FLORIDA STATE COLLEGE AT JACKSONVILLE
JOB DESCRIPTION, 2025

CHIEF INFORMATION SECURITY OFFICER

FLSA STATUS: EXEMPT – PAY GRADE: 29 - A

JOB FAMILY: INFORMATION TECHNOLOGY – JOB FUNCTION: BUSINESS SERVICES

GENERAL STATEMENT OF JOB

The Chief Information Security Officer (CISO) oversees the strategic, comprehensive, and enterprise-wide information security and IT risk management program to ensure the security, integrity, and availability of data, data systems, and data networks across the entire College. This position oversees the day-to-day operations of existing security solutions and addresses and resolves security breaches. This position leads efforts to safeguard and protect the College's IT assets and associated technology, applications, systems, infrastructure, processes, and sensitive data and ensures compliance with global laws, regulations, and industry standards. This position proactively collaborates with departments to implement security best practices and aligns with the College's strategic goals. The CISO works directly with the Chief Information Officer (CIO) to determine acceptable levels of risk and provides guidance on the evolving cybersecurity landscape.

CHARACTERISTIC DUTIES AND RESPONSIBILITIES

Supports the development and execution of the College's information security governance program, including establishing a cybersecurity steering committee or advisory board. Works closely with College staff to ensure compliance with applicable laws, global regulations, and data privacy requirements. Collaborates with the Data Privacy Officer to integrate privacy considerations as necessary. Provides regular status updates to the Chief Information Officer (CIO), enterprise risk teams, senior leaders, and board members.

Contributes to the development and implementation of an enterprise-wide information security vision and strategy aligned with the College's business objectives. Designs, implements, and maintains a comprehensive cybersecurity framework to safeguard the integrity, confidentiality, and availability of institutional data.

Manages security risk management programs, ensuring information security is embedded into enterprise architecture. Works with business units to integrate risk mitigation processes and improve security posture across departments. Ensures security is embedded in the College's technology strategy and project delivery process, providing risk assessments for technology initiatives, third-party contracts, and cloud security.

Develops, maintains, and enforces information security policies, standards, and guidelines to address global regulatory requirements and evolving cyber threats. Works with internal and external stakeholders to ensure compliance with FERPA, HIPAA, GLBA, NIST, and other regulatory frameworks.

Manages and delivers targeted cybersecurity training and awareness programs for all employees and authorized system users. Establishes metrics to measure security awareness effectiveness.

Prepares and manages information security budgets and monitors for variances to ensure cost-effective security investments.

Leads the security incident response process, including rapid containment and mitigation of security breaches, coordination of response actions, and collaboration with law enforcement or regulatory agencies when necessary. Monitors emerging threats and cybersecurity risks, advising stakeholders on proactive measures. Oversees the College's vulnerability management program and risk assessments, ensuring prompt remediation of security gaps.

Enhances the information security management framework, leveraging industry best practices such as the NIST Cybersecurity Framework, ISO 27001. Establishes a structured approach to risk ownership, accountability, and security governance.

Serves as the College's primary cybersecurity liaison, collaborating with external agencies, including law enforcement, advisory bodies, peer institutions, vendors, and regulatory organizations.

Develops and oversees disaster recovery and business continuity strategies, ensuring alignment with enterprise resilience goals. Coordinates testing and execution of security recovery plans.

Ensures the security, privacy, and integrity of digital environments and systems of the College to support student success.

Performs other related duties, as required.

SUPERVISION RECEIVED

Supervision is received from the supervising administrator.

SUPERVISION EXERCISED

Supervision is exercised over assigned staff.

MINIMUM QUALIFICATIONS

Bachelor's degree in a related field from a regionally accredited institution and two (2) years of related experience and working knowledge of key laws, frameworks, and guidelines used in managing and protecting information like FERPA (Family Educational Rights and Privacy Act, HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), ITIL (Information Technology Infrastructure Library and NIST (National Institute of Standards and Technology).

PREFERRED QUALIICATIONS

Bachelor's degree from a regionally accredited institution and five (5) years of related experience and a Certified Information Systems Security Professional (CISSP) certification.

MINIMUM QUALIFICATIONS OR STANDARDS REQUIRED TO PERFORM ESSENTIAL JOB FUNCTIONS

Physical Requirements: Must be physically able to operate a variety of machines and equipment including computer, office equipment, telephone, etc. Physical demands are essentially those of sedentary work. Tasks may require extended periods of time at a keyboard or workstation.

Data Conception: Requires the ability to compare and/or judge the readily observable, functional, structural, or compositional characteristics (whether similar to or divergent from obvious standards) of documentation, files, accounts, and equipment.

Interpersonal Communication: Requires the ability to speak and/or signal people to convey or exchange information. Includes issuing and receiving assignments, instructions, and/or directions.

Language Ability: Requires ability to read Standard English, as well as basic technical data, policy and procedure manuals, codes, etc. Requires the ability to prepare forms and reports using prescribed formats. Requires the ability to communicate with a broad array of individuals from various professional backgrounds.

Intelligence: Requires the ability to apply principles of logical thinking to define problems, collect data, establish facts, and draw valid conclusions; to interpret a variety of instructions or inquiries furnished in written and/or oral form; to acquire knowledge of topics related to occupation.

Verbal Aptitude: Requires the ability to record and deliver information, to explain procedures, and to follow oral/written instructions. Must be able to communicate effectively with co-workers, the public, and students.

Numerical Aptitude: Must be able to add, subtract, multiply and divide; calculate decimals and percentages.

Form/Spatial Aptitude: Requires the ability to inspect items for proper length, width, and shape, and visually read various information.

Motor Coordination: Requires the ability to coordinate hands and eyes accurately in operating modern office equipment and machinery.

Manual Dexterity: Must have minimal levels of eye/hand/foot coordination.

Color Discrimination: May not require the ability to differentiate between colors and shades of color.

Interpersonal Temperament: Requires the ability to deal with people beyond receiving instructions. Must be adaptable to performing under moderate levels of stress, imposed by frequent deadlines, peak workloads, or public/student contact.

Physical Communication: Requires the ability to talk and hear: (talking - expressing or exchanging ideas by means of spoken words; hearing: perceiving nature of sounds by ear).

Environmental Requirements: Tasks are regularly performed without exposure to adverse environmental conditions (e.g., dirt, cold, rain, fumes).

Effective: 07/17/2025