University Human Resources
395 Hudson Street
New York, NY 10014
T.646.664.3311
Classified.Centex@cuny.edu

Personnel Order 2024-07

October 24, 2024

Amendment to Classification Plan

The following title is hereby added to the Competitive Class Service of the City University of New York:

Title & Title Code	Level	Minimum	Maximum
IT SECURITY SPECIALIST Title Code 05603	Level 1	$104,304	$121,371
	Level 2	$113,533	$132,453
	Level 3	$124,471	$158,414

The salaries listed above are as of this date. *IT Security Specialist* has been designated as *Hard-to-Recruit* and the starting salaries will be at the minimum (incumbent) rate listed above for each level.

This title is accreted to DC 37, Local 2627.

This Personnel Order must be posted conspicuously for a 30-day period.

Doriane K. Gloria
Senior Vice Chancellor, University Human Resources

THE CITY UNIVERSITY OF NEW YORK
Classified Civil Service Position Description

Title	IT Security Specialist
Title Codes	05603 Annual (full-time)
FLSA Status	Non-Exempt due to collective bargaining agreements.
Date Issued	October 24, 2024

General Duties and Responsibilities

This position encompasses professional and responsible technical consultative and/or administrative work. Under administrative direction of a university IT manager, with broad latitude of independent action or decision, serves as subject matter expert on IT security, identity, and access infrastructure; provides IT security architectural guidance; designs security solutions; conducts IT risk assessments and recommended mitigating solutions.

There are three (3) Assignment Levels within this classification. All personnel perform related work. Assignment Levels 2 and 3 may supervise staff. This specification describes typical assignments; related duties may be assigned as needed.

Assignment Level I

Monitors industry developments through multiple sources; consults with vendors.

Ensures compliance with university security policies and standards.

Oversees security testing plan including routine penetration testing, security controls assessments, and third party cybersecurity engagements.

Recommends updates and improvements to university security policies and standards.

Identifies probable system exposure, compromise, problems, or design flaws and escalates issues to upper management to limit serious performance impact.

Defines, manages, and monitors data security, confidentiality, integrity, and availability.

Sets up, overs, and maintains security devices, as well as creates guidelines for identifying, reporting, and addressing computer security incidents (e.g., Security Device Management and Incident Response).

Monitors developments regarding various IT architectural platforms, including hardware, software and network communication components, operating systems, LDAP, server networking, basic load-balancing, DNS, certificate management, and HTTPS.

Reviews and analyzes design documentation to ensure appropriate security controls are in place.

Collaborates with application development, network, server, database, and storage teams regarding IT security aspects of new technologies, services, and system requirements.

Plans, defines and maintains policies, standards, configurations, and operating procedures and guidelines regarding IT security, identity, and access management in a moderate environment.

Analyzes, designs, implements, tests, troubleshoots, integrates, documents, and configures moderate IT security infrastructure in coordination with others, to maximize performance and capacity.

Plans, initiates and applies new moderate security infrastructure architecture or design changes.

Provides security design assistance on moderately complex new products and internally developed projects.

Assists in the development and review of moderately complex technical specifications for the procurement of various IT security systems and services, including the evaluation of vendor submissions solicited via bids, requests for information and proposals.

Participates as a team member in planning, designing, implementing, and maintaining highly secure application architecture solutions that includes network devices, servers, storage, cloud, and virtualization technologies.

Participates as a team member in planning, designing, implementing, and maintaining identity and access management services that include directory services, identity integrators/connectors, authentication services, web single sign-on and federation services, role and group management and delegated administration services.

Serves as subject matter resource regarding security design of applications, networks, servers, storage and virtualization, directory services, identity connectors, authentication, web single sign-on and federation, and application servers providing delegated administration, role management, and web services.

Performs, manages and documents structured security assessment plans of moderately complex applications and infrastructure.

Assignment Level II – In addition to Assignment Level I tasks, performs the following tasks:

Plans, defines and maintains policies, standards, configuration and operating procedures and guidelines regarding IT security, identity, and access in a complex environment.

Analyzes, designs, implements, tests, troubleshoots, integrates, documents, and configures complex IT security infrastructure in coordination with others, to maximize performance and capacity.

Plans, initiates and applies new complex security infrastructure architecture or design change.

Provides security design assistance on new products and internally developed projects.

Assists in the development and review of complex technical specifications for the procurement of various IT security systems and services, including the evaluation of vendor submissions solicited via bids, requests for information and proposals.

Leads or participates in a team in planning, designing, implementing, and maintaining highly secure application architecture solutions that includes network devices, servers, storage, and virtualization technologies.

Leads or participates in a team in planning, designing, implementing, and maintaining identity and access management services that include directory services, identity integrators/connectors, authentication services, web single sign-on and federation services, role and group management and delegated administration services.

Reviews and analyzes design and/or accreditation documentation to ensure appropriate security controls are in place.

Performs security assessments of complex applications and infrastructure.

Consults with university executives to provide IT Security policy guidance.

