METROLINK

JOB DESCRIPTION

Job Title: Assistant Director (Various)
Working Title: Assistant Director, Business Information Security Officer (BISO)
FLSA Status: Exempt
Salary Grade: 11B

PURPOSE OF POSITION

The Assistant Director, Business Information Security Officer (BISO), will understand the key assets and processes, define and evolve cybersecurity strategy, identify and evaluate risks and controls, and suggest incremental controls or risk mitigation strategies where necessary. Additionally, the Assistant Director, BISO, will ensure business compliance with Information Security Policies and Standards while continuously monitoring and reporting on risks and documented exceptions. The Assistant Director, BISO, helps the business achieve its objectives while not compromising the security posture. The Assistant Director, BISO, will work under the general direction of SCRRA's Chief Technology Officer, and the position will collaborate with internal and external auditors to ensure compliance with SCRRA's cybersecurity procedures and industry standards.

DISTINGUISHING CHARACTERISTICS

This job description is not part of a job series.

SUPERVISION EXERCISED AND RECEIVED

- Receive general oversight from executive level management.
- This position will have no direct reports.

ESSENTIAL DUTIES AND RESPONSIBILITIES

The duties listed below are intended to describe the general nature and level of work being performed and are not to be interpreted as an exhaustive list of responsibilities.

- Lead, develop, and implement SCRRA-wide or large-scale business unit information and operational technology security strategies, programs, plans, programs, policies, and procedures designed to protect the integrity and security of the SCRRA network, data resources, operations, and other information assets in accordance with SCRRA policies and industry standards.
- Develop and maintain in-depth understanding of region/business unit processes, systems, technologies, data, customers, consumers, and partners.
- Evaluate the overall technology portfolio for adherence to security policies and procedures for all SCRRA corporate and operational systems (e.g. positive train control (PTC)).
- Coordinate auditing, compliance, and certification requirements.
- Leads cyber security training program for the agency, consumers, and partners as needed.
- Act as the key security resource for the IT leadership, the IDTS Business Partners, and other local personnel.
- Partner with all Departments to achieve effective working relationships that can further the effectiveness of the Security program.
- Lead development of the Information Security Policies and Standards throughout the agency.
- Lead implementation of cybersecurity solutions required to meet business objectives.

- Review and audit technical implementations of physical security solutions required to meet business objectives.
- Lead information security operations in partnership with all departments.
- Proactively identify noncompliance and areas of potential improvement, and issue corrective actions to department manager.
- Engage with clients and customers as needed to assist the business to achieve its objectives by representing our security program, supporting internal and external audits, assisting in customer communication of security incident, etc.).
- Participate in region/business unit-related conferences, client-facing engagement, and industry forums to represent the Cyber Security program.
- Provide regular and timely reporting on the status of cybersecurity throughout the agency.
- Provide escalation path for security issues, incidents, and inquiries.
- Review work of the Security Incident Response and Crisis Management teams to ensure effectively driving incidents to acceptable resolution; assist with investigations as needed.
- Provide Cyber Security Guidance for agency personnel.
- Drive remediation activities throughout the agency.
- Work with the Compliance and Information Risk Management team to drive policy and regulatory compliance.
- Responsible for the PCI-DSS annual compliance submission requirement and developing a monitoring program to ensure SCRRA is PCI compliant.
- The responsibilities outlined above are representative of the role but not exhaustive. Additional duties may be assigned as needed, and reasonable accommodations will be provided to qualified individuals with disabilities in accordance with applicable laws.

MINIMUM QUALIFICATIONS

Education and Experience

- Bachelor's degree in computer science, Information Systems, Cybersecurity, Auditing or a related field.
- A minimum of eight (8) years of relevant experience.
- A minimum of five (5) years of experience in supervising and monitoring the work of subordinate staff or project managers, including monitoring and evaluating staff.
- A combination of training, education, and/or experience that provides the required knowledge, skills, and abilities may be considered when determining minimum qualifications. Advanced relevant coursework may also substitute for a portion of required experience.

Preferred Qualifications

- A minimum of five (5) years of experience in business security policy development, metrics capture, analysis, and system authorization.
- Certification pertaining to information security and data privacy protection (CISSP, CISA, CRISC, CISM, CEH, etc.)
- Experience in compliance, government or financial industry.
- Experience in the design and implementation of information security programs.
- Knowledge and experience with security and governance frameworks: SSAE-18 (SOC-2), HIPPA, PCI-DSS, ISO27991, NIST, Fedramp.

Knowledge, Skills, and Abilities

Knowledge of:

- Advanced level understanding of business theory, business processes, management, and business operations.
- Advanced level understanding of planning, organizing, and developing Information Technology security and physical security system technologies.
- Extensive experience in enterprise security document creation.
- Experience in designing and delivering employee security awareness training.
- Experience in developing Business Continuity Plans and Disaster Recovery Plans.
- Strong understanding of IP, TCP/IP, and other network administration protocols.
- Expert-level understanding of key network and technical security controls.
- Security best practices including experience with NIST 800-53, ISO27001 and PCI DSS.P

Skilled in:

- Applying IT in solving security problems.
- Setting and managing priorities.
- Executive-level presentations.
- Maintaining interpersonal relationships.

Ability to:

- Analyze and solve problems.
- Apply organizational information security policies at a business unit level.
- Develop conceptual frameworks and apply sound principles for the secure operation of SCRRA technology resources.
- Define and develop security strategy and roadmaps.
- Facilitate cross-functional team meetings and build consensus.
- Understand business needs and work collaboratively with business stakeholders and team members.
- Implement and manage the administration of relevant security systems and solutions.
- Recommend and implement changes in security policies and practices in accordance with changing needs.
- Promote and oversee strategic security relationships between internal resources and external entities, including other government agencies, vendors, and partner organizations.
- Communicate effectively, both orally and in writing.
- Maintain, and accurately complete records.
- Establish and maintain effective working relationships with supervisors, fellow employees, and the public

PHYSICAL REQUIREMENTS

- Transition between a stationary position at a desk or work location and move about Metrolink facilities or other work site locations
- Operate tools to perform the duties of the position, such as computers, office equipment, and work-related machinery
- Transport equipment or boxes up to 25 lbs
- Exchange ideas by means of communication
- Visual acuity to detect, identify, and observe employees or train movement and any barriers to movement when working on or near railroad tracks
- Hear and perceive the nature of sounds when working on or near railroad tracks

- Balance, ascend/descend, climb, kneel, stoop, bend, crouch, or crawl within assigned working conditions and or locations

Working Conditions

Position requires work in a normal office environment with little exposure to excessive noise, dust, or temperature. Work may also be conducted in outdoor environments, at construction sites, Railroad Track and Right-of-Way environments, and warehouse environments, with possible exposure to individuals who are hostile or irate, moving mechanical parts, and loud noises (85+ decibels, such as heavy trucks, construction, etc.)

Southern California Regional Rail Authority is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the Authority will provide reasonable accommodations to qualified individuals with disabilities and encourages both prospective and current employees to discuss potential accommodations with the employer.

Last Updated: June 2026