

City of New York
Department of information Technology & Telecommunications
Job Posting Notice

Civil Service Title: Computer Systems Manager	Level: M3
Title Code No: 10050	Salary: \$63,519/\$68,500 - \$135,000
Business Title: Director, IT Security Operations and the Security Operation Center (SOC)	Work Location: Brooklyn, NY
Division/Work Unit: IT Security	Number of Positions: 1
Job ID: 196948	Hours/Shift: Day - Due to the necessary technical management duties of this position in a 24/7 operation, candidate may be required to be on call and work various shifts such as weekends and/or nights/evenings.

Job Description

DoITT provides for the sustained, efficient and effective delivery of IT services, infrastructure and telecommunications to enhance service delivery to New York City's residents, businesses, employees and visitors. As the City's technology leader, DoITT is responsible for maintaining the foundational IT infrastructure and systems that touch every aspect of City life from public safety to human services, from education to economic development crossing the full spectrum of governmental operations.

The successful candidate will serve as the Director of IT Security Operations and the Security Operations Center (SOC), reporting to the IT Security Division. Responsibilities will include: Manage and oversee a team that screens critical security changes affecting citywide services and internet applications, oversee and ensure compliance with change control management policies, enhance timely client service delivery; control extranet and business partner access into the City's networks, and respond to security incidents; ensure that resources are correctly and efficiently allocated to key areas of work and that priorities are always covered adequately; publish vulnerability alerts and oversee the documentation of security procedures; manage IT security projects and programs and supervise security change management; ensure established change management procedures are followed and executed by the appropriate technical teams; participate in strategic planning for the deployment of information security technologies and program enhancements; monitor security vulnerabilities, threats and events in the network and host systems; develop strategies to effectively use the current security systems and tools to proactively protect and monitor the security posture of the network; establish metrics and KPIs to effectively communicate the current security state of the environment; develop processes to effectively handle incident response for security events and coordinate investigative activities involving IT security; act as focal point for all IT security investigations, manage full investigation with recommended courses of action, and report any significant security breaches to the CISO; prepare financial forecasts for security operations and proper maintenance coverage for security assets; ensure SOC requirements and incident response are executed with help from cross functional teams and IT organizations within DoITT and City Agencies; ensure the development of strategic and tactical SOC security metrics are applied to daily operations for reporting to stakeholders; ensure that the IT security operations is staffed appropriately; provide leadership and guidance to attract, develop, and retain security personnel; promote awareness of the security program, its capabilities, services, and overall business objectives; prepare senior level technical reports for executive management; and manage special projects and initiatives as assigned. The position's responsibilities include commitment to and compliance with the City's EEO policy.

Minimum Qualification Requirements

1. A master's degree in computer science from an accredited college and three years of progressively more responsible, full-time, satisfactory experience using information technology in computer applications programming, systems programming, computer systems development, data telecommunications, database administration, planning of data/information processing, user services, or area networks at least 18 months of this experience must have been in an administrative, managerial or executive capacity in the areas of computer applications programming, systems programming, computer systems development, data telecommunications, data base administration, or planning of data processing or in the supervision of staff performing these duties; -or-
2. A baccalaureate degree from an accredited college and four years of experience as described in "1" above; -or-
3. A four-year high school diploma or its educational equivalent approved by a State's department of education or recognized accrediting organization and six years of experience as described in "1" above; -or-
4. A satisfactory combination of education and experience equivalent to "1", "2" or "3" above. However, all candidates must have at least a four-year high school diploma or its educational equivalent approved by a State's department of education or recognized accrediting organization and must possess at least three years of experience as described in "1" above, including the 18 months of administrative, managerial, executive or supervisory experience as described in "1" above.

NOTE: The following types of experience are not acceptable: superficial use of preprogrammed software without complex programming, design, implementation or management of the product; use of word processing packages; use of a hand held calculator; primarily the entering or updating of data in a system; the operation of data processing hardware or consoles.

Preferred Skills

The successful candidate should possess the following: 7+ years' experience managing security operations and security operations center; strong negotiation and conflict management skills; strong Client Management skills and strong problem solving skills; demonstrated experience working with technical and non-technical staff; exceptional knowledge of Microsoft programs such as MS Word, Excel, PowerPoint and Access; outstanding collaboration and team building skills; strong written and verbal communication skills; excellent analytic, organization, presentation and facilitation skills; ability to manage multiple tasks under tight deadlines; and the ability to interface with executive level management and give senior level presentations; working knowledge of NGFW technology, enterprise remote access solutions, SIEM, DNS, SMTP, SSL certificate encryption and authentication services, and NetFlow analysis tools. In addition, the following certifications are preferred: CISM, CISSP, GCIIH or CEH.

To Apply

For City employees, please go to Employee Self Service (ESS), click on Recruiting Activities > Careers, and search for Job ID #196948

For all other applicants, please go to www.nyc.gov/jobs/search and search for Job ID #196948

-or-

If you do not have access to a computer, please mail resume indicating Job ID # to:

Department of Information Technology and Telecommunications (DoITT) Recruitment Office - 255 Greenwich Street - 9th Floor - New York, NY 10007

SUBMISSION OF A RESUME IS NOT A GUARANTEE THAT YOU WILL RECEIVE AN INTERVIEW

APPOINTMENTS ARE SUBJECT TO OVERSIGHT APPROVAL

Posting Date: June 23, 2015

Post Until: Filled