DUTY STATEMENT Duty Statement for Professional / Analytical Classifications State Compensation Insurance Fund

Employee's Name (First, Last)	
Program Information Technology - System Engineering	Work Unit Quality Assurance
Position's Authorized Classification (and Range) Information Technology Specialist II	Report To IT Manager II
Position Title Lead Application Security Engineer	Position Serial Number ###.###
Incumbent Appointment Classification DOMAIN: Information Security Engineering ☐ The incumbent is underfilling the position in the Not Applicable classification. S/he will be given appropriate training, direction, and feedback	CBID R01 FLSA Status ☐ Covered, Work Week Group 2 ☒ Not Covered, Exempt WWG ☒ E or ☐ SE

PURPOSE/SCOPE:

Briefly describe or summarize the position's major functions. Why the position exists? Typically includes the following:

- Intent/Purpose of the position
- Degree of direction/supervision (Under what direction)
- Nature and level of the work

Example: Under direction (*degree of supervision*), perform the full range (*scope*) of varied, sensitive**, and complex** (*level of work*) analytical and consultative work necessary to effectively administer the program's _____ function (*reason for the position*).

** "Sensitive" and "Complex" should be defined

Under the general direction of the Vice President of Systems Engineering (IT Manager II), the ITS II Application Security Engineer leads application security initiatives across various State Fund applications and plays a lead role in the team, advisor to IT leaderships, and participates in projects as a subject matter expert and/or other capacity.

• Develop, implement, and deliver Enterprise-Level Application Security Strategy for projects or programs in all security principles, risks, attacks, OWASP security guidelines, Threat modeling, RASP and industry best practices to perform techniques such as SAST, DAST, IAST, RASP and Application Penetration Testing.

• Collects, organizes, and analyzes statistical information from variety of sources both technical, and non-technical to support high-quality application security test design.

• Application Security expert in "Quality AGILE + DevSecOps" transformation initiatives across UI, Microservices, APIs, CI/CD/CT integration, and handling Cloud Native architectures.

• Deliver end-to-end project & product software development / testing lifecycle (SDLC / STLC) needs such as BRD review, security architecture / design review including TDD or SDD, security risks / technical assessment, meet defined target timelines, represent Application security with Project/Dev managers, support and train Dev, DevOps, functional QA and QA security teams in enhancing & strengthening application security capabilities.

Supervisor's Statement: I have discussed the duties of the position with the employee		
Supervisor's Name (Print) Danny Wang	Supervisor's Signature	Date
Employee's Statement: I have discussed with my supervisor the duties of the position and have received a copy		
Employee's Name (Print)	Employee's Signature	Date

Duty Statement Origination or Revision Date May 28, 2026

KEY RESULTS/ESSENTIAL FUNCTIONS: Specifically describe the 3-5 Key Results (or Essential Functions) of the position in order of their importance to achieve the purpose/scope of the position.

Each Key Result/Essential Function description should have statement(s) consisting of

1	2	3
An action verb: What is done? Define or elaborate on common vague words (e.g., "coordinates", "monitors", "assists")	The immediate object of the action	The reason for the action: Why?

In all aspects of performing the following Key Results/Essential Functions the incumbent will
- comply with the Code of Conduct and
- maintain regular and predictable attendance and/or communication availability during working hours.

The statements contained in this duty statement reflect general details as necessary to describe the principal results/functions of this job. It should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties as assigned, including work in other functional areas.

40%

1) Develop, plan, research, design and implement robust application security strategy initiatives including security architectures or design reviews, risk assessments, security testing and debugging technical issues of the most complex** software systems and software projects.
(This is an essential function of the job.)

a. Provide technical guidance and mentor other team members for success and delivery of projects and initiatives. Complete all planned work by the target dates established. Meet target dates for project milestones.

b. Apply application security methodologies and tools to complex applications for finding security risks or weaknesses and security vulnerabilities early in the SDLC process.

c. Provide project status to management, project sponsors, and the project team as detailed in the project plan or by request. Ensure that required reports are clear, concise and timely.

d. Develop application security test requirements for Web / Cloud & API Applications Security Testing for all releases using automated tools and manual testing. Conduct different types of application security testing including penetration testing in line with Open Web application Security project (OWASP) standards and guidelines.

e. Ensure automation-first approach utilized in all deliverables to increase efficiency as designed and meet testing requirements.

f. Design test plans for DAST, IAST, Pen Test, assess OWASP Top 10 Most Critical Web Application Security Risks, public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures, understanding network and firewall configurations & changes.

g. Participate with the project team and Quality Management team in post-implementation project review.

h. Follow established departmental procedures and guidelines.
   i. Observe system development standards and guidelines (Systems Development Life Cycle).
   ii. Utilize tools, application version control and utilities following departmental guidelines.
   iii. Observe departmental procedures for providing QA security signoff.

i. Translate complex processes, methodologies, issues or risks into easy to understand summaries for senior and executive level leadership

j. Ensure that all required documentation is complete, clear and usable by its intended audience.

**Most complex consist of features including but not limited to the following:
• Capture and define the security test requirements and review security architecture, technical designs including BRDs, TDDs or SDDs or comprehensive Security Requirements Checklists.
• Plan, research, and design robust security test strategy for any IT project.
• Perform vulnerability testing, risk analysis, and security assessments.
• Research security standards, security systems and authentication protocols for secure SDLC including Threat Modeling and other industry best practices.

30%

2) Lead the most complex** projects, initiatives and maintenance projects and teams to plan, design, develop, test and implement new and enhanced enterprise security in applications/systems to meet business needs.
(This is an essential function of the job.)

a. Coordinate/lead the team in the process of collecting, reviewing, and analyzing business requirements, recommending technical solutions, preparing design specifications and implementing design solutions on the most complex projects and application under test (AUT)

b. Collaborate with business & IT stakeholders to facilitate the planning and delivery of most secured IT solutions.

c. Coordinate and consult with software vendors for product utilization. Evaluate vendor software packages from security perspective.

d. Effectively manage the most complex projects to ensure that the end product or service is secured and delivered on schedule and within scope and established budget.

e. Establish controls (e.g., project plans, schedules and risk analysis) and monitoring means to ensure the timely completion of project objectives and deliverables.

f. Manage security testing scope, prioritize workloads, verify business rules and business processes, and assign tasks.

g. Maintain and update project status reports to reflect current project information and statistics.

h. Collaborate with Business Project Leader/Liaison if needed including QA functional & automation test leads

i. Translate complex processes, methodologies, issues or risks into easy to understand summaries for senior and executive level leadership

10%

3) Deliver end-to-end project & product software testing lifecycle (STLC) needs such as requirement review, technical assessment, test estimation, meet defined target timelines, represent QA security with project managers, support and train the functional QA and QA security teams in enhancing & strengthening security function.
(This is an essential function of the job.)

a. Conduct systems analysis of business processes. Evaluate current and proposed information and business process flows and business requests for applications/ systems.

b. Gather and analyze business requirements. Submit Security Test Strategy and Test plan as needed.

c. Ensure that System architecture or design specifications including TDDs or SDDs are reviewed from security perspective before it's ready for development and testing with high standards.

d. Enhance/ maintain existing computer programs/ applications to increase operating efficiency, adapt to new

requirements or correct errors.

10%

4) Provide enterprise architectural and technical security leadership to meet business objectives. (This is an essential function of the job.)

a. Contribute the highest level of technical knowledge, business expertise, and leadership in meeting the State Fund's business objectives.

b. Define, implement and maintain Corporate or Enterprise security policies and procedures

c. Oversee security awareness programs and educational efforts

d. Be recognized by IT management, business partners, employees, and consultants as a subject matter expert.

e. Respond immediately to security-related incidents and provide a thorough post-event analysis.

f. Define all entry points to the system, such as: files, sockets, hypertext transfer protocol (HTTP) requests, named pipes, pluggable activities, protocol handlers, malicious server responses and so on.

g. Research and evaluate emerging technology tools, practices and techniques and provide direction for development strategies.

h. Create architectural diagrams and blue prints as needed to point out technical gaps from security standpoint

10%

5) Act as a subject matter expert and technical advisor/resource and provide training to IT QA staff.

a. Assign, direct and review the work of assigned security team members and/or other IT QA team members

b. Advise internal & external consultants as needed.

c. Effectively facilitate the transfer of knowledge from external consultants to employees.

d. Mentor other application security engineers and/or programmers in securing systems, Secure SDLC methodologies, security deliverables management, security risks, tools and techniques for remediation.

e. Provide application security architectural and risk assessment and advise to management.

f. Provide clear and accurate information and/or assistance to IT and business unit personnel within the requested time frame.

g. Participate as an application security architect or subject matter expert in the most complex system engineering projects or application security initiatives.

100%

REQUIRED QUALIFICATIONS/COMPETENCIES (KNOWLEDGE, SKILLS/ABILITIES):

KNOWLEDGE AREAS:

Ability to effectively provide technical risk assessment of technologies in networks, applications, wireless, social engineering, code reviews and war dialing

Write technical reports that include suggested resolution for identified problem areas and perform operational risk assessment.

Knowledge of the requirements for the installation and implementation of the most complex information technology software systems.

General understanding of State Fund's business and Strategic Goals.

Ability to flow from black box to gray box to white box tests dependent on client needs.

Working knowledge of State Fund's security policies and practices.

Working knowledge of project management principles.

Working knowledge of application promotion to production procedures.

Proficient knowledge of three or more State Fund business systems/applications or processes (Quote, Policy, Claims, Data Management, Back office, HR & Legal apps).
Knowledge of security technologies and skill in using TCP/IP.
Working knowledge of State Fund Information Technology principles, current trends, methods and practices.
Knowledge of emerging technologies and their applications to business processes, business or systems process analysis, design, testing, and implementation techniques.
Proficient knowledge of security architect testing in one or more of the following web development frameworks: C#, .NET Core, .NET Framework, Visual Basic, Java, MVC, Entity Framework, JavaScript, Ajax, JQuery, AngularJS, ReactJS, Web API/Service, CGI, CORBA, WCF, SQL, PL/SQL, HTML, XML, CSS, Python, GO and more advanced programming languages.
Proficient knowledge of working with one or more of the following databases: Oracle, SQL Server, DB2, MS Access.
Proficient knowledge of utilizing computer aid tools, IDE.
Working knowledge of security testing tools: Synopsys, Contrast, IBM Appscan, Burp Suite, Tamper Data, Live http Headers, HP Fortify, VeraCode, OWASP Top 10, N-Stealth, Hailstorm, Paros, SANS Top 20, Acunetix, Nessus, Smart Bear products.
Working knowledge of IT tools: Chef, Splunk, Vagrant, Dynatrace

SKILLS/ABILITIES:

Skill/Ability to research, analyze, and evaluate information to make and support decisions

Skill/Ability to influence others and negotiate agreements and consensus among project partners, work peers, and other stakeholders

Skill/Ability to achieve results according to objectives

Skill/Ability to manage multiple projects and tasks and work under pressure

Skill/Ability to provide training

Skill/Ability to handle stressful situations while being firm but tactful

Skill/Ability to prepare effective reports and coordinate, facilitate, and make presentations

Ability to handle the the requirements for the installation and implementation of the most complex information technology software systems.

Ability to write complex programs, develop detailed program specifications, analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions

Skill/Ability to apply creative thinking in the design and development of methods of processing information with information technology systems

Ability to communicate effectively (both orally and in writing) and establish and maintain cooperative relationships with those contacted in the course of the work

Ability to delegate work assignments at the appropriate level of responsibility and coordinate the activities of technical personnel

Ability to learn and apply new technology information quickly and effectively.

Ability to evaluate vendor software packages from security perspective.

Ability to effectively provide technical risk assessment of technologies in networks, applications, wireless, social engineering, code reviews and war dialing
Ability to write technical reports that include suggested resolution for identified problem areas and perform operational risk assessment
Ability to flow from black box to gray box to white box tests dependent on project needs
Ability to perform Dynamic Application Security Testing (DAST)
Ability to perform Static Application Security Testing (SAST)
Ability to perform Interactive Application Security Testing (IAST)
Ability to perform Web Application Penetration Testing
Ability to perform Product Security Testing
Ability to perform Cloud Application Security Testing

Ability to perform API / Web Services Security Testing
Ability to perform Security Architecture Design Review
Ability to perform Application Security Risk Assessment

WORK ENVIRONMENT:

Physical Requirements

Computer data entry, frequent light lifting, bending, reaching, carrying, and telephone work; mobility to various working areas

Incumbent works in the usual office and as-needed work from home environment.

Travel

Travel may be required.

Travel to various work sites and locations for training and/or meetings.

Emergency call backs

Emergency call backs may be needed.

Work Hours

On call 24/7, as needed.

Will occasionally involve work in the evenings and on weekend.