

BRIEF DESCRIPTION:

The purpose of this position is to maintain and enhance the security architecture of College computers and networks. This is accomplished by monitoring and configuring intrusion detection systems; monitoring and configuring peer-to-peer management systems; performing network and vulnerability scanning; coordinating and/or assisting with incident responses; testing and implementing new security hardware and software; coordinating information security tasks; identifying needs and gaps in security systems; assisting the Chief Information and Technology Officer with creating and modifying information security policies, procedures, standards, and guidelines; and performing other duties that may be assigned.

ESSENTIAL FUNCTIONS:

Note: This information is intended to be descriptive of the key responsibilities of the position. The list of essential functions below does not identify all duties performed by any single incumbent in this position. Additional duties may be assigned.

Monitor and configure intrusion detection systems (IDS) and intrusion prevention systems (IPS) to protect the College network from malicious network attacks and to identify compromised faculty, staff, and student machines; develop, deploy, and document security software tools.

Monitor and configure peer-to-peer (P2P) management systems to ensure that available network bandwidth is available to allow research and educational use of the network;

Assist with monitoring and configuring network access control (NAC) systems.

Perform network and vulnerability scanning to ensure that College systems are appropriately protected; perform system administration tasks in support of information security activities; perform system administration tasks in support of information security systems; perform I.T. security audits and back-up and engage in disaster recovery planning and implementation; and develop and deliver training, consulting, or seminars in the computer security community.

Coordinate, lead, and/or assist with information security incident response, recovery, and event handling needs.

Implement and test new security hardware and software; evaluate security of new software, operating systems, protocols, and network architectures.

Assist Network Services team in troubleshooting network connectivity issues to confirm that they are not caused by the IDS, P2P management systems, or NAC systems.

Coordinate information security tasks, and perform information security assessments; maintain awareness of software vulnerabilities and security threats; evaluate, install, test, modify, and debug existing software tools.

Identify needs and gaps, perform remediation, make recommendations and work with College Information Technology and product vendors to remedy those items.

Assist the Chief Information & Technology Officer with creating and modifying information security policies, procedures, standards, and guidelines.

JOB REQUIREMENTS:

Formal Education: Knowledge is acquired through the attainment of a Bachelor's degree preferably in Computer Science or related field.

Experience: Three years; knowledge and experience with key programming languages such as C, C++, Perl, Unix and application development environments; experience with internet network communications such as TCP/IP, HTTP, DNS, SMTP, NTP, BGP required.

SIGNATURE – REVIEW AND COMMENTS:

I have reviewed this description and find it to be an accurate representation of the demands of the position.

Signature of Employee

Date

Job Title of Supervisor

Signature of Supervisor

Date

Job Title of Department Head

Signature of Department Head

Date

Comments: _____

The above statements are intended to describe the general nature and level of work being performed by individuals assigned to this position. They are not intended to be an exhaustive list of all responsibilities, duties, and skills required. This description is subject to modification as the needs and requirements of the position change.