Technology and Data Security Analyst
San Diego Community College District

Job Title	Technology and Data Security Analyst
Department	Information Technology
Institution	San Diego Community College District
	San Diego, California
Date Posted	Jun. 7, 2024
Application Deadline	07/05/2024
Position Start Date	Available immediately
Job Categories	Professional Staff
Academic Field(s)	Information Technology
Apply Online Here	https://apptrkr.com/5310447
Apply By Email	

Job Description

Image not found or type unknown

Technology and Data Security Analyst

San Diego Community College District

Closing Date: 7/5/2024

Position Number: 00120546

Location: District

Position Type:

Technology and Data Security Analyst
San Diego Community College District

Classified

The Position:
Posting Details (Default Section)

Closing Date: 07/05/2024

Open Until Filled: Yes

Classification Title: Technology and Data Security Analyst

Working Title: Technology and Data Security Analyst

Location: District

Pay Information

Range M ($7,515.15- $12,546.85) per month based on the 2023 Supervisory and Professional Employees' Association - Salary Schedule B

New employees will begin on Step A ($7,515.15). Promoted or transferred employees will be placed as specified in the CBA. The District offers a comprehensive fringe benefit package including employer paid: medical, dental, and vision plans; sick and vacation leave; and opportunities for professional development. Initial Salary Placement, Promoted or transferred employees will be placed as specified in the SPAA - Supervisory & Professional Administrators Association Handbook. This position is FLSA Exempt and may not accrue overtime. A temporary probationary period will be applied to the employee entering this assignment. The SDCCD Employment Web Page provides a link to employee collective bargaining agreements and handbooks, and more information about terms and conditions of employment to include salary and benefits.

Position Equivalent FTE: 1.0 FTE

No. Months: 12 months

Position Number: 00120546

FLSA Status: Exempt (does not accrue overtime)

Position Type: Classified

Technology and Data Security Analyst
San Diego Community College District

Bargaining Unit: Supervisory & Professional

Range: M

Department: Information Technology

The Position

Applications are currently being accepted for a Technology and Data Security Analyst in the Information Technology Services department, located at the San Diego Community College District. Hours are M-F 8 am to 5 pm. Selected candidate must be willing to adjust work days/hours based on the department's needs.

Please note that an employee may be transferred to any site at the option of the Chancellor.

Classification Description: Click **here** for description.

Desired Qualifications

Knowledge, skills and abilities:

- Network and server architecture and design including firewalls, routing, switching, operating systems, applications, access control, and data transmissions.
- Security assessment and testing tools.
- Technical sources of information for vulnerability alerts and advisories, security threat intelligence, and computer security standards, trends, and developments.
- Federal, state, and local regulations and guidelines related to information security such as HIPAA, FERPA, FISMA, NIST, SOC2 and GLBA Principles and methods of risk management and analysis as applied to technology and information security.
- Principles of data management, including data replication, retention, and security controls.
- Methods and techniques of technical documentation and record keeping.
- Principles of training.

Ability to:

- Conduct vulnerability audits, forensic investigations, and risk management assessments.
- Detect, investigate, and analyze threats and emergency security incidents.

- Respond immediately to security-related incidents and provide a thorough post-event analysis.
- Evaluate controls and procedures to mitigate risks, hazards, and threats to IT systems and their operation.
- Monitor internal and external policy compliance. Manage personal and institutional data per legal, regulatory, administrative, and contractual requirements.
- Consistently use and promote professional standards and practices related to assignments.
- Actively contribute to a culture of constructive collaboration and innovation with colleagues.
- Maintain high levels of customer service and satisfaction.
- Provide effective and timely liaison among management, programmers, security team staff, and auditors on IT security issues and activities.
- Effectively communicate highly technical information accurately, concisely and in understandable terms, both orally and in writing.
- Foster a culture of constructive and effective collaboration and innovation within the architecture, solution designers, operations team, and other functions.
- Train technical staff in the application of information security concepts and practices.
- Stay abreast of current trends and technical advancements in the area of information security and apply knowledge to solving complex problems.

