San Diego Community College District

CLASSIFICATION DESCRIPTION

Page:	**1 of 3**
Job Code:	**D1835**
Original Date:	**05/2024**
Last Revision:	**07/2024**
Staff Type:	**Classified**
FLSA status:	**Exempt**
Salary Range:	**07**

Title: **Technology and Data Security Analyst**

Unit: **Supervisory and Professional**

DEFINITION

Under the supervision of the Associate Vice Chancellor, Information Technology Services or assigned manager, use independent judgment to assess, analyze, and enhance the security, integrity, and confidentiality of all enterprise systems, networks, assets, and communication technologies utilized throughout the District.

EXAMPLE OF DUTIES

1. Analyze, develop, and enforce security applications, policies, standards, and procedures to safeguard data against unauthorized access, disclosure, alteration, or destruction. Collaborate with the campus community to enhance the security of the IT infrastructure.

2. Lead the design, testing, and implementation of security solutions and controls across all SDCCD locations, ensuring comprehensive coverage.

3. Partner with campus and district technology teams to secure applications and infrastructure assets.

4. Continuously monitor security systems and logs; identify and manage security incidents, including troubleshooting, diagnosing, documenting, and reporting. Coordinate investigative efforts and respond to urgent security situations.

5. Work closely with developers and IT personnel to ensure production applications adhere to established security protocols and standards.

6. Facilitate training sessions on security and privacy for administrators, faculty, and staff; develop effective security incident notification processes.

7. Engage with vendors to perform thorough vulnerability assessments to detect and address potential security threats. Collaborate with law enforcement as necessary.

8. Conduct regular audits and inspections of information systems to verify the effectiveness of security measures and recommend improvements to mitigate risks.

9. Assess and recommend software solutions for IT security, including firewalls, anti-virus, encryption, and intrusion detection systems.

10. Oversee the operation of the Security Operations Center (SOC), Security Information and Event Management (SIEM) systems, and Data Loss Prevention (DLP) strategies.

11. Manage and update security systems and policies, including servers, firewalls, email security, and Microsoft 365 configurations.

12. Develop and enforce security protocols and practices; lead security education initiatives for staff.

13. Oversee network authentication protocols' security for wired and wireless connections.

14. Evaluate the security measures of third-party service providers and software systems that handle sensitive District data.

15. Ensure timely system maintenance and patching according to best practices and in alignment with security policies.

16. Stay informed on emerging security threats and solutions through professional development, networking, and industry collaboration.

17. Perform other related duties as assigned.

DESIRABLE QUALIFICATIONS

Knowledge:

Advanced knowledge of desktop and server operating systems, including Windows and Linux.
Compliance and industry cybersecurity frameworks such as NIST 800 and ISO standards.
Disaster recovery and backup, including business continuity planning.
Emerging technologies and the possible impact on existing information systems, instructional processes, and business operations.
Enterprise resource planning systems, Microsoft 365, Active Directory, and Azure Active Directory.
General research techniques and data-driven analytics.
Incident response best practices and software license compliance laws.
Modern office administrative practices and the use of tools, including computers, websites, and other applications, related to this job.
Principles of program design, coding, testing, and implementation.
Principles of training, support, and services to end-users.
Troubleshooting tools for computing hardware, servers, and network equipment, including but not limited to switches, routers, and firewalls.

Skills and Abilities:

Analyze situations accurately and adopt an effective course of action.
Apply current NIST and ISO standards to current operations.
Communicate complicated technical issues and their risks to stakeholders and management.
Coordinate, develop, and implement projects.
Establish and maintain effective and cooperative working relationships with others.
Prepare clear and concise system documentation and reports.
Prioritize assigned tasks and projects.
Respond to incidents and events promptly.
Work with attention to detail and independently with minimum supervision.

Training and Experience:

Any combination of training and experience equivalent to: a Bachelor's Degree from an accredited institution with major coursework in computer information systems, computer science, business administration, or a related field and two years of progressively responsible experience performing information security duties, which may include implementing, overseeing, and/or managing information security technologies, processes, or programs, including identification, protection, detection, response, and recovery activities.

Certification:

Professional security or privacy certification, such as the Global Information Assurance Certification (GIAC), GIAC Incident Handler Certification (GCIH), Cloud Forensics Responder (GCFR), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or other similar credentials.

WORKING CONDITIONS

Physical Requirements:

Category III: Typically sedentary in nature.

Environment:

Work is performed primarily in an office environment with a computer, monitor, keyboard, and mouse and may require prolonged periods of sitting.