CALIFORNIA HIGH-SPEED RAIL AUTHORITY
DUTY STATEMENT

RPA #22-201

CLASSIFICATION TITLE	**OFFICE/BRANCH**	**LOCATION**
Information Technology Specialist I	Information Technology/ Information Security	Sacramento
WORKING TITLE	**POSITION NUMBER**	**EFFECTIVE**
Information Security Analyst	311-400-1402-021	06/20/2022

GENERAL STATEMENT:

Under the direction of the Information Technology Manager II, the incumbent will work independently as well as part of a team to coordinate and/or perform a variety of Information Technology (IT) services and functions. The incumbent is responsible for performing various oversight duties in support of the California High-Speed Rail Authority's (Authority) Information Security Program ensuring protection of Authority information assets and compliance with federal and state information security mandates, policies, standards, and procedures.

This position requires the incumbent to communicate effectively orally as well as in writing; conduct themselves professionally in dealing with other employees and contractors; develop and maintain knowledge and skills related to the position's specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner, and adhere to departmental policies and procedures regarding attendance, leave, and conduct.

This position is designated under the Conflict-of-Interest Code. The position is responsible for making, or participating in the making, of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete form 700 within 30 days of appointment. Failure to comply with the Conflict-of-Interest Code requirements may void the appointment.

All work will be accomplished in accordance with IT Standards; the State Administrative Manual (SAM) Sections 4800 through 5953 and Sections 6700 through 6780; the California Technology Agency's (CTA) Statewide Information Management Manual (SIMM); the Department of Finance (DOF) Office of Technology Review, Oversight and Security (OTROS) rules and policies; DOF Budget Letters; the State's Information Organization, Usability, Content Currency, and Accessibility (IOUCA) Working Group policies and the Authority's Desktop and Mobile Computing Policy, IT Security policies and procedures and IT Standards.

TYPICAL DUTIES:

The Information Security Analyst must be able to work independently and collaboratively with other IT Office staff to produce deliverables and implement/affect change. The following Information Technology Domains are applicable to the incumbent's duties/tasks:

☒ Business Technology Management	☐ Information Technology Project Management
☐ Client Services	☐ Software Engineering
☒ Information Security Engineering	☒ System Engineering

Percentage Essential (E)/ Marginal (M)	Job Description

30% (E) **Risk and Compliance Management**

- Ensure Authority compliance with state and federal information security risk management requirements, including SAM § 5300, et seq., SIMM, and the National Institute of Standards and Technology (NIST).
- Identify and prioritize risk assessments, maintenance of standards and templates for risk assessments, and compilation of risk assessment data into summary reports.
- Conduct risk assessments of IT systems; the underlying technical security controls; administrative processes regarding the privacy and security of confidential data; and physical security controls protecting Authority-owned hardware, software, and data.
- Participates in information system risk assessments and designing security countermeasures to mitigate identified risks, performs research and develops recommendations to mitigate risks, and works with technical staff to create security variance requests when required.
- Stay abreast of current cyber threats to Authority information resources.

20% (E) **Security Policies, Standards, and Procedures**

- Develop, maintain, and conduct information security and privacy awareness training/phishing campaigns.
- Develop emails, newsletters, phishing campaigns, or other communications for Authority staff to promote security and privacy awareness or education.
- Recommend, track, and maintain Authority information security policies, mandates, and procedures.
- Participate in program, administrative, or operational reviews of information security programs to ensure programs and operations are meeting established goals/objectives and regulatory guidelines.

- Develop and document procedures to support new processes or process changes, including any training or reference materials to support implementation.
- Recommend technical roadmaps, enterprise architecture security standards, and strategies to best align technology solutions with business and organizational needs.

20% (E) **Privacy Program Management and Data Loss Prevention**

- Recommend, create, and manage an enterprise privacy, data classification, and data loss prevention program to ensure compliance with state, federal, and other regulatory requirements, as well as ensuring the confidentiality, integrity, and availability of Authority data.
- Perform FIPS 199 information systems and data classification to assess the potential impact on Authority assets and operations should the information or information system become compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.
- Monitor and review proposed modifications to existing systems to ensure appropriate information security and privacy safeguards are maintained.
- Serve as the backup to the Authority's Privacy Officer.

20% (E) **Technology Recovery Planning**

- Serve as the Authority's Technology Recovery Plan coordinator.
- Develop, manage, and lead an enterprise Technology Recovery program to ensure timely operations recovery following an interruption in service caused by a technology system outage or a declared disaster.
- Coordinate business impact analyses and management of tabletop recovery exercises with both business and technical staff.
- Lead periodic table-top testing of the Technology Recovery Plan and document gaps to improve processes and procedures.
- Participate in the recovery of failed systems.

10% (M) **Other Duties**

- Actively participate in team meetings, technology initiatives, or other assignments.
- Maintain up to date knowledge about state policies, processes, and industry best practices related to IT administration and information security.
- Invest in personal development through continuous education to maintain position-related knowledge.
- Other duties as required.

