CalSAWS Job Description

SECURITY AND OPERATIONS MANAGER

Salary Determined by Employer
RGS Salary Range:
$10,206.08 - $16,203.71 Monthly

JOB DESCRIPTION

The Security and Operations Manager provides strategic leadership and hands-on oversight of security and operational functions for CalSAWS, a complex, multi-county eligibility system supporting public assistance programs statewide. This role verifies and maintains system security, performance stability, and operational excellence in alignment with the CalSAWS System Security Plan (SSP) and Maintenance and Operations (M&O) Plan(s). The Manager leads a team of Technical Security Analysts and acts as the Product Owner for Identity and Access Management (IAM), driving initiatives to enhance resiliency, protect sensitive data, and align with federal and state security standards.

RESPONSIBILITIES

- Key responsibilities include, but are not limited to:
    - Direct, plan, and organize operational and security activities aligned with project deliverables and timelines.
    - Oversee development, review, and approval of key work products such as SLA compliance reports, infrastructure services plans, and technical architecture reviews.
    - Verify and maintain adherence to the Infrastructure Services Plan, M&E Services Plan, and System Security Plan (SSP).
    - Review and evaluate System Change Requests (SCRs) to maintain system integrity.
    - Prepare and present status reports for leadership and stakeholder consumption.
    - Provide guidance and review on security-related technical designs to verify and maintain alignment with operational goals.
    - Coordinate information security activities with infrastructure and development teams to verify and maintain seamless integration across the enterprise.
    - Evaluate proposed system designs for compatibility with long-term strategic plans, ensuring they are scalable and flexible.
    - Provide expert technical support and security guidance throughout all system lifecycle phases.
    - Manage and participate in assessment and analysis of planning and procurement documents for technical accuracy.
    - Escalate and resolve operational and security issues in a timely manner, maintaining transparent communication with leadership.
    - Develop, enforce, and continuously improve policies and procedures related to system and data protection.
    - Monitor system metrics and lead incident response and recovery activities in alignment with ITIL and NIST best practices.
    - Verify and maintain compliance with industry standards and organizational policies, including NIST SP 800-53 Rev 5, ISO 27001, and CalSAWS governance.

IAM Product Owner Responsibilities:

- Define and maintain the IAM product vision and roadmap aligned with business goals and compliance mandates.
- Translate business and regulatory requirements into prioritized product features and user stories.
- Collaborate with Security, IT, HR, and Application Owners to verify and maintain IAM meets cross-functional needs.
- Oversee implementation and optimization of IAM components such as lifecycle management, RBAC, MFA, SSO, and privileged access management.

- Verify and maintain audit readiness and continuous improvement of IAM processes based on feedback, KPIs, and audits.
- Track and report key performance indicators (KPIs) to measure IAM effectiveness and posture.
- Provide documentation and training to support teams and end users for IAM adoption and usage.

DESIRABLE SKILLS AND CAPABILITIES

Candidates of this position should have applicable experience, skills, and capabilities to perform the following functions and activities:

- Strong analytical and problem-solving skills.
- Advanced product and project management capabilities.
- Strong organizational and leadership abilities.
- Proven ability to lead cross-functional teams through project stages.
- Effective communication and stakeholder engagement skills.
- Working knowledge of public assistance programs and related state policies.
- Familiarity with Zero Trust, cloud security, and DevSecOps practices.

QUALIFICATIONS AND REQUIREMENTS:

MINIMUM REQUIREMENTS:

TRAINING AND EXPERIENCE:

Bachelor's degree in Information Technology, Cybersecurity, Computer Science, Information Systems, or related field AND five (5) years of progressively responsible experience in IT operations, systems security, or infrastructure management, including two (2) years of supervisory or technical leadership experience.

-OR-

Four (4) years of experience as an Information Technology Manager I or equivalent in public agency operations overseeing security protocols and enterprise systems.

-OR-

Four (4) years of experience in managing the security design, implementation, and maintenance of large-scale enterprise systems with at least two (2) years of supervision of technical staff in a multi-agency environment.

PREFERRED CERTIFICATIONS:

- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager
- ITIL Foundation (v3 or v4) – Information Technology Infrastructure Library
- PMP – Project Management Professional
- GIAC Security Essentials (GSEC) or similar cloud/DevSecOps-related certifications (optional)

IDENTIFICATION:

A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

CalSAWS Job Description

PHYSICAL CLASS:

2-Light.

OTHER REQUIREMENTS:

N/A

SPECIALTY REQUIREMENTS

N/A