

# Security Manager

**Job Title:** Security Manager  
**Department:** Media, Computer, and Telecommunications Services  
**Supervisor:** Assistant Vice President for Technology  
**Date:** June 2006  
**Updated:** April 2008

## **A. PURPOSE OF THE JOB:**

The Information Technology (IT) Security Manager's role is to provide vision and leadership for developing and supporting security initiatives. The Information Technology Security Manager directs the planning and implementation of enterprise IT system, business operation, and facility defenses against security breaches and vulnerability issues. This individual is also responsible for administering audits of existing systems while directing the administration of security policies, activities, and standards.

## **B. DUTIES:**

1. Major duties:
  - a. Participates as a member of the senior information technology management team in governance processes of the organization's security strategies,
  - b. Leads strategic security planning to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment, and management of current and future security technologies,
  - c. Develops and communicates security strategies and plans to executive team, staff, partners, customers, and stakeholders,
  - d. Develops, implements, maintains, and oversees enforcement of policies, procedures, and associated plans for system security administration and user system access

based on law, system policies, and industry-standard best practices,

- e. Acts as advocate and primary liaison for the University's security vision via regular written and in-person communications with the officers of the universities, department heads, and end users,
- f. Works closely within the IT department on campus technology development to fully secure information, computer, network, and processing systems,
- g. Manages the administration of all computer security systems and their corresponding or associated software including firewalls, intrusion detection systems, cryptography systems, and anti-virus software,
- h. Coordinates with University Police and Safety the management and administration of the facility's security systems and their corresponding equipment or software including; fire alarms, locks, intruder detection systems, sprinkler systems, and anti-theft measures,
- i. Develops, tracks, and supervises the security services annual operating and capital budgets for purchasing, staffing, and operations,
- j. Ensures that facilities, premises, and equipment adhere to all applicable laws, Texas A&M System (TAMUS) polices, Department of Information Resources regulations, and Texas Administrative Code,
- k. Recommends and implements changes in security policies and practices in accordance with changes in local, TAMUS, state or federal law, policies, and rules,
- l. Creatively and independently provides resolution to security problems in a cost-effective manner,
- m. Defines and communicates University plans, procedures, policies, and standards for the organization for acquiring, implementing, and operating new security systems, equipment, software, and other technologies,

- n. Assesses and communicates any and all security risks associated with any and all purchases or practices performed by TAMU-CC,
- o. Collaborates with IT leaders, privacy officer, and Human Resources to establish and maintain a system for ensuring that security and privacy policies are met,
- p. Assists with the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements,
- q. Where necessary, supervises recruitment, development, retention, and organization of security staff in accordance with TAMU-CC budgetary objectives and personnel policies,
- r. Promotes and oversees strategic security relationships between internal resources and external entities, including government, vendors, and partner organizations, and
- s. Remains informed on trends and issues in the security industry including current and emerging technologies and prices. Advise, counsel, and educate executive and management teams on their relative importance, and financial impact.

2. Occasional and subordinate duties: Performs other duties as assigned.

**C. KNOWLEDGE AND SKILLS:**

1. Required education:

- a. Bachelor's Degree in Computer Science, Management Information Systems (MIS), Business Administration or related area,
- b. Master's or PhD. Degree in Computer Science, MIS, or Business Administration,
- c. Certification in CISSP, and
- d. At least three years experience as an information security professional for state agency or large corporation.

2. Skills required:

- a. Proven experience in planning, organizing, and developing IT security and facility security system technologies,
- b. Experience in planning and executing security policies, and standards development,
- c. Excellent knowledge of technology environments, including information security, building security, and defense solutions,
- d. In-depth knowledge of applicable laws and regulations as they relate to security,
- e. Proven leadership ability,
- f. Excellent written and oral communication skills,
- g. Excellent interpersonal skills,
- h. Strong negotiating skills, and
- i. Must be able to lift 40 lbs.

**D. FISCAL RESPONSIBILITY:**

Incumbent has no direct fiscal responsibility, but is required to evaluate systems and make recommendations to the Assistant Vice President for Technology.

**E. APPLICATION OF KNOWLEDGE AND SKILLS:**

The most creative aspects of the job related duties include the development of security and technology pertaining to University Rules and Procedures and information technology security training designed for University students, staff, and faculty. The incumbent combines these efforts with other aspects of information security such as campus-wide system and network assessments, and to develop a complete security framework that is being integrated into the University's daily operations.

The most challenging part of fulfilling the duties of this position includes maintaining good communications and developing strong relationships with a wide variety of University staff and faculty. The incumbent must leverage these working relationships to help integrate information security throughout the University in a manner that strengthens departmental and business continuity while minimizing the impact the day- to- day operations. These relationships are also utilized during the infrequent situations pertaining to potential or actual information security related incidents. To properly fulfill these duties the incumbent is required to maintain knowledge and training on a wide variety of system and network resources relating to security as well as day- to- day operations.

**F. SUPERVISION:**

The incumbent has no direct supervision of University employees, but must advise, mentor, and train these employees on information security- related issues.

**G. EXTENT OF PUBLIC CONTACT:**

The incumbent is required to interact with all members of the University community, TAMUS personnel, and personnel in state regulatory agencies.

1. Within the University: daily contact daily contact occurs with staff.
2. Weekly contact: occurs with students, faculty, staff, and vendors.
3. Periodic contact within the University: occurs with senior administrative personnel.
4. Periodic contact outside of the University: occurs with a wide variety of non-University personnel to include a variety of vendors and personnel from other state agencies and schools.