KNOWLEDGE AND ABILITIES:

Knowledge of: Information technology concepts, practices, and principles to provide a foundation for technology related work; Principles, techniques, and procedures related to the delivery of information technology services; the System Development Lifecycle including the associated methodologies, tools, and processes; the organization's business processes and procedures; education tools and techniques; performance monitoring tools and techniques; and data administration techniques and best practices; Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques.

Ability to: Perform research and data gathering; analyze information and evaluate results to choose the best solution and solve problems; communicate effectively verbally and in writing as appropriate for the needs of the audience; utilize reporting tools to develop and analyze statistical reports; interpret and explain technical information to non-technical individuals; interpret customer requests to meet service needs and resolve problems; provide customer service; work cooperatively with staff at all levels; proficiently use computers and productivity software; and understand and align technology proposals with business needs; use initiative; act independently with flexibility and tact; use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems; perform technical analysis of proposed technology solutions; comprehend technical documents to interpret specifications, system implementations, capabilities, interdependencies, and compatibilities; serve as a technical liaison; develop and effectively utilize all available resources; develop end-user training materials; and gather data to perform statistical analysis and report outcomes; Formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, state, department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions which are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs.

DESIRABLE QUALIFICATIONS:

- Associate or bachelor's degree in an IT-related field preferred;
- 2 years of related experience in Information Security operations or equivalent combination of education and experience;
- Possession of one of the following active certifications is desirable:
    - CompTIA Security+
    - GIAC Information Security Fundamentals
    - Associate of (ISC)2
    - Certified Information Systems Security Professional (CISSP)
    - Certified Information Security Manager (CISM)
    - Certified Information Systems Auditor (CISA)
- Ability to maintain confidentiality of sensitive tasks or assignments;
- Ability to independently analyze and resolve issues;
- Aptitude and desire for continuous learning;
- Project lead experience;
- Ability to think critically and prepare and produce clear and concise documentation (e.g., user manual, processes and procedures, plans, policies, etc.);
- Ability to establish and maintain cooperative working relationships with all levels of staff and management, communicate effectively with peers, users, developers, management, and others;
- Demonstrate a service-oriented, customer relations-sensitive attitude;
- Knowledge of Security Awareness Training solutions such as KnowBe4 Security Awareness;
- Exercises good judgment in the performance of responsibilities, requiring minimum supervision;
- Exhibits a talent and passion for information security; is creative and resourceful in solving problems;
- Thorough understanding of NIST, SAM, and SIMM.

SUPERVISION EXERCISED OVER OTHERS:

This level does not supervise but may act in a lead capacity. The IT Specialist I has defined responsibility and authority for decision making related to assignments or in an advisory function.

RESPONSIBILITY FOR DECISIONS AND ACTIONS:

At the IT Specialist I level, incumbents are responsible for individual decisions and actions. Performs a wide variety of tasks requiring regular innovative problem-solving within broadly stated and non-specific guidelines. As a subject matter expert, this level is responsible for actions that could have a serious detrimental effect on the operating efficiency of the undertaking or function.

CONSEQUENCE OF ERROR:

The consequence of error at the IT Specialist I level may result in loss of data, user dissatisfaction, and impact to the organization, project, or work unit, and related support units. Consequences include operational down time, loss of business continuity, and poor customer service and performance.

SPECIAL PERSONAL CHARACTERISTICS:

- Ability to learn new technologies quickly and thoroughly;
- Ability to resolve technical problems quickly and tactfully;
- Ability to read and interpret operating and maintenance instructions and procedure manuals;
- Ability to work effectively under tight time constraints, client demands, and the pressure of multiple deadlines;
- Adhere to departmental policies and procedures regarding attendance, leave, and conduct.

INTERPERSONAL SKILLS:

- Excellent communications skills both orally as well as written;
- Excellent analytical skills to troubleshoot problems or offer alternatives for problem resolution;
- Conduct themselves professionally in dealing with other employees and contracted staff.

PHYSICAL, MENTAL, AND EMOTIONAL ABILITIES:

The employee must be able to focus for long periods of time, multi-task, adapt to changes in priorities and complete tasks or projects with short notice. Incumbent will be required to use a computer, mouse and video display terminal and will be required to sit for long periods of time at a computer screen. The employee must develop and maintain cooperative working relationships and display respect for others in all contact opportunities.

WORK ENVIRONMENT:

At their base of operation, employee will work in a climate-controlled office which may fluctuate in temperature and under artificial light. Employees may be required to travel outside of their work area to perform general tasks. Employee must carry a cell phone and respond to calls after hours to provide resolution to IT system problems or other urgent business needs. The employee will also be required to:

- Work occasional nights and weekends as necessary;
- Effectively work under pressure;
- Occasionally travel as required.

I have read, and understand the duties listed above and can perform them either with or without reasonable accommodation. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

Name of Employee: _____

Signature:	Date:

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

Name of Supervisor: _____

Signature:	Date: