Senior Security Analyst

A. PRIMARY ROLE
Under general supervision, support the security consulting, information gathering, analysis, sharing, incident response, and information product development activities of the University Information Security Office (UISO). Serve as senior liaison and investigator to the staff and management of the Vice President for Information Technology (VPIT), University Information Technology Services (UITS), and university departments and regional campuses in examining their technology environments for system and information security exposures, making judgments as to level of risk, and subsequently with the identification and implementation of appropriate protections. This position has university-wide responsibilities.

B. PRIMARY JOB DUTIES AND RESPONSIBILITIES

30% Design, develop, and implement security processes, software, and systems; evaluate, recommend, and implement vended security software. Analyze, develop, implement, and maintain network and system security analysis and other tools. Assist development of UISO information product, strategies, and concept of operations.

25% Collect, disseminate, and analyze information regarding active security threats, system vulnerabilities and solutions, intrusion methods and protections, current best security and system configuration practices. Participate in on-call rotation.

15% Recommend and implement security policies and procedures based on analysis of systems, threats, and current higher education security climate.

10% Provide advice to and/or participate in the evaluation of proposed software or hardware to determine security or data integrity implications.

10% Respond to incidents of computer security breaches and other incidents involving the use of technology, and provide advice to and/or participate in the collection of technical evidence as required.

10% Act as a technical resource for other UISO staff. Provide training to teammates. Attend training, seminars, and conferences. Develop and maintain knowledge in many various technology areas, including the many aspects of computing, data and voice networking, and security software.

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 / programming / systems administration experience is required. One (1) year of experience in development, administration, and maintenance of security systems and software is required. One (1) year of computer incident response and investigation experience is desirable.

Required knowledge, skills, and abilities:
A 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.) is required. A
demonstrated in-depth 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 is required. A demonstrated ability to clearly and effectively document the areas of primary responsibility is required. Position requires demonstration of excellent oral/written communication skills, presentation skills, and interpersonal skills. Limited Criminal Histories (LCH) checks will be required for all finalists.

PREFERRED: A demonstrated ability to program in C, Perl, Python, or other widely-used, general purpose language is desirable. A demonstrated ability to apply security tools in small- and large-scale vulnerability assessments (vulnerability scanners, password cracking tools, etc.) is desirable. A 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. Practical experience with one or more relational database packages is desirable. Experience in a university-based technology environment is preferred.

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.