Hardware and Software Environment

- Microsoft 365, Azure, Microsoft Windows Server, Extreme Network Routing, Switching, Wireless Access Points and Controllers, Microsoft Defender for Endpoint, Microsoft End-Point Manager/InTune, Apple imaging and device administration.

Required Education, Training and Experience

- Bachelor's degree from an accredited University with a major in computer science, management information systems, or a closely related field. Graduate degree preferred.
- Seven years of progressively responsible experience in networking, Information Technology and associated systems, and system security.
- Seven years of experience serving in a project lead or supervisory capacity over complex technical assignments.

Licenses; Certificates; Special Requirements

Preferred certifications include Certified Information Systems Security Professional (CISSP), Security Essentials Certification (GSEC),Information Security Fundamentals (GISF), Certified Vulnerability Assessor (CVA), Systems Security Certification Professional (SSCP), Microsoft Azure Fundamentals (AZ-900), Microsoft Azure Administrator (AZ-104), Microsoft Security, Compliance and Identity Fundamentals (SC-900), CCNP (Security), CompTIA A+. Foreign Degree: **Applicants with foreign degrees from colleges or universities outside of the United States must have their coursework evaluated by a professional association that is a member of the National Association of Credential Evaluation Services(NACES)or Academic Credentials Evaluation Institute, INC.(ACEI). A copy of the evaluation must be submitted with your on-line application.** Commitment to Diversity: All applicants must have demonstrated cultural competency and sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students, faculty and classified professionals. Special Instructions to Applicants: To ensure **full** consideration, qualified candidates must submit a **complete** online application that includes the items listed (extraneous material will not be reviewed). References to resumes or other uploaded documents within the online application will be considered an "incomplete" application; please enter "N/A" if any section does not apply.

1. Fully completed online application;
2. Cover letter;
3. Resume; AND,
4. Three (3) references listed within the online application.

Important: To ensure consistency and fairness to all candidates, please do not submit materials other than those requested (i.e., personal photo, articles you've written, etc.). Please only upload requested documents using respective document name labels. Uploading extraneous materials, unless specifically requested within this posting, may result in your application not being reviewed. Only complete application packets will be forwarded to the committee.

- Application materials sent via mail, fax, or email will **not** be accepted.
- Note that correspondence, including interview invitations, will be sent to you via email.
- All inquiries, nominations and applications will be held in the strictest confidence.

Conditions of Employment:

Technology and Data Security Analyst
San Diego Community College District

SELECTED CANDIDATE IS REQUIRED TO COMPLETE THE FOLLOWING PRIOR TO EMPLOYMENT:

- Submit "official" transcripts as stated on application (From all institutions listed in the online application);
- Provide a Certificate of Tuberculosis Exam for initial appointment (Note: The certificate must be renewed every 4 years as a condition of continuing employment);
- Have fingerprints taken by a Live Scan computer at the District's expense (Clearance must be received prior to first day of employment);
- Present original documents for proof of eligibility to work in the United States **as required by the I9 Employment Eligibility Verification form**; AND
- Attend a new hire processing appointment in People, Culture, and Technology Services located at the District Administrative Offices.

EMPLOYMENT AFTER RETIREMENT

If you accept a contract (permanent) position with SDCCD and are a retired annuitant with CalPERS or CalSTRS, you must reinstate from your retirement system. Please reference the **CalPERS** or **CalSTRS** website for further information.

EMPLOYEE BENEFITS

SDCCD provides a comprehensive fringe benefit package for its full-time classified employees. The District contributes toward the cost of the premium (including dependent coverage) for the medical insurance plan options. Additional benefits include dental, vision, sick leave, vacation and opportunities for professional development. Contract employees become members of the California Public Employees' Retirement System (CalPERS) upon appointment.

