Senior Information Security Analyst

Job Code 50012106

General Description
The Senior Information Security Analyst researches, analyzes, applies and promotes information security best practices within the Information Technology division and across the entire University.

Examples of Duties
Conduct and coordinate risk analysis and assessment of existing and proposed information technology resources. Oversee vulnerability and penetration testing activities and tool utilization. Recommend long and short range courses of actions to minimize risk.
Identify, evaluate, operate and maintain appropriate systems and services to detect security threats and vulnerabilities and to prevent successful breaches and exploits. Develop and analyze network and system metrics for anomalies and potential security issues.
Develop and implement firewall, intrusion prevention, patch management and malware protection policies and solutions.
Address questions from users, other technical staff, law enforcement, and external affiliates regarding information security incidents, issues and best practices.
Provide oversight and management of security incident to prevent additional damage and preserve forensic evidence.
Review network and system records for anomalies and potential security breaches. Prepare incident reports for university management and external regulatory bodies as required.
Facilitate communication of security notices and alerts. Participate in security training for multiple groups from end users to technical support staff. Identify technical training and skill enhancements needed by IT Security.
Actively participate in security and technology groups and associations, both internal and external to the university.
Recommended, draft, and follow policies and procedures to ensure the security of information assets against unauthorized or accidental modification, destruction, or disclosure.
Assist with special project assignments as directed by superiors.

Knowledge, Skills, and Abilities
Knowledge of: Laws, standards, guidelines, and policies relating to information security; computer operating systems; outside resources and contacts; information security tools.
Skill in: problem solving and decision making; prepare clear accurate documents; working with a team
Ability to: Understand reference materials; work under pressure; communicate effectively with both technical and non-technical personnel.

Experience and Education
To qualify for this classification, an individual must possess any combination of experience and education that would likely produce the required knowledge, skills, and abilities.

Other Requirements