County of Santa Barbara
Chief Information Security Officer

Title

Chief Information Security Officer

Description

The County of Santa Barbara, Chief Information Security Officer's role is to provide vision and leadership for developing and supporting security initiatives. The Chief Information Security Officer directs the planning and implementation of enterprise IT system, business operation, and facility defenses against security breaches and vulnerability issues. This individual is also responsible for auditing existing systems, while directing the administration of security policies, activities, and standards.

Responsibilities

Strategy & Planning

- Participate as a member of the senior management team in governance processes of the organization's security strategies.
- Lead strategic security planning to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment, and management of current and future security technologies using a risk-based assessment methodology.
- Develop and communicate security strategies and plans to executive team, staff, partners, customers, and stakeholders.
- Assist with the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements.
- Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.

Acquisition & Deployment

- Define and communicate corporate plans, procedures, policies, and standards for the organization for acquiring, implementing, and operating new security systems, equipment, software, and other technologies.

Operational Management

- Act as advocate and primary liaison for the company's security vision via regular written and in-person communications with the company's executives, department heads, and end users.
- Work closely with IT department on corporate technology development to fully secure information, computer, network, and processing systems.
- Manage the administration of all computer security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
- Manage the administration of the facility's security systems and their corresponding equipment or software, including fire alarms, locks, intruder detection systems, sprinkler systems, and anti-theft measures.
- Develop, track, and control the security services annual operating and capital budgets for purchasing, staffing, and operations.
- Ensure that facilities, premises, and equipment adhere to all applicable laws and regulations.

- Recommend and implement changes in security policies and practices in accordance with changes in local or federal law.
- Creatively and independently provide resolution to security problems in a cost-effective manner.
- Assess and communicate any and all security risks associated with any and all purchases or practices performed by the company.
- Collaborate with IT leader, privacy officer, and human resources to establish and maintain a system for ensuring that security and privacy policies are met.
- Where necessary, supervise recruitment, development, retention, and organization of security staff in accordance with corporate budgetary objectives and personnel policies.
- Promote and oversee strategic security relationships between internal resources and external entities, including government, vendors, and partner organizations.
- Remain informed on trends and issues in the security industry, including current and emerging technologies and prices. Advise, counsel, and educate executive and management teams on their relative importance and financial impact.

Position Requirements

Formal Education & Certification

- University degree in the field of computer science or business administration. Master's or PhD. degree in one these fields or Information Security preferred.
- Industry Security Certifications such as: CISSP, CISM, CEH, etc.

Knowledge & Experience

- At least 10 years of experience managing and/or directing an IT and/or security operation.
- At least 5 years' experience working in the public sector.
- Proven experience in planning, organizing, and developing IT security and facility security system technologies.
- Experience in planning and executing security policies and standards development.
- Excellent knowledge of technology environments, including information security, building security, and defense solutions.
- Considerable knowledge of business theory, business processes, management, budgeting, and business office operations.
- Substantial exposure to data processing, hardware platforms, enterprise software applications, and outsourced systems.
- Good understanding of computer systems characteristics, features, and integration capabilities.
- Experience with systems design and development from business requirements analysis through to day-to-day management.
- Excellent understanding of project management principles.
- Superior understanding of the organization's goals and objectives.
- Demonstrated ability to apply IT in solving security problems.
- In-depth knowledge of applicable laws and regulations as they relate to security.
- Proven leadership ability.

Personal Attributes

- Ability to set and manage priorities judiciously.
- Excellent written and oral communication skills.
- Excellent interpersonal skills.
- Strong negotiating skills.

- Ability to present ideas in business-friendly and user-friendly language.
- Exceptionally self-motivated and directed.
- Keen attention to detail.
- Superior analytical, evaluative, and problem-solving abilities.
- Exceptional service orientation.
- Ability to motivate in a team-oriented, collaborative environment.

Work Conditions

- On-call availability and periodic overtime.
- Sitting for extended periods of time.
- Dexterity of hands and fingers to operate a computer keyboard, mouse, and other computing equipment.