CalSAWS Job Description

DATA PROTECTION & PRIVACY MANAGER

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 Data Protection & Privacy Manager, is responsible for driving concepts, techniques, and standards across Data Security Posture Management (DSPM), Data Loss Prevention, Insider Risk, and data classification. Working without appreciable direction to identify and evaluate fundamental issues and provide strategy and direction for this functional area as an individual contributor. This role enables consistent privacy-by-design by integrating privacy requirements into Security-by-Design workflows.

RESPONSIBILITIES

The Data Protection & Privacy Manager will be responsible for:

Data Protection and Governance

- Own and build a scalable data protection and governance program, strategy, and operating model ensuring data is accurate, consistent, and secure across enterprise.
- Execute a data protection strategy including DSPM coverage expansion, DLP maturity, and insider risk program.
- Own and oversee the discovery, classification, and risk assessment of CalSAWS data across all environments.
- Define and implement data governance policies aligned with privacy, security, compliance, and ethical AI standards.
- Provide strategy and direction for the full lifecycle of data protection controls spanning data in motion, data at rest, and data in use, across endpoint, cloud, email, and network channels.
- Oversee the development, deployment, and continuous tuning of DLP policies leveraging tools
- Develop and mature the behavioral analytics and detection capability for intentional and accidental data misuse, leveraging Splunk UBA and DLP telemetry to identify anomalous data access, movement, and exfiltration patterns.
- Serve as subject matter expert on data security, data governance, data risk, AI/ML, and emerging data technologies.
- Provide governance oversight for major data programs, AI/ML initiatives, and digital transformation.
- Champion a data-driven and risk-based culture.
- Own the enterprise Insider Risk Program strategy, establish case management, investigation, and escalation protocols for insider risk incidents while preserving integrity and chain of custody.

Security Program Implementation

- Perform security review of technical architectural 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.

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 security & 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, Cybersecurity, or a related field. Master’s degree preferred.

- Five (5) years of experience in information security or data protection, with demonstrated depth in DSPM, DLP, and insider risk disciplines in a multi cloud environment., privacy, data security, or a similar operational role.
- Two (2) years of program leadership, governance, or supervisory experience.
- Hands-on experience in data protection -by-design, AI/ML systems, input/output monitoring, data residency enforcement, and access control.
- Strong understanding of security and privacy principles as they apply to data (access controls, classification, retention, least privilege, auditability)
- 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, CDPSE, CIPM 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