



Position Title:	Chief Information Security Officer	Job Code:	0706-00E
Reports To:	VP, Chief Information Officer	Job Group:	PEC
Department:	Information Systems	Salary Grade:	19
Prepared By/Date:	C. Flynn 07/2007	FLSA Status:	Exempt
Approved By/Date:	K. Herleman 07/2007		
Revised:	Jennifer C. Brito/11-25-2009		

Summary:

The Chief Information Security Officer (CISO) reports directly to the college Vice Provost, Chief Information Officer and is responsible for the information security of Miami Dade College and the coordination of information security efforts across the college. The CISO coordinates the process to build a college-wide information security strategy and vision. The CISO oversees the creation and maintenance of the over-arching MDC information security policy, leads security risk assessment efforts, leads disaster recovery and business continuity planning and owns the college's awareness and training program.

Essential Duties and Responsibilities:

- Manages the development, implementation, and maintenance of MDC information security and privacy policies, standards, guidelines, baselines, processes and procedures in compliance with state and federal regulations and standards.
- Leads the college's incident response, information security training and awareness, disaster recovery and business continuity teams.
- Manages operating budget of \$600k to \$750k and is responsible for subordinates' salaries of \$140k to \$700k.
- Monitors and reports on the security operations and maintenance teams' functions, activities and compliance.
- Provides security direction and oversight on all IT-related systems and projects.
- Performs security assessments of all third-party access and outsourcing contracts.
- Provides guidance and advocacy of regarding prioritization of infrastructure investments that impact information security.
- Monitors information security trends and keep MDC's senior management informed about information security related issues and activities affecting the college.
- Understands potential threats, vulnerability, control techniques, and communicate this information to senior management.
- Maintains relationships with local, state, and federal law enforcement and other related government agencies.
- Develops an information security training and awareness program.
- Acts as ombudsman for disputes, requests for exceptions, and complaints regarding college-wide information security systems security policies, practices and related issues.
- Manages the information security assurance team including user provisioning.
- Performs other related duties as assigned.

Knowledge, Skills and Abilities:

- Knowledge and understanding of higher education, governmental agency or corporate/industry information security experience; CISO preferred.
- Knowledge of related Acts: Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability Accountability Act (HIPAA), Gramm-Leach-Bliley (GLB) Act,

Communications Assistance for Law Enforcement Act (CALEA).

- Knowledge and understanding of college organization, goals and objectives, and policies and procedures.
- Knowledge of the current and developing information technology services requirements in a large educational institution.
- Knowledge of industry information technology and impact on processes.
- Knowledge of business continuity planning, auditing and risk management.
- Knowledge of formal asset classification and control procedures.
- Knowledge and experience with vendor and contract negotiation.
- Persuasive leader who can serve as an effective member of the leadership team and communicate information security related concepts to a broad range of technical and non-technical employees.
- Excellent organizational and communication skills (both oral and written).
- Strong interpersonal skills and the ability to effectively communicate with a wide range of individuals and constituencies in a diverse community.
- Ability to write reports, business correspondence, and procedure manuals.
- Ability to read, analyze, and interpret general business periodicals, professional journals, technical procedures, or governmental regulations.
- Ability to work and effectively prioritize in a highly dynamic decentralized work environment.
- Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.
- Ability to effectively present information and respond to questions from top management, groups of managers, clients, customers, and the general public.
- Ability to solve practical problems and deal with a variety of concrete variables in situations where only limited standardization exists.
- Ability to carry out supervisory responsibilities in accordance with the College's policies and applicable laws, including: interviewing, hiring, and training employees; planning, assigning, and directing work; appraising performance; rewarding and disciplining employees; addressing complaints and resolving problems.
- Ability to work with user communities of diverse backgrounds and skill levels.

Work Environment:

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job.

While performing the duties of this job, the noise level in the work environment is usually moderate.

Physical Demands:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is regularly required to sit and reach with hands and arms; use hands to finger, handle, or feel objects, tools, or controls; talk or hear; and stand and walk.

Specific vision abilities required by this job include close vision, distance vision, color vision, peripheral vision, depth perception, and the ability to adjust focus.

Essential Personnel:

This function/position has been designated as "essential." This means that when the College is faced with an institutional emergency, employees in such positions may be required to remain at their work

location or to report to work to protect, recover, and continue operations at the College.

Minimum Requirements:

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily.

- Bachelor of Science (BS) from an accredited college/university in a related field of study such as Computer Science or Information Systems and eight (8) to ten (10) years of progressive experience in computing and information security preferably in an academic environment; or an equivalent combination of education and experience.
- To perform this job successfully, an individual must possess proficiency in Microsoft Windows and Microsoft Office applications to include Excel, PowerPoint, Project, Word, as well as email (Outlook) and Internet browser applications. Mac OS X, z/OS platforms and Unix/Linux operating systems preferred.
- Must be proficient in the following languages: Visual Basic, HTML and related internet languages and scripting.
- Database Management System requires MS SQL Server and MS ISA Server knowledge.
- CISSP or other related security accreditation/certification required.
- Employee may travel up to 10%.

ACKNOWLEDGEMENT

I have read and acknowledge receipt of a copy of my job description.

Signature

Date

Printed Name