CalSAWS Job Description

PRIVACY & DATA SECURITY OFFICER

Salary Determined by Employer
RGS Salary Range:
$9,684.12 - $15,375.00 Monthly

JOB DESCRIPTION

Under the direction of the Chief Information Security Officer (CISO), the Privacy & Data Security Officer, is responsible for executing and coordinating day-to-day privacy operations, data security, and security objectives embedded within the CalSAWS Information Security Program. This role enables consistent privacy-by-design by integrating privacy requirements into Security-by-Design workflows, vendor and system reviews, and InfoSec compliance and governance initiatives, while at same time operationalizing security-by design.

RESPONSIBILITIES

The Privacy & Data Security Officer will be responsible for:

Security Program Implementation & Oversight

- Translate CISO-directed strategy into program plans, maturity roadmaps, and measurable program deliverables.
- Develop and maintain enterprise security KPIs and dashboards for leadership, governance bodies, and vendor oversight.
- Oversee the Data Security program
- Perform security review of technical designs, architecture changes, system enhancements, and vendor proposals for adherence to established policies and security/privacy requirements.
- Identify program-level gaps and control deficiencies; recommend solutions and monitor corrective actions to completion.
- Ensure program documentation and controls remain consistent with state and federal expectations for systems handling sensitive data.

Privacy Intake, Triage, and Operational Execution

- Operate the CalSAWS privacy intake process, including monitoring & acknowledging requests, gathering required context, and routing to appropriate reviewers.
- Track requests through completion with clear ownership, timelines, and closure documentation.
- Maintain organized records of requests, decisions, approvals, and supporting evidence for audit and client readiness.
- Coordinate workflow artifacts (DSARs, PIAs, DPIAs, TIAs), ensuring inputs, documentation, approvals, and follow-ups are completed.
- Serve jointly with the CISO as a resource to counties, DHCS, CDSS, CWDA, and vendors on integrated security and privacy practices.

Embedded Privacy-by-Design within Security-by-Design

- Drive privacy-by-design within Security-by-Design reviews by gathering key inputs (data categories, purpose, retention, sharing, access).
- Ensure technical implementation of privacy-related safeguards, including access controls, logging, encryption, and secure data handling practices.

- Prepare decision-ready summaries outlining processing context, risk considerations, and required approvals.
- Promote repeatable standards and playbooks to improve consistency and efficiency.

Third Party and System Review Support

- Perform Third Party Security Risk assessments
- Coordinate privacy components of vendor onboarding and system changes, emphasizing data minimization, appropriate use, retention, and sharing constraints.
- Partner with Procurement and business stakeholders to gather inputs and document outcomes.
- Maintain review artifacts and track remediation actions to closure.

Data Inventories, Records, and Evidence Management

- Conduct structured data inventory activities using standardized templates.
- Maintain accurate, defensible processing records as systems, vendors, and processes evolve.
- Coordinate documentation and evidence for privacy assessments (including DPIAs).
- Support audits and client inquiries by organizing and presenting privacy documentation.

Privacy Awareness Training Support (InfoSec-Owned Program)

- Coordinate privacy-related inputs for the Annual Security training program
- Track training completion and coverage metrics; prepare summary reporting for leadership

Incident Response Coordination

- Serve as operational coordinator for medium-severity security incidents, ensuring proper documentation, containment oversight, and after-action reviews.
- Collaborate with the Security & Operations Manager and vendors to ensure incidents are managed in alignment with defined procedures and SLAs.
- Support privacy investigations and privacy impact assessments by providing technical evidence, system insight, and control verification.
- Ensure incident response workflows include privacy considerations, including escalation and reporting requirements.
- Ensure appropriate escalation, tracking, and record retention.
- Maintain privacy incident documentation for audit and regulatory readiness.

QUALIFICATIONS AND REQUIREMENTS

MINIMUM QUALIFICATIONS

TRAINING AND EXPERIENCE:

- Bachelor’s degree in Information Security, Computer Science, Information Systems, or a related field. Master’s degree preferred.
- Five (5) years of experience in information security, privacy, data security, or a similar operational role.
- Two (2) years of program leadership, governance, or supervisory experience.
- Working knowledge of privacy-by-design principles (data minimization, appropriate use, retention, transparency, and sharing constraints).

- Working knowledge of data security and security architectural reviews
- Experience working in large-scale enterprise or public-sector environments is strongly preferred.
- Experience supporting vendor onboarding, system/security reviews, procurement/TPRM processes, and data inventories/ROPA-style records.
- Experience managing structured workflows (intake, triage, documentation tracking, and closure) across multiple stakeholders.
- Strong organizational, documentation, and follow-through skills; able to manage multiple parallel requests and deliverables across stakeholders.
- Clear, concise written communication, including summaries, decision logs, and audit/client-ready documentation.
- Sound judgment with appropriate escalation of risks or uncertainties; high discretion in handling sensitive information.
- Ability to collaborate effectively with business, procurement, security, and compliance teams.
- Certifications (Preferred)
  - CISSP, CISM, CRISC, CCSP, or equivalent security certifications.
  - Privacy certifications (CIPP/US, CIPT) are desirable.
  - ITIL or similar operational framework certifications a plus.

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

N/A

SPECIALTY REQUIREMENTS

N/A