Information Technology Security Analyst II

Salary Group: B25
Class Code: 0236

CLASS TITLE	CLASS CODE	SALARY GROUP	SALARY RANGE
INFORMATION TECHNOLOGY (IT) SECURITY ANALYST I	0235	B23	$55,184 - $90,393
IT SECURITY ANALYST II	**0236**	**B25**	**$63,104 - $103,491**
IT SECURITY ANALYST III	0237	B27	$76,356 - $129,137

GENERAL DESCRIPTION

Performs highly complex (senior-level) information security analysis work. Work involves coordinating and/or planning, implementing, and monitoring security measures for information systems and infrastructure to regulate access to computer configuration and data files and to prevent unauthorized modification, destruction, or disclosure of information. May supervise the work of others. Works under limited supervision, with considerable latitude for the use of initiative and independent judgment.

EXAMPLES OF WORK PERFORMED

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

Coordinates agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.

Confers with users to discuss issues such as account permission and data access needs, security violations, and programming changes.

Advises management and users regarding security configurations and procedures.

Designs, automates, manages, and deploys security applications and infrastructure program activities.

Develops and recommends plans to safeguard computer configurations and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.

Modifies and monitors computer configuration and data files to incorporate new software and virus protection systems, correct errors, or change individual access status.

Plans and deploys continuous automated security compliance capabilities.

Monitors, evaluates, and maintains systems and procedures to protect data systems and databases from unauthorized access.

Participates in the development of information technology disaster recovery and business continuity planning.

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

Regulates and reviews access to computer configuration and data files and prevents unauthorized modification, destruction, or disclosure of information.

Researches, evaluates, and recommends systems and procedures for the prevention, detection, containment, and correction of data security breaches.

Trains users and promotes security awareness to ensure system security and to improve application, server, and network efficiency.

May supervise the work of others.

Performs related work as assigned.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Experience in information security analysis work. Graduation from an accredited four-year college or university with major coursework in information technology security, computer information systems, computer science, management information systems, or a related field is generally preferred. Education and experience may be substituted for one another.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge of the limitations and capabilities of computer systems; of technology across all mainstream network, operating system, and application platforms; of operational support of networks, operating systems, Internet technologies, databases, and security applications; and of information security practices, procedures, and regulations.

Skill in the use of computers and applicable software; and in configuring, deploying, monitoring, and automating security applications and infrastructure.

Ability to resolve complex security issues in diverse and decentralized environments, to learn new information and security technologies, to communicate effectively, and to supervise the work of others.