Clark Atlanta University
Job Description

Position Title:	**Senior Security Engineer**
Department:	**Office of Information Technology and Communications**
Reports To:	**Vice President, Chief Information Officer**

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):

Reporting to the Vice President, Chief Information Officer, the Senior Security Engineer provides strategic and policy leadership in the implementation and management of the University Information Technology (IT) Security program. Provides ongoing direction for developing, deploying, maintaining, operating, educating on, and evolving the University's IT security architecture, controls, standards, processes and procedures.

Examples of Duties and Responsibilities:

- Provides technical leadership and non-technical leadership, including education, to ensure and increase university information security awareness.
- Provides leadership in establishing University information security architecture, controls, standards, policies, processes and procedures.
- Develops an information security vision and strategy that is aligned to the University's priorities and enables and facilitates the institution's business objectives and ensures senior stakeholder buy-in and mandate.
- Creates a risk-based process for the assessment and mitigation of any information security risk in the University's ecosystem.
- Provides academic and business units with information security risk assessments and provides or assists with the development and deployment of protective measures.
- Works with the compliance staff to ensure that all information owned, collected or controlled by or on behalf of the university is processed and stored in accordance with applicable laws and other global regulatory requirements, such as data privacy.
- Collaborates and liaises with the compliance officer(s) to ensure that data privacy and compliance requirements are enforced where applicable.
- Oversees the monitoring of University-wide security tools and investigates breaches of security controls, taking action according to University established process and procedure.
- Ensures that disaster recovery and business resumption plans exist in alignment with the business (i.e. Business Impact Analysis, Business Continuity, etc.) regulatory requirements (i.e. Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, etc.).

- Works with the CIO, appropriate IT committees, university executives, Deans and top administrators in administrative departments and divisions to ascertain University information security priorities. Works with the Governance process on funding for identified priorities.
- Directs multiple complex information security development projects, information identity and access management processes, and manages information security systems so that the day-to-day IT functions of the University supporting teaching, learning, and administration can work securely.
- Monitors the external threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action.
- Creates and manages a targeted information security awareness training program for all students, faculty, and staff and establishes metrics to measure the effectiveness of this security training program for the different audiences.
- Understands and interacts with University regents, administrative and academic units through committees to ensure the development of and consistent application of policies and standards across all technology projects, systems and services, including privacy, risk management, compliance and business continuity management.

Knowledge, Skills and Abilities

- Proven and extensive experience in planning, organizing, developing and implementing IT security strategies and related initiatives.
- Should have strong leadership, management, and team-building skills.
- Proficiency in IT security management, industry best practices and standards.
- Proven ability to identify, prioritize, and communicate impact of IT security initiatives.
- Substantial knowledge and exposure in developing and testing business continuity and disaster recovery plans.
- Experience in and knowledge of IT security auditing.
- Proven ability to measure, monitor, and report on the success of IT security related initiatives.
- Understanding of effective IT security system and network architectures, concepts, techniques, and tools.
- Understanding and experience managing network and system security components such as firewalls and intrusion detection/prevention systems.
- Knowledge of applicable IT security related laws and regulations.
- Substantial exposure to the operation of institution-wide networks, systems, and applications.
- Proven ability to work effectively in a coordinating role across multiple constituencies to achieve tactical and strategic goals.
- Proven ability to direct the development and implementation of short and long-term cohesive IT security strategies.
- Ability to work effectively with administrators, faculty, and staff.
- Excellent oral and written communication skills.
- Self-motivated and self-directed/driven.

- Excellent analytical, evaluative, and problem-solving capabilities.
- Positive attitude, proven ability to work successfully with diverse populations and demonstrated commitment to promote and enhance diversity and inclusion.

Minimum Hiring Standards

Education	Bachelor's degree or equivalent experience required
Years of Experience Required	Eight (8) years of experience in a combination of IT Security, IT Risk Management and general IT positions; Experience developing and implementing IT security policies and procedures.
Years of Management/Supervisor Experience	N/A

Preferred Qualifications

Education	Advanced degree preferred
Certifications	Certifications such as CISSP (Certified Information Systems Security Professional), CISM (ISACA Certified Information Security Manager), CISA (ISACA Certified Information Systems Auditor), or Security+ preferred
Experience	Experience working in an IT department at higher education institutions preferred