Provides training, conducts new hire orientations, and produces ongoing monthly security awareness newsletters.

Serves as subject matter expert regarding security design of complex applications, networks, servers, storage and virtualization, directory services, identity connectors, authentication, web single sign-on and federation, and application servers providing delegated administration, role management, and web services.

Assignment Level III – In addition to Assignment Level I and Assignment Level II tasks, performs the following tasks:

Plans, defines and maintains policies, standards, configuration and operating procedures and guidelines regarding IT security, identity, and access in a complex enterprise scale environment.

Analyzes, designs, implements, tests, troubleshoots, integrates, documents, and configures complex, enterprise scale IT security infrastructure in coordination with others, to maximize performance and capacity.

Plans, initiates and applies new complex, enterprise scale security infrastructure architecture or design changes.

Provides security design assistance on complex, enterprise scale new products and internally developed projects.

Leads or participates in a team in planning, designing, implementing, and maintaining highly secure, enterprise scale application architecture solutions that includes network devices, servers, storage, and virtualization technologies.

Leads or participates in a team in planning, designing, implementing, and maintaining complex, enterprise identity and access management services that include directory services, identity integrators/connectors, authentication services, web single sign-on and federation services, role and group management and delegated administration services.

Serves as subject matter expert regarding security design of enterprise scale applications, networks, servers, storage and virtualization, directory services, identity connectors, authentication, web single sign-on and federation, and application servers providing delegated administration, role management, and web services.

Reviews and analyzes design and/or accreditation documentation to ensure appropriate security controls are in place.

Performs security assessments of complex, enterprise scale applications and infrastructure.

Consults with senior university executives to provide IT Security policy guidance.

Qualification Requirements

1. A baccalaureate degree in computer science, engineering or a related field from an accredited college or university **and** five (5) years of satisfactory full-time experience providing IT security architectural guidance, designing security solutions, and/or conducting IT risk assessments and recommended mitigating solutions; **or**
2. A baccalaureate degree from an accredited college or university **and** six (6) years of satisfactory full-time experience as described in “1” above; **or**
3. A high school diploma or its educational equivalent **and** ten (10) years of satisfactory full-time experience as described in “1” above; **or**
4. Education and/or experience which is equivalent to "1," "2" or "3" above. The following may substitute for some of the required experience required in "1," "2" or "3" above, as follows:
    - College education (undergraduate credits) may substitute for up to four (4) years of the required experience in "3" above on the following basis:
        A. 30 to 59.9 semester credits substitute for 1 year of experience; **or**
        B. 60 to 89.9 semester credits substitute for 2 years of experience; **or**
        C. 90 to 119.9 semester credits substitute for 3 years of experience; **or**
        D. 120 or more semester credits substitute for 4 years of experience.
    - Graduate credits in information technology, computer science or a related field may substitute for up to two (2) years of experience in "1" or "2" above on the following basis:
        A. 15 to 29.9 graduate credits substitute for 1 year of required experience; **or**
        B. 30 or more graduate credits substitute for 2 years of required experience.
    - Each of the following certifications may substitute for one (1) year of the required experience in "1," "2" or "3" above:
        A. Certified Information Systems Security Professional (CISSP) issued by ISC2; **and/or**
        B. Certified Ethical Hacker (CEH) issued by EC-Council; **and/or**
        C. CompTIA Security+ issued by CompTIA; **and/or**
        D. Certified Information Security Manager (CISM) issued by ISACA; **and/or**
        E. Certified Information Security Auditor (CISA) issued by ISACA; **and/or**
        F. GIAC Security Essentials (GSEC) issued by GIAC; **and/or**
        G. Certified Cloud Security Professional (CCSP) issued by ISC2.

However, all candidates must have a high school diploma or its educational equivalent and at least three (3) years of experience as described in "1" above.

Assignment Level II or III:

Level II: After meeting the Qualification Requirements above, an additional two (2) years of satisfactory full-time experience providing IT security architectural guidance, designing security solutions, and/or conducting IT risk assessments and recommended mitigating solutions is required for Level II.

Level III: After meeting the Qualification Requirements above and the Level II requirements, an additional two (2) years of satisfactory full-time experience providing IT security architectural guidance, designing security solutions, and/or conducting IT risk assessments and recommended mitigating solutions is required for Level III (for a total of 4 years of experience above the Qualification Requirements).

English Language Proficiency: Demonstrated English language proficiency, including ability to speak, read, write, and understand English well enough to meet minimally acceptable performance standards set for job duties.

Motor Vehicle Driver License: A Motor Vehicle Driver license, valid in New York State, may be required for some, but not all positions.

Note: CUNY considers full-time work to be at least 35 hours per week. Part-time experience of at least 20 hours per week may be prorated by half and credited instead of, but not in addition to, full-time experience during the same period (e.g., two months of related work experience at 20-34 hours per week equates to one month of full-time related work experience.) Part-time experience of fewer than 20 hours per week **cannot** be credited at all.

Direct Lines of Promotion

From: None To: None