

# Indiana University

Vice President for Information Technology and CIO

Job Description

---

JOB TITLE:

**Chief Information Technology Security and Policy Officer (PA19)**

REPORTS TO:

**Vice President for Information Technology (VPIT) and Chief Information Officer**

OFFICE:

**Office of the Vice President for Information Technology (VPIT) and Chief Information Officer (OVPIT/CIO)**

---

JOB SUMMARY:

Under the general direction of the Vice President for Information Technology and Chief Information Officer, and in conjunction with other areas of the University and external agencies where necessary, the Chief IT Security and Policy Officer is responsible for high-level analysis, development, interpretation, and education for Indiana University related to

- Information technology policy.
- Information policy.
- Information and system security policy, practices, and assessment.
- Disaster recovery and business continuity/resumption.

JOB DETAIL:

For activities related to the above responsibilities, and under authority expressly assigned by the Board of Trustees of Indiana University, the Chief IT Security and Policy Officer interacts and coordinates with University executive administration, campus and department technology directors, computing advisory groups, university and external governance and judicial authorities, university and external technology specialists, and individual members of the university and Internet communities. Serves as advisor to the Vice President and other university executive administrators on technology and information policy and security issues. Serves on the OVPIT/CIO cabinet, and on the University Information Technology Services department senior management team. Serves as a member of the University Committee on Institutional Data and the Committee of Data Stewards. In addition, directs and participates in high-level technology security assessment, program planning, and reporting for Indiana University. Maintains budget and staffing levels appropriate for activities. Attends conferences and training, and interacts with external peers as required to maintain knowledge of current issues and best practices.

The Chief IT Security and Policy Officer directs the resources and activities of the Information Technology Policy Office, which

- Analyzes issues related to information technology policy -- assesses current issues, performs legal research, and reports findings.
- Develops technology appropriate use policies in conjunction with university administrators, committees, and governance authorities.
- In conjunction with University data management committees, stewards, and managers, develops and administers appropriate sensitive information handling and storage policies, as well as awareness and educational programs.
- Reviews technology and information policies for continued applicability and effectiveness, and interprets current policy related to specific issues, situations, and incidents.
- Guides policies through appropriate review, approval, and endorsement processes.
- Communicates technology and information policies to the university community through presentations, memos, articles, classes, and media releases.
- Interacts with OVPIT, UITs, and other university managers to ensure consistent application of policies and standards across all technology projects, systems and services.
- Analyzes and tracks reports of inappropriate use of technology and institutional/personal information, including computer security incidents, and guides the investigation and resolution of such incidents.
- Interacts with students, staff, and faculty and their respective governance authorities and judicial processes to resolve complaints and issues related to appropriate use of technology and institutional/personal information.
- Develops and administers security education and awareness programs.
- Prepares media responses and completes media projects related to technology and information use.
- Reviews and reports on proposed information technology- and personal privacy-related state and federal legislation, and provide advice on potential impact to university operations.
- Administers computing accounts for UITs-managed computer systems on both IUB and IUPUI campuses, as well as for other systems under contract.
- Develops and maintains global directory services, including enterprise directories, and identification, authentication, authorization mechanisms, as well as associated maintenance processes, and online address books.
- Develops and maintains a common and consistent set of account and access procedures for users of IU networks and systems on all campuses.
- Interacts with Risk Management, Internal Audit, University Counsel, and other internal "control" agencies, and with civil, law enforcement, and other external judicial authorities to ensure mutual cooperation.
- Coordinates 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 UITs or OVPIT technology services.

In addition, the Chief IT Security and Policy Officer directs the activities of the IT Security Officer and the Information Technology Security Office, which:

- Continually assesses and reports on computer systems and telecommunications security risks within the University technology environment.
- Develops, implements, and administers technical security programs, including consulting, security certifications, education, publications, and online resources.
- Develops and maintains, and/or consults with other technical staff on, security services such as mechanisms for identifying, authenticating, and authorizing users attempting access to IU technology resources and information.
- Provides direction and guidance to UITS and members of the University community to assure compliance with technical security standards and appropriate use policies.
- Provides security-related input to strategic and tactical planning, budget preparation, initiatives and projects planning, internal and external reporting, and other management activities as required.
- Coordinates the Indiana University Computer Emergency Response Team (IU-CERT).
- Provides input into the development of University and departmental computing appropriate use and other related policies and programs.
- Maintains an adequate staff of security analysts and technical investigators.
- Interacts with various law enforcement agencies, risk managers, data managers, auditors, and legal agencies as required.
- Attends conferences and training and other opportunities for collegial exchange as required to maintain proficiency.

#### QUALIFICATIONS:

- A Master's degree in Computer Science, Information Systems Management, Public Policy, or Law is required.
- *Applications from candidates with an undergraduate degree in any of the above mentioned fields of study will be considered if the candidate has extensive experiences related to technology policy and security administration, if the candidate has extensive experiences or abilities in the areas listed as required or desirable below, and if the candidate can reasonably achieve professional certification (CISSP) within 1 year of appointment.*
- Ten (10) years of experience in computing or related technology areas, of which 5 years must be high-level service management, planning, and policy development is required.
- Must demonstrate excellent verbal and written communication skills.
- Extensive experience with data and computer security is very highly desirable.
- Professional certification (e.g., CISSP) is highly desirable.
- Experience in developing and administering technology policy is very highly desirable.

- Experience with information and personal privacy issues (educational records privacy specifically), copyright and software piracy law, development of press releases and other media interactions, IS audit and control issues, and research techniques are all very highly desirable.
- Experience in a higher education environment is highly desirable.
- Experience directly managing technologies, staff, and budget in support of research computing, student computing, administrative computing, and/or telecommunications is very helpful.