NETWORK/COMPUTER SECURITY SPECIALIST

DISTINGUISHING FEATURES OF THE CLASS: This is a technical position that involves responsibility for assisting in the development and implementation of data access security safeguards and protective measures to ensure protection of computer data from internal and/or external users. An employee in this class is responsible for developing and testing software deployment tools, firewalls and intrusion detection systems. Additional responsibilities may include installing computer security software, conducting regular security audits, preparing security status reports, educating users on computer security, creating security documentation for users, assisting in disaster recovery and gathering evidence regarding cybercrimes. The work is normally performed under the direct supervision of a higher level employee within the Mid Hudson Regional Information Center (MHRIC). Supervision is not normally a function of this class. Does related work as required.

TYPICAL WORK ACTIVITIES: The typical work activities listed below, while providing representative examples of the variety of work assignments in the title, do not describe any individual position. Incumbents in this title may perform some or all of the following, as well as other related activities not described.

Assists in the development and implementation of data access security measures by identifying, analyzing and resolving security and system problems relating to data access security, applications, programs and functions;

Maintains the agency firewall which includes rule modification, updates and event log monitoring;

Manages and monitors the agency's email domains for data loss prevention (DLP) policy enforcement;

Manages the agency's Secure File sharing and collaboration systems;

Manages and monitors the Enterprise Anti-Virus and Anti-Malware systems which include providing updates and monitoring activity;

Works with GSuite administration on mitigating cyberattacks and SPAM;

Analyzes security risks and develops an Incident Response Plan in the event of a data compromise;

Identifies compromised machines and reports on security measures taken to address threats;

Monitors the computer data network system for security threats and unauthorized users;

Works with the Active Directory (AD) administration on AD policies related to security;

Oversees and participates in phishing testing and training for staff;

Provides periodic email and presentations to staff and districts on Cyber security trends;

Runs and/or coordinates periodic vulnerability and penetration tests on the agency network;

Prepares security status reports;

May conduct periodic audits of various system users to determine user removal, transfer or limitation of access.

FULL PERFORMANCE KNOWLEDGES, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS: Thorough knowledge of state-of-the-art computer security; thorough knowledge of network protocols, encryption techniques, firewalls, virtual private networks, database structures, wireless communications and access security techniques; good knowledge of computer performance monitoring techniques; good knowledge of requirements and capabilities of the agency's hardware and related peripheral equipment; ability to analyze, evaluate and identify security problems quickly and efficiently; ability to read, interpret and apply technical information; ability to prepare security status reports; ability to communicate effectively both orally and in writing; ability to establish and maintain good working relationships with customers and vendors; initiative, tact, sound judgement.

MINIMUM QUALIFICATIONS: Either:

A. Graduation from a New York State registered or regionally accredited college or university with a bachelor's or higher level degree, in Computer Science, Information Technology, Management Information Systems, or closely related field and three (3) years of full-time paid, or its' part-time equivalent experience in the computer field (network (LAN/WAN), server or workstation engineering, programming or systems security); **OR**

B. Graduation from a New York State registered or regionally accredited college or university with an associate's or higher level degree, in Computer Science, Information Technology, Management Information Systems, or closely related field and five (5) years of full-time paid, or its' part-time equivalent experience in the computer field (network (LAN/WAN), server or workstation engineering, programming or systems security); **OR**

C. Graduation from high school, or possession of a high school equivalency diploma and seven (7) years of full-time paid, or its' part-time equivalent experience in the computer field (network (LAN/WAN), server or workstation engineering, programming or systems security); **OR**

D. An equivalent combination of training and experience as indicated above.

ULSTER COUNTY Adopted: April 25, 2017
4504 NC SEC SP
Classification: Competitive
OA