CalSAWS Job Description

CHIEF INFORMATION SECURITY OFFICER

Salary Determined by Employer
RGS Salary Range:
$13,565.05 - $19,477.60 Monthly

JOB DESCRIPTION

The Chief Information Security Officer (CISO) leads the strategic direction of cybersecurity, cloud security, and enterprise-wide governance, risk, and compliance (GRC) for CalSAWS (California Statewide Automated Welfare System) is to provide a comprehensive, reliable and efficient automated social services system that supports the needs of all 58 counties in California. This executive role is responsible for defining the security vision, building a resilient security architecture, and leading compliance efforts with California and federal regulatory requirements.

The CISO reports directly to executive leadership and collaborates with stakeholders across state and county agencies, technology partners, auditors, and oversight bodies. This role drives risk management, security operations, and the adoption of frameworks such as NIST and Zero Trust, while leading a team that includes the Information Security Officer (ISO) and Security Engineer.

RESPONSIBILITIES

- Lead the design and execution of a multi-year enterprise cybersecurity strategy aligned with CalSAWS' mission, risk tolerance, and operational objectives
- Oversee the governance, risk, and compliance (GRC) program, including security policy management, internal controls, risk assessments, and audit coordination
- Direct enterprise cloud security efforts across hybrid and multi-cloud environments, with a focus on data protection, identity management, and secure architecture
- Manage the development, maintenance, and validation of System Security Plans (SSPs) to support CalSAWS compliance with State of California policies and applicable federal requirements
- Serve as the primary liaison to external auditors, regulatory agencies, and oversight bodies, representing CalSAWS in all matters related to security posture and compliance
- Advise executive leadership on cybersecurity threats, regulatory shifts, and technology trends, translating complex risks into business-aligned decisions
- Lead the incident response program, including investigation coordination, stakeholder communication, and root-cause remediation planning
- Develop and track measurable security metrics (KPIs/KRIs) to assess program maturity, guide investment decisions, and report progress to leadership and stakeholders
- Partner with the Privacy Office to align data governance practices—including classification, access controls, and retention policies—with security and privacy mandates
- Drive the third-party and vendor risk management program, including reviews of security controls, contractual obligations, and integration of risks into the enterprise risk register
- Lead and develop a cross-functional cybersecurity team, fostering collaboration, accountability, and continuous learning across disciplines
- Navigate complex public-sector stakeholder relationships and provide executive-level communication that aligns technical strategies with organizational priorities

DESIRABLE SKILLS AND CAPABILITIES

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

- Strong leadership, decision-making, and executive communication skills
- Deep understanding of enterprise security architecture, regulatory compliance, and operational security models
- Hands-on experience with Zero Trust, DevSecOps, and cloud security strategies
- Proven ability to manage GRC programs and security compliance across large-scale systems
- Experience in building and guiding security teams within complex technical and regulatory environments
- Ability to lead multi-disciplinary teams and navigate complex stakeholder relationships in public-sector environments
- Demonstrated ability to translate technical risk into business impact for executive and non-technical audiences
- Familiarity with public assistance programs and applicable state and federal data privacy laws
- Strong understanding of California state security, risk, compliance frameworks (e.g. SIMM/SAM) and applicable federal regulations (e.g. HIPAA, FIPS, NIST) and MITRE, OWASP, CSF)

QUALIFICATIONS AND REQUIREMENTS

MINIMUM QUALIFICATIONS

TRAINING AND EXPERIENCE:
Graduation from an accredited college or university with a bachelor's degree in Cybersecurity, Information Technology, Computer Science, Information Systems, or a related field, and at least Seven (7) years of progressively responsible experience in cybersecurity, compliance, and risk management, including two (2) years in a senior security leadership role such as CISO

-OR-

Four (4) years of experience as a CISO, Deputy CISO, or similar role in a public-sector organization responsible for enterprise security and risk governance

-OR-

Four (4) years of experience managing security strategy and audit compliance for a large-scale, multi-agency system, including two (2) years of direct supervision of security personnel

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.

PHYSICAL CLASS:

2 - Light.

OTHER REQUIREMENTS

LOCATION:

This is a hybrid role. Applicants need to be in the commutable Greater Sacramento Area.

SPECIALTY REQUIREMENTS

REQUIRED:

- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager

OPTIONAL:

- CCISO – Certified Chief Information Security Officer
- ITIL Foundation (v3 or v4) – Information Technology Infrastructure Library