POSITION TITLE:
Director of Information Security and Compliance

REPORTS TO:
Assistant Vice President for Information Technology

POSITION SUMMARY:
Under the general direction of the Asst. Vice President for Information Technology, and in conjunction with other areas of the University and external organizations when necessary, the Director of Information Security and Compliance is responsible for high-level analysis, development, interpretation, and professional development related to information and system security policy, practices and assessment, as well as disaster recovery and business continuity.

POSITION DETAIL:
In relation to the above activities, the Director of Information Security and Compliance interacts and coordinates with LMU administration, campus and department technology representatives, ITAC and other computer and policy advisory groups, LMU governance bodies, and external authorities as necessary. This individual serves as advisor to the Assistant Vice President and other University executive administrators on issues of information security and policy compliance. This Director will assist as a member of the management team for the office of Information Technology Services, advising and supporting the various Directors in areas of security and compliance.

Under the direction, and with the support, of the Asst Vice President for Information Technology, The Director of Information Security and Compliance plans, directs and participates in technology security assessment activities, program planning and reporting for LMU. Attends conferences and training, and interacts with external peers as required to maintain knowledge of current issues and best practices. The Director participates actively in security-related industry efforts, providing value to LMU through such participation. He or she serves as the University-designated Information Security and Compliance officer when required by legal authority.

Specific activities include:

- Analyzing issues related to information technology security policy – assessing current issues, performing legal research and reporting findings.
- Developing technology appropriate use policies in conjunction with university administrators, committees, and governance bodies.
- Developing and administering appropriate sensitive information handling and storage policies, as well as awareness and education programs.
- Reviewing current technology and information policies and practices for continued applicability and effectiveness with respect to security and governmental compliance.
- Analyzing and tracking reports of inappropriate use of technology and institutional/personal information, including computer security incidents, and guides the investigation and resolution of such incidents.
- Interacting with students, faculty and staff and their respective governance organizations to resolve complaints and issues related to the inappropriate use of technology and institutional/personal information.
- Developing and administering security education and awareness programs.
- Reviewing and reporting on proposed information technology and privacy-related legislation, and providing advice on potential impact to University operations.
- Overseeing the design and administration of computer account provisioning for LMU systems Determining the appropriate design and maintenance of global directory services, identification, authentication, and authorization mechanisms.
- Developing a common and consistent set of account and access procedures for users of LMU networks and systems.
- Overseeing and approving the design and deployment of network and application security controls, including the approval of access controls, network and data architectures, and logging and monitoring tools.
- In conjunction with the AVP for Information Technology, interacting with the Chief Financial Officer, Internal Audit, University Counsel and other internal control resources, as well as external civil and law enforcement authorities, to promote mutual cooperation.
- Coordinating the development and maintenance of disaster recovery and business continuity/resumption plans and procedures, for the timely recovery of critical business and academic functions supported by the office of Information Technology Services.
- Assessing and reporting on computer systems and telecommunications security risks.
- Developing and implementing technical security programs for the purpose of improving the knowledge and effectiveness of ITS personnel.
- Providing security-related input to strategic and tactical planning, budget preparation, project planning, internal and external reporting, and other management activities.
- Developing and implementing a computer emergency response capability for LMU.

QUALIFICATIONS:

Required:
Bachelor’s Degree from an accredited four-year institution. A Masters’ degree in Computer Science, Information Systems Management, Public Policy or Law is preferred.
Ten (10) years of experience in computing or related area of technology, of which five (5) years must be in management, policy and security. Demonstrated excellent verbal and written communication skills, as well as presentation skills. Writing samples will be required.
Professional certification, either CISSP or appropriate GIAC-series. If certification is not currently held, it must be obtained within the first year of employment in this position.
Extensive experience with both application and network security.

Desired:
Experience in developing and implementing technology policy.
Knowledge of, and experience with, information and personal privacy legislative requirements (e.g. FERPA, GLBA, HIPAA)