systems and architecture used in a college setting.
7. Knowledge of OSI model layer networking technologies and concepts.
8. Knowledge of server virtualization technologies.
9. Knowledge of safety policies and safe work practices applicable to the work.

1. Ability to assess IT security in both central (District Office) and college environment.
2. Ability to assist in developing local architectures and security solutions.
3. Ability to conduct timely investigations and responses to computer security-related incidents and threats including viruses, worms and other system compromises.
4. Ability to ensure compliance with all federal, state and local legislation related to information security.
5. Ability to provide comprehensive information security awareness and training.
6. Ability to assist with investigations initiated by internal and external authorities.
7. Ability to monitor and identify any anomalous traffic and compromised systems on campus networks.

8. Ability to work with other Academic Information Services staff to deploy anti-virus and other security-related desktop system software for campus-wide use.
9. Ability to communicate effectively, both orally and in writing.
10. Ability to demonstrate sensitivity to and understanding of diverse academic, socioeconomic, cultural, ethnic and disability issues.
11. Ability to establish and maintain effective working relationships with those encountered in the course of work.

(12/2021)