



		Issue Date – 8/1/07
Title Systems Security Specialist, Lead	Salary Schedule - PI	Class Code – NE503
Union Non-Represented	Salary Grade - 15	EEO Code – 50
	FLSA – Exempt	E-Class - NE

Basic Purpose:

Provide leadership on implementation for all aspects of information security, including firewall technology, intrusion detection systems, event correlation, in order to provide a both a secure environment and maintain data integrity for the University networks. Provides critical operational tools and framework required to investigate and resolve all unauthorized attempts to access official institutional resources. Leads security project initiatives and conducts regular information security audits to identify “at risk areas” and communicates specific solutions to University customers.

Essential Functions:

- Serve as project leader; prepare project plans and specifications, and set direction for information security policies, processes, and procedures throughout the University. Also serve as expert on security principles, standards, and processes.
- Research current and emerging information security technology trends. Evaluate, test, design, provide comparative analysis for new technologies or to make purchase recommendations to further improve information security at the University. Serve as lead technical contact and liaison during product discovery with faculty, staff, third-party vendors and suppliers
- Conduct security audits and vulnerability assessments for all departments on campus. Conduct penetration testing, security assessments, and traffic analysis and generate related reports. Research, document, and explain security risks to University employees and review results with relevant system administrators for resolution. Identify specific technical recommendations to improve the existing security of the systems. Conduct appropriate follow-up to ensure identified security issues have been resolved.
- Lead information security efforts in resolving all identified security breaches throughout the University network, including leading project teams for both security resolution and proactive measure to prevent future security issues.
- Take lead coordination responsibility for implementing and managing all firewalls throughout the University network, including policy evaluation and implementation, application debugging, and directing staff in secure implementation of services provided behind the firewall.
- Implement and maintain all VPN solutions (i.e. remote campus access) for the University. Involve C&IT and business units in processes to assess and improve the information security infrastructure at the University.
- Manage, maintain, and update all intrusion detection systems to protect the University from malicious activity. Monitor system and network performance for any abnormalities and lead investigations into any cause of abnormalities.

- Provide work direction to professional staff assigned to security function. Lead project teams of assigned student or technicians working on project initiatives.

Minimum Qualifications:

- Experience evaluating new information security technologies and demonstrated ability to provide direction and guidance in information security matters to departments across campus.
- Experience with all major operating systems and how they pertain to various information security issues (e.g. Windows, Mac OS X, Linux, and Solaris).
- Experience evaluating possible security solutions for customers and conducting analysis of the customers' budget, needs and expectations, network data, and technical capability.
- Experience conducting information security audits, distilling the information, and presenting the results and remedial solutions to customers in an understandable format.
- Experience working with firewall technology and implementation, intrusion detection systems, and VPN technology.
- Experience using log analysis and event correlation to detect and identify possible malicious activity on the University network.
- Considerable knowledge of common application software (e.g., Nessus, Nmap, tcpdump, netcat, Wireshark, honeyd, Netscreen-Security Manager, Metasploit, Isof, and Sysinternals tools) and network infrastructure, components, and protocols (e.g. routers, switches, TCP/IP, etc) and familiarity with Juniper, Cisco, Avaya, and Netscreen platforms.