Director of Information Security Services  
(University Manager)

DESCRIPTION

The Director of Information Security Services is the leader of the data/information security function for Stanford University, which includes responsibility for information security strategy, security architecture development, and global function oversight. The scope of this role covers all utilized enterprise technologies, including mainframe, distributed and infrastructure-based systems. As the university’s senior information security officer, this person also has enterprise-level responsibility for all data/information security policies, standards, evaluations, roles and university-wide awareness. This person will work with user, technical, internal audit and risk management in the development and implementation of an information security strategy, designed to provide a high level of security over information processing resources while preserving and enhancing system usability.

The Director of Information Security Services reports directly to the Executive Director of Information Technology Systems and Services (ITSS) and also has a reporting relationship to the Director of Internal Audit specifically for oversight and support in the conduct of special security analyses and network and application intrusion studies.

This person will be responsible for directing the activities of the data security function. Responsibilities will include the following:

- Develop, implement and manage the overall enterprise process for information security strategy and the associated architecture.
- Develop and implement policies, standards and guidelines related to information security.
- Oversee the continuous monitoring and protection of information processing resources. Evaluate suspected security breaches and recommend corrective actions.
- Serve as the enterprise focal point for computer security incident response planning and execution.
- Define and implement an ongoing Stanford University risk assessment program, which will define, identify and classify critical information assets, assess threats and vulnerabilities regarding those assets and implement safeguard recommendations.
- Assist internal audit in the development of appropriate criteria needed to assess the level of new/existing applications and/or technology infrastructure elements for compliance with enterprise security standards.
- Assist in the review of applications and/or technology environments during the development or acquisitions process to (1) assure compliance with university security policies and directions and (2) assist in the overall integration process regarding Stanford’s own technology environment.
- Oversee the development, and be the enterprise champion, of a corporate security awareness training program.
- Manage security functions related to university information systems or data centers.
- Evaluate changes to the processing environment for security impact and present findings to management.
- Assist schools, departments, and administrative offices in applying best practices in securing the data and information systems under their control.
- Evaluate and recommend to management security features and products related to all information processing environments, firewalls, client/server, networks — local area network (LAN)/wide area network (WAN) — Wireless Networks and distributed systems.

QUALIFICATIONS/EXPERIENCE

This person must be able to develop and implement flexible security solutions, dictated by the needs of a hybrid and rapidly evolving centralized/decentralized academic and business environment. The individual must be a results-oriented person who can achieve tangible improvements in the data security arena.
The candidate will have the following:

- A college degree (BA/BS) or equivalent work experience
- Excellent staff management skills
- The ability to interface with top management
- Eight to 10 years of information systems processing experience
- Familiar with information security concepts and objectives
- Excellent communication skills, both written and verbal
- A business-based attitude; i.e., the recognition that no policies can be implemented without demonstrable academic or business benefit
- Customer service experience
- Awareness of the following:
  - Vulnerability testing in addition to penetration testing
  - Developing security practices as a people problem vs. a technical problem
  - Standards-based architecture, with an understanding of how to get there, including compliance