IT Security Analyst Job Description

Duties and Responsibilities:

- Actively participates in the daily coordination and remediation of all security incidents in the organization
- Oversees the monitoring, investigating, and reporting of security related events
- Creates updates and oversees execution of security assessments and analysis of systems on a daily, weekly, monthly, quarterly, and annual basis
- Ensures successful compliance of HIPAA, NIGC, MICS, and PCI within the organization
- Conducts assessment on the security of new applications and programs prior to installation or upgrades
- Responsible for monitoring and responding to alerts within the information technology infrastructure
- Responsible for monitoring and ensuring that end-users adhere to Information Technology policies, standards, and best practices
- Responsible for ensuring that all servers and other IT related equipment is hardened for compliance and/or industry standards
- Ensures that company meets all security standards for internal or external audits
- Ensures that all information technology/service diagrams are up to date and appropriately documented
- Identifies and addresses computer vulnerabilities in internal servers, external servers, and applications
- Oversees the administration, documenting, and monitoring inventory control for all network equipment
- Follows the Security Incident Management Response Policy in responding to security incidents
- Guides the Incident Response Team in handling information security incidents
- Provides quick updates of security incidents to the network operations manager

- Improves information security posture through the application of findings from investigation of security incidents
- Responsible for validating and maintaining incident response plan and processes to address potential threats
- Responsible for the compilation and analysis of data for proper reporting and metrics
- Scans and patches applications when vulnerabilities may be present or released
- Performs daily audits of firewall(s), log management, intrusion detection systems, and content filtering controls
- Ensures all levels of staff are provided with relevant trainings on security matters.

IT Security Analyst Requirements – Skills, Knowledge, and Abilities

- Education: IT security analysts require a Bachelor's degree in Computer Science or Information Sciences, or in a similar field from a four-year college or university
- Certification: It is required that IT security analysts are certified. Certifications from accredited bodies, including Certified Information Systems Security Professional (CISSP), CISA (Certified Information Security Auditor), GIAC/CISM/CCIE/CCNA, or other specialized security certifications
- Knowledge: They require 5 years of Information Technology experience, including Network Security experience. However the length of time is variable depending on the hiring organization. it is required that they have knowledge of national and international regulatory compliances, standards, and frameworks such as ISO, SOX, and PCI DSS
- They may also be required to possess knowledge of UNIX and Windows operating systems; good knowledge of networking and routing protocols; experience in Penetration Testing and hacking techniques; good understanding and knowledge of security concepts, protocols, processes, architectures, and platforms (authentication and access control technologies, intrusion detection, network traffic analysis, Web Application Firewalls, Encryption and Key Management, SIEM technology, incident handling, media/malware analysis, etc.)

- Computer skills: It is essential that they possess superior computer skills, and be proficient in software applications currently in use by the company
- Communications skill: They require both verbal and written communication skills to communicate with all members of the IT team in a professional manner, and in order to successfully accomplish departmental and company goals
- Presentation skills: IT security analysts must possess the ability to clearly and effectively present information in one-on-one and small group situations
- Research skills: Their job requires them to carry out investigations on incidences as well as document findings; hence it is essential that they have the ability to define problems, collect data, establish facts, and draw valid conclusions
- Stress management: They must possess the ability to react to high pressure dynamic changing environments in a coordinated and rational manner
- Apt for learning: They must be willing to maintain and update current knowledge of industry best practices for strategy, design, and operational support for information technology security
- It is also important that they are naturally curious people with strong problem solving and analytical skills.