

**Information Technology Security Analyst I**

Salary Group: B23

Class Code: 0235

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

**GENERAL DESCRIPTION**

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

**EXAMPLES OF WORK PERFORMED**

Performs risk assessments and reviews of account permissions, computer data access needs, security violations, and programming changes.

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

Develops plans to safeguard computer configuration 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.

Implements continuous automated security compliance capabilities.

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

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

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

Researches 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.

Assists in designing and deploying security applications and infrastructure program activities.

Assists in advising management and users regarding security configurations and procedures.

May develop information technology disaster recovery and business continuity planning.

May assist in encrypting data transmissions and defining firewall configuration to protect confidential information in transit.

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 applicable software; and in configuring, deploying, and monitoring 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 provide guidance to others.