

Information Technology Security Analyst II

| Job Code | Job Title | Pay Grade |
|----------|--|-----------|
| 1623P3 | Information Technology Security Analyst II | 32 |

CONCEPT:

Plan, coordinate and implement security measures for information systems to regulate access to computer data files and prevent unauthorized modification, destruction, or disclosure of information.

TASKS

- Confer with users to discuss issues such as computer data access needs, security violations, and security related requirements of programming changes.
- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Document computer security and emergency measures, policies, procedures, and tests.
- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Modify computer security files to incorporate new software, correct errors, or change individual access status.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Monitor use of data files and regulate access to safeguard information in computer files.
- Perform risk assessments and execute tests of information technology systems to ensure function and continuity of business computer related programs and activities and security measures.
- Review violations of computer security procedures and discuss with management.
- Coordinate implementation of the computer security system plan.
- Research security and disaster recovery information technologies of potential benefit to the organization.
- Identify and document the projected costs and benefits of information security technology capabilities.
- Coordinate or conduct security related systems training for users and organizational management

LEVELS OF WORK

IT Security Analyst II: This is specialized technical work providing security and disaster recovery for information technology systems. Incumbents will implement, monitor and maintain information technology security and disaster recovery policies and procedures; researches, selects, modifies and maintains security software applications, provides technical assistance to users to resolve security problems, assists users with security requirements, grants access to users, and maintains documentation regarding the software security systems and disaster recovery. Tasks are varied involving several steps and require analytic thought. Assignments are given with general objectives for the desired outcome and incumbent has moderate latitude in establishing priorities and procedures. Work is outcome-oriented with progress reported periodically.

Minimum Requirements: Successful completion of 12 hours in computer science coursework or certification and six months experience in providing security and disaster recovery for information technology systems. Education may be substituted for experience as determined relevant by the agency.

Necessary Special Requirements

Some positions in this class series may require a security clearance at the time of appointment.

NC: 08/05

REV: 7/14

REV: 6/16