Position – Director of Information Security

About the Clemson University Foundation (CUF)

CUF seeks financial support through annual gifts, capital campaigns, planned giving and other ongoing fund-raising programs. CUF manages and disburses assets prudently within a policy that encourages the enhancement of the resources of the Foundation.

Position Description

Job Department:	Director of Information Security
Reports to:	Chief Technology Officer
Job Location:	Clemson, South Carolina – Hybrid Work Schedule
Minimum Education:	Bachelor's Degree
Work Schedule:	Standard Hours – 37.5/week
Expected Salary Range:	($107,000 - $129,000)

To apply: Email a cover letter and resume to CUFHR@clemson.edu.

Position Summary

The Director of Information Security develops and manages the security strategy, overseeing application security, compliance, and risk management for the Clemson University Foundation and Clemson Advancement. This role involves ensuring robust security for systems and applications, advising executive leadership, and integrating security into the software development lifecycle.

Job Duties

Strategic Security Management *– 50%*

Develop and oversee the enterprise security strategy, ensuring compliance with standards and regulations (e.g., FERPA, PCI, GDPR). Conduct security assessments, design security architectures, and integrate security practices into the software development lifecycle.

Incident Response & Risk Management *– 20 %*

Investigate and remediate security incidents, collaborating with development teams for quick resolution. Develop security policies and manage vendor risk. Create and implement risk-based management processes.

Audit and Process Improvements *– 20 %*

Recommend and evaluate security tools. Enhance security processes to address emerging threats. Ensure system compliance with industry standards and assist with audits. Communicate security risks and strategies to technical and non-technical stakeholders.

Training and Education *– 10%*

Develop and deliver training on secure coding and application security. Enforce security policies.

Requisite Knowledge

Technical Skills: Expert in information system security and risk management. Proficiency in programming languages such as C, C++, C#, PHP, and Java, as well as expertise in firewall protocols and operating systems including Windows, Macintosh, Unix, and Linux. Must have a proficient understanding of the software development lifecycle.

Cybersecurity Fundamentals: Understanding of risk assessment, compliance, network and security architectures, and threat modeling.

Managerial Abilities: Strong in project management, security assessment, and service oversight. Capability to lead teams and interact effectively with stakeholders.

Strategic Thinking: Skill in anticipating emerging threats and implementing preventive measures. Proficient in security testing tools, secure coding practices, and vulnerability management.

Incident Response: Experience in coordinating or planning for rapid and effective responses to incidents. Excellent problem-solving, communication, and documentation skills.

Basic Skills

Leadership: Exhibit exemplary management behavior including integrity, leadership, team building, and good judgment to achieve organizational goals. Communicates with executive management and all users on information technology security, services, and systems.

Well Organized: Maintains quality support by establishing and enforcing organizational security standards. Review service level agreements and contracts for security and backup concerns.

Communication: Excellent interpersonal, written/verbal communication and leadership skills with the ability to make recommendations to all levels of the organization.

To apply: Email a cover letter and resume to CUFHR@clemson.edu.

Equal Employment Opportunity Statement: Clemson University Foundation is an Equal Employment Opportunity employer. We make every effort to provide fair and equal treatment based on merit in all our employment decisions, including but not limited to decisions concerning hiring, retention, promotions, working conditions, compensation, benefits, training, and all other privileges, terms, and conditions of employment. We pledge to treat all employees fairly without regard to race, color, religion, sex, sexual orientation, gender identity and/or expression, pregnancy, national origin, age, disability, genetics, military or veteran status, or any other characteristic protected by applicable law.