Clark Atlanta University
Job Description

Position Title:	**Title III Information Security Analyst II**
Department:	**Office of Information Technology and Communications**
Reports To:	**AVP, Information Services/ Title III Program Administration**

The following statements are intended to describe the general nature and level of work to be performed. They are not intended to be construed as an exhaustive list of all responsibilities, duties and skills required of personnel so classified.

General Function (Description):

The Information Security Analyst II role demands technical proficiency, meticulous attention to detail, and dedication to implementing top-tier security practices. The primary objective is to maintain the confidentiality, integrity, and accessibility of our data, thereby safeguarding sensitive information from potential breaches. In this role, you will be entrusted with the responsibility of safeguarding our organization's digital infrastructure, ensuring that our information systems remain secure and resilient against evolving cyber threats. This position is funded by Title III, a federal grant from the U.S. Department of Education. Continued employment is contingent upon the availability of grant funding. The selected candidate must allocate 100% of their time and effort to work that directly supports Title III program objectives.

Examples of Duties and Responsibilities:

- Implement security measures, including configuring and maintaining security software and systems.
- Install, configure, and maintain security software, tools, and systems such as firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus software, and encryption protocols.
- Monitor networks and systems for security breaches, analyzing logs and alerts for potential threats.
- Respond promptly to security incidents, investigating and mitigating breaches, and documenting findings.
- Manage regular vulnerability assessments and penetration tests, developing and implementing remediation plans.
- Enforce security policies and procedures, providing guidance for compliance with industry standards.
- Develop and deliver security awareness training programs for employees.
- Maintain accurate records of security-related activities and prepare reports (malware occurrences, remediation, and performance reports) for management.
- Prepare reports and presentations for management and regulatory authorities as required.
- Work closely with network administrators, system administrators, and OITC staff, to implement security measures and address security concerns.

Knowledge, Skills and Abilities

- Proven experience in a cybersecurity role, with a strong understanding of security principles.
- In-depth knowledge of networking protocols, operating systems, and security technologies.
- Familiarity with cybersecurity frameworks such as NIST, ISO 27001, or CIS Controls.
- Experience with security tools and software, including firewalls, IDS/IPS, SIEM, antivirus, and vulnerability scanning tools.
- Strong analytical and problem-solving skills, with excellent communication abilities.
- Relevant certifications such as CompTIA Security+, CEH, or GSEC are advantageous.

Minimum Hiring Standards:

Education	Bachelor's degree in Computer Science, Information Technology, or a related field (or equivalent work experience).
Years of Experience Required	Three to five years of industry standard Computer Science or Information Technology.
Years of Management/Supervisor Experience	N/A