State Classification Job Description

Information Security Officer

CLASS TITLE	CLASS CODE	SALARY GROUP	SALARY RANGE
INFORMATION SECURITY OFFICER	0238	B31	$123,252 - $208,449

GENERAL DESCRIPTION

Performs highly advanced (senior-level) information security work providing direction and guidance in strategic operations and planning. Work involves developing security and business continuance standards and action plans; developing security architecture and policies based on business needs, risk assessments, and regulatory requirements; and conducting information security risk analysis and system audits. Works under minimal supervision, with extensive latitude for the use of initiative and independent judgment.

DISTINGUISHING CHARACTERISTICS

The Information Security Officer job classification series is intended for employees that direct and determine enterprise-wide information security standards. Employees typically develop and implement information security standards and procedures, ensuring that all information systems are functional and secure. In contrast, the Cybersecurity Officer job classification series focuses on preventing data breaches and monitoring and reacting to cyber-related attacks. Those employees direct the analysis and assessment of vulnerabilities in the infrastructure, investigate available tools and countermeasures to remedy the detected vulnerabilities, and recommend solutions and best practices.

EXAMPLES OF WORK PERFORMED

Directs the deployment of security infrastructure.

Directs the agency risk management program through planning, developing, coordinating, and implementing information technology disaster recovery and business continuity planning.

Directs and/or conducts research related to security trends and technology.

Oversees the implementation of computer system security plans with agency personnel and outside vendors.

Oversees the ongoing development and implementation of statewide information and cybersecurity policies, standards, guidelines, and procedures to ensure information security capabilities cover current threat capabilities.

Develops and implements agency policies for encryption of data transmissions and the erection of firewalls to conceal information as it is being transmitted and to eliminate tainted digital transfers.

Develops and manages information security and risk management awareness and training programs.

Reviews technical risk assessments and new and existing applications and systems, including data center physical security and environment.

Reviews results of special investigations, internal audits, research studies, forecasts, and modeling exercises to provide direction and guidance.

Reviews guidelines, procedures, rules, and regulations; and monitors compliance.

Reviews information security budgets and provides final approval.

Performs related work as assigned.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Experience and/or education in a field relevant to the work being performed. Agencies have the discretion to identify the general or specialized experience, education, or certifications required for positions and may tailor qualification requirements to be specific and meet the agency's business needs. Agencies also may substitute experience and education for one another, if appropriate and allowed by statute.

KNOWLEDGE, SKILLS, AND ABILITIES

- Knowledge of local, state, and federal laws and regulations relevant to information security, privacy, and computer crime; the principles and practices of public administration and management; the limitations and capabilities of computer systems; technology across all network layers and computer platforms; and operational support of networks, operating systems, Internet technologies, databases, and security applications.

- Skill in the use of a computer and applicable software; and in configuring, deploying, and monitoring security infrastructure.

- Ability to direct and organize program activities; to identify problems, evaluate alternatives, and implement effective solutions; to develop and evaluate policies and procedures; to prepare reports; to resolve advanced security issues in diverse and decentralized environments; to communicate effectively; and to supervise the work of others.

REGISTRATION, CERTIFICATION, OR LICENSURE

May require certification as a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), or Certified in Risk and Information Systems Control (CRISC).