Lead Security Analyst

A. PRIMARY ROLE
Under general supervision, support the security assessment of departmental information technology activities for the University Information Security Office (UISO). Provide analysis and facilitation of departmental compliance and activities using common IT infrastructure in support of cybersecurity risk reduction. Serve as analyst for the staff and management of the Vice President for Information Technology (VPIT), University Information Technology Services (UITS), university departments, and regional campuses in examining their technology environments for system and information security vulnerabilities, making judgments as to the risk levels, and identifying appropriate protections. This position has university-wide responsibilities.

B. PRIMARY JOB DUTIES AND RESPONSIBILITIES
40% Participate and lead review team activities by analyzing risks, evaluating IT infrastructure and plans, and assessing compliance with policy.

25% Review and enhance departmental security assessment processes, highlighting risks and trends in IT management across IU; create, update, and maintain assessment documentation as needed; utilize and maintain enterprise governance risk and compliance (EGRC) system to facilitate departmental compliance.

15% Works with governance and compliance officials and decision-makers, providing them with the information risk management guidance they need to comply with University policy.

10% Recommends security policies, procedures, and best practices based on analysis of systems, threats, and current higher education security climate.

10% Acts as a technical resource for other UISO staff. Attends training, seminars, and conferences. Gains and maintains a significant depth of knowledge of risks and safeguards in various technology areas.

C. QUALIFICATIONS
Minimum education:
Baccalaureate degree in Computer Science or related field. Combinations of related education and experience will be considered.

Minimum experience:
Three (3) years of advanced systems analysis/systems administration experience is required. Including one (1) years of experience in developing, implementing or maintaining physical, technical or administrative information security safeguards. Practical experience with one or more relational database packages is desirable. Experience in a university-based technology environment is preferred.

Required knowledge, skills, and abilities:
A demonstrated knowledge of Microsoft Windows operating systems, Active Directory, and the utilities used in system administration, system and kernel customization, security analysis, system logging, and security incident diagnosis. Demonstrated knowledge of the IP protocol suite, specifically relating to TCP
and UDP protocol behavior, and interdependencies with the applications suite (DNS, SMTP, HTTP, etc.).
A demonstrated ability to clearly and effectively document the areas of primary responsibility is required.
Excellent oral/written communication skills and interpersonal skills.

Ability to travel to IU campuses across the state in accordance with IU Travel Management Services policies and procedures, (http://www.indiana.edu/~travel/index.shtml).

PREFFERED: A demonstrated ability to apply security tools in small- and large-scale vulnerability assessments (vulnerability scanners, password cracking tools, etc.). Demonstrated knowledge of UNIX operating systems and the utilities used in system administration, system and kernel customization, security analysis, system logging, and security incident diagnosis is desirable. Demonstrated knowledge of Unix-like operating systems and the utilities used in system administration, system and kernel customization, security analysis tools, system logging, and security incident diagnosis is desirable.

Limited Criminal Histories (LCH) checks will be required for all finalists.

D. LEVEL OF DECISION MAKING
Effort involves interaction and coordination with a wide range of technical, management, governance, compliance, and audit staff, both internal and external to the university, from entry-level programmers to highly skilled technical staff to functional unit managers. Meeting multiple expectations and competing demands, while juggling projects with multiple and sometimes conflicting priorities and deadlines is required on a continual basis.

E. SCOPE AND IMPACT
This position has a university-wide scope, recommends IT policies and safeguards that impact the entire university, and periodically reviews and revises IT policies in conjunction with the University Information Policy Office.

F. DIRECTION PROVIDED TO OTHERS
NONE

G. PHYSICAL REQUIREMENTS
Must be able to stare at a computer screen particularly for long periods of time. Must be able to perform detailed work (programs, documents or instruments); communicate verbally and in writing; interact with staff and clients; handle the stress of performing multiple concurrent tasks with constant interruptions.
Requires creativity in identifying complex problems and finding solutions quickly and accurately; attention to detail in communicating issues and implementing solutions; mental discipline in resolving problems; ability to adapt to changing priorities.