Classification Description

Job Title: Information Security Officer   **Pay Grade:**   TE010

Job Code: T061   **FLSA Status:**   Exempt

Job Purpose

The Information Security Officer will implement and monitor security controls to prevent unauthorized access to sensitive information stored at Florida SouthWestern State College. The Information Security Officer will be responsible for monitoring and verifying account creation and termination. Daily maintenance will include; monitoring, maintaining, and implementing enterprise wide security equipment (Firewalls, Antivirus Servers, Patch Management Systems, etc.), security applications, security processes, and troubleshoot security system errors.

General Responsibilities

Essential Functions

Manages the development, implementation, and maintenance of the Florida SouthWestern State College information security and privacy policies, standards, guidelines, baselines, processes and procedures in compliance with state and federal regulations and standards.

Conducts security risk assessments on all computing systems and components, both new and current, utilizing the appropriate security diagnostic tools.

Monitors and reports possible security deficiencies and assists with corrective action; this includes but not limited to desktop antivirus and security update plans.

Evaluates, understands and implements security standards (NIST) to ensure the College is compliant with both state and federal security requirements.

Assists in the evaluation, design and improvement of the desktop and server systems' security patch management process.

Coordinates the development and maintenance of information security policies and standards.

Monitors and ensures compliance with the College Information Security policy.

Assists the College's General Counsel in performing public record requests as it relates to technological needs.

INFORMATION SECURITY OFFICER

Monitors the internal control systems to ensure that appropriate access levels are maintained.

Provides security direction and oversight on all Information Technology related systems and projects.

Develops information security training and awareness programs as directed.

Identifies and responds to potential threats, vulnerability, control techniques, and communicates this information to senior management.

Monitors information security trends and keeps senior management informed about information security related issues and activities affecting the College.

Acts as regulator for disputes, requests for exceptions, and complaints regarding College wide information security systems security policies, best practices and security related issues.

Monitors LAN/WAN to include: implementation, intrusion detection, remote access and vulnerability reports.

Implements and manages IDS/IPS, firewalls, URL, dlp, packet filters, concentrators, and proxy services required to control access.

Monitors protection levels and security related events.

Monitors and reports on the security operations and maintenance teams' functions, activities and compliance.

Provides guidance with maintaining a Disaster Recovery Plan for network.

Participates in departmental meetings, in-service training and other activities as required; attends conferences, seminars and professional meetings as designated.

Provides and maintains cellular telephone and high-speed internet technology services, which allow immediate accessibility to the College through text and voice messages by cellular phone, and responds as directed.

These essential job functions are not to be construed as a complete statement of all duties performed; employees will be required to perform other job-related duties as required. An employee with a disability is encouraged to contact the Human Resources Office to evaluate the job in greater detail in order to determine if she/he can safely perform the essential functions of this job with or without reasonable accommodation.

<u>Knowledge, Skills and Abilities</u>

<u>Minimum Qualifications</u>

Bachelor's degree from a regionally accredited institution of higher education in computer science or related area of specialization.

Five years (5) of related technical network experience <u>with the last two (2) years</u> of experience devoted to information technology security.

One or more of the following:
- Three (3) years' experience with implementing and maintaining a centralized AV solution
- Three (3) years' experience with implementing and maintaining a centralized patch management solution
- Five (5) years' experience securing windows systems and account rights
- Five (5) years' experience in securing publicly accessed systems, i.e. web servers and centralized storage systems

Demonstrated experience using a personal computer, office software such as MS Office and electronic mail.

Demonstrated ability to:
- Think critically and creatively, have a high standard of integrity, and be motivated to incorporate best practices into the organizational culture.
- Exhibit a thorough knowledge of policies, procedures, and outside regulations pertaining to the position.
- Possess a working knowledge of operational and fiscal analysis techniques.
- Make presentations in front of various group sizes.
- Take initiative and independently plan, organize, coordinate and perform work in various situations where numerous and diverse demands are involved.
- Anticipate, investigate, and analyze problems and address them proactively.
- Communicate effectively, both orally and in writing.
- Establish and maintain effective working relationships with faculty, staff, students and the public.
- Work in a fast-paced, demanding environment.
- Work independently and follow through on assignments.
- Exhibit solid organizational skills and be detail oriented.
- Work with a variety of constituencies and be willing to contribute to a team effort.
- Exercise discretion and good judgment at all times and in all contexts and maintain confidentiality.
- Work effectively with all constituencies of the College.
- Collect, organize, analyze and present information in a meaningful manner.
- Collaborate and be effective working with diverse populations.

INFORMATION SECURITY OFFICER

Critical Skills/Expertise

All employees are expected to:
- Promote a common purpose consistent with stated College goals and demonstrate a commitment to students and the learning environment.
- Possess the knowledge of general written standards and procedures utilized, and have the ability to read, interpret, and follow procedural and policy manual related to the job tasks.
- Demonstrate the ability to respond to supervision, guidance and direction in a positive, receptive manner and in accordance with stated policies.
- Provide quality customer service by creating a welcoming and supportive environment.
- Present a professional image in word, action and attire.
- Demonstrate professionalism in dealing with a diverse population while understanding and respecting each other's view of the world, personalities and working styles.
- Conduct oneself in a manner consistent with the College's standards of ethical conduct.
- Apply effective techniques to create working relationships with others to achieve common goals; successfully communicates and collaborates with others to achieve goals.
- Demonstrate skills necessary to look at situations and processes critically to make recommendations for improvement.

Work Conditions/Physical Demands/Special Conditions

Physical: Routinely requires the ability to see, hear, and speak. Routinely requires sitting, bending, stooping, walking. On occasion, incumbents may be required to lift 20 or more pounds.
Environmental: Normal general office.
Mental: Routinely requires the ability to interpret, analyze and perform critical thinking skills.

Approved: November 23, 2010. Revised: May 9, 2011, March 18, 2013, July 1, 2014, and July 7, 2022.