

Information Security Analyst

Information Technology Series



Company Overview:

<Please insert a short paragraph talking about your company and what makes it unique. Include details that capture the core values, culture, and mission of your company, so job seekers clearly understand the environment in which they will be working.>

Job Summary and Responsibilities:

Information security analysts plan, implement, upgrade, and monitor security measures for the protection of an organization's systems, computer, networks and data. They may also be responsible for maintaining appropriate security controls and responding to computer security breaches (e.g., viruses). Key responsibilities include maintaining the organization's firewall and other security systems, providing security risk analysis to management, and juggling other complex non-routine work.

<Add any additional responsibilities or changes relevant to this role at your company.>

Required Competencies:

OCCUPATIONAL COMPETENCIES

- **Core Operating Systems:** Familiarity with how to install, configure, maintain and monitor multiple core operating systems (e.g., Windows, Linux, iOS, Android) for computer and mobile devices in local and enterprise-wide scenarios; familiarity with A+ certification domain areas
- **Network Protocols:** Familiarity with how to facilitate and protect communications utilizing common TCP/IP suite protocols like DNS, DHCP, SMTP, SNMP, FTP, TCP, ILS, etc.
- **Information Security:** Familiarity with CISSP domain concepts like how to install, configure, troubleshoot, and maintain networks, hardware, software, etc. in a secure manner to ensure their confidentiality, integrity, and availability; utilize security solutions (e.g., access control, intrusion detection, etc.) to defend, monitor, and remediate; identify, analyze, and mitigate security risks and threats



FOUNDATIONAL COMPETENCIES

- **Critical Thinking:** Use thorough critical analysis to identify risks and rewards of alternative solutions, conclusions, or approaches to problems related to security controls; use independent thought to think outside the box and read between the lines when looking for problems
- **Active Listening:** Give full attention to what superiors and clients are saying, taking care to fully understand by restating what's said, and asking questions to clarify as needed; provide enough feedback to make sure the other person is comfortable you thoroughly understood what's been said
- **Judgment & Decision-Making:** Apply logic when considering the relative risks and rewards of potential actions to choose the appropriate one; evaluate the impact of vulnerabilities and possible solutions; considering both the smaller and larger impacts of a decision to the situation at hand and the organization overall; willingness to take a step back to gather additional, valuable information before acting

Find additional competencies for this role using Skillful's occupation deep dive at www.skillful.com/employers.

Preferred Competencies:

OCCUPATIONAL COMPETENCIES

- **General Networking Tools & Concepts:** Familiarity with how to provide network support for commonly-used tools/devices, including routers, switches, Ethernet, firewalls, frame relay, LAN, VPN, and WAN; understanding of network fundamentals, including network OSI model
- **Auditing:** Ability to examine and analyze system records/logs to monitor status, identify security threats, evaluate risk, and escalate issues; familiarity with audit planning and management concepts from common certifications (e.g., CISA); use analysis to measure performance against baselines

FOUNDATIONAL COMPETENCIES

- **Complex Problem Solving:** Identify complex problems and review related information to develop, evaluate, and implement solutions; solve problems or roadblocks by collecting additional insights or resources to find a solution
- **Systems Analysis:** Determine how a system should work and the downstream business impact of changes in conditions, operations, or the environment; apply risk analysis in the evaluation of inputs and outputs when determining expected outcomes



Example Activities:

- Install systems and software to encrypt data transmissions and erect firewalls to conceal confidential information when transmitted and keep tainted digital transfers out of the system
 - Handle security threats from everyday, limited problems (e.g., desktop virus) and collaborate with others to handle serious, system-wide threats (e.g., virus propagating across the network and sending data externally).
 - Develop plans, policies, and procedures to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs
 - Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated
 - Monitor use of data files and regulate access to safeguard information in computer files
-

Required Certifications:

<Note: Insert Required Certifications *but only if truly required.*>

Job Details:

- Location
- Department
- Job ID
- Classification
- Insert additional details of this position if applicable