Technology and Data Security Analyst
San Diego Community College District

Posting Number: CL01667

Major Responsibilities:

Qualifications:

Desired Qualifications:
Knowledge, skills and abilities:

- Network and server architecture and design including firewalls, routing, switching, operating systems, applications, access control, and data transmissions.
- Security assessment and testing tools.
- Technical sources of information for vulnerability alerts and advisories, security threat intelligence, and computer security standards, trends, and developments.
- Federal, state, and local regulations and guidelines related to information security such as HIPAA, FERPA, FISMA, NIST, SOC2 and GLBA Principles and methods of risk management and analysis as applied to technology and information security.
- Principles of data management, including data replication, retention, and security controls.
- Methods and techniques of technical documentation and record keeping.
- Principles of training.

Ability to:

- Conduct vulnerability audits, forensic investigations, and risk management assessments.
- Detect, investigate, and analyze threats and emergency security incidents.
- Respond immediately to security-related incidents and provide a thorough post-event analysis.
- Evaluate controls and procedures to mitigate risks, hazards, and threats to IT systems and their operation.
- Monitor internal and external policy compliance. Manage personal and institutional data per legal, regulatory, administrative, and contractual requirements.
- Consistently use and promote professional standards and practices related to assignments.
- Actively contribute to a culture of constructive collaboration and innovation with colleagues.
- Maintain high levels of customer service and satisfaction.
- Provide effective and timely liaison among management, programmers, security team staff, and

auditors on IT security issues and activities.
- Effectively communicate highly technical information accurately, concisely and in understandable terms, both orally and in writing.
- Foster a culture of constructive and effective collaboration and innovation within the architecture, solution designers, operations team, and other functions.
- Train technical staff in the application of information security concepts and practices.
- Stay abreast of current trends and technical advancements in the area of information security and apply knowledge to solving complex problems.

Hardware and Software Environment

- Microsoft 365, Azure, Microsoft Windows Server, Extreme Network Routing, Switching, Wireless Access Points and Controllers, Microsoft Defender for Endpoint, Microsoft End-Point Manager/InTune, Apple imaging and device administration.

Required Education, Training and Experience

- Bachelors degree from an accredited University with a major in computer science, management information systems, or a closely related field. Graduate degree preferred.
- Seven years of progressively responsible experience in networking, Information Technology and associated systems, and system security.
- Seven years of experience serving in a project lead or supervisory capacity over complex technical assignments.

Licenses; Certificates; Special Requirements
Preferred certifications include Certified Information Systems Security Professional (CISSP), Security Essentials Certification (GSEC),Information Security Fundamentals (GISF), Certified Vulnerability Assessor (CVA), Systems Security Certification Professional (SSCP), Microsoft Azure Fundamentals (AZ-900), Microsoft Azure Administrator (AZ-104), Microsoft Security, Compliance and Identity Fundamentals (SC-900), CCNP (Security), CompTIA A+.

Licenses:

Pay Information:

Technology and Data Security Analyst
San Diego Community College District

Range M ($7,515.15- $12,546.85) per month based on the 2023 Supervisory and Professional Employees Association - Salary Schedule B

New employees will begin on Step A ($7,515.15). Promoted or transferred employees will be placed as specified in the CBA. The District offers a comprehensive fringe benefit package including employer paid: medical, dental, and vision plans; sick and vacation leave; and opportunities for professional development. Initial Salary Placement, Promoted or transferred employees will be placed as specified in the SPAA - Supervisory & Professional Administrators Association Handbook. This position is FLSA Exempt and may not accrue overtime. A temporary probationary period will be applied to the employee entering this assignment. The SDCCD Employment Web Page provides a link to employee collective bargaining agreements and handbooks, and more information about terms and conditions of employment to include salary and benefits.

To apply, visit: https://www.sdccdjobs.com

All applicants must have demonstrated cultural competency and sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds of community college students and staff.

Contact Information

Please reference Academickeys in your cover letter when applying for or inquiring about this job announcement.

Contact

Information Technology
San Diego Community College District

,