CYBERSECURITY, M.S.

New Jersey City University (NJCU) offers a hybrid Master of Science (M.S.) in Cybersecurity program, combining face-to-face and online learning, to equip students for careers in the rapidly growing field of cybersecurity.

With the dramatic increase in high-profile cybersecurity incidents reported in the media, the demand for highly skilled security professionals is growing significantly as businesses and government agencies across the globe seek to protect their networks and data. The M.S. in Cybersecurity program will provide a range of skills required for an increasingly connected world, where security of information is critical. This degree prepares students with mathematical, technical and business tools to secure an organization's information system. The MS in Cybersecurity is designed to provide a strong foundation and detailed technical knowledge in information security, computer security, network security, and software security as well as an appreciation of the social, policy, ethical and legal aspects of security and privacy.

Duration & Structure: 12-month program, 10 courses, totaling 30 credits

Information Security Pathway

- Core Courses (12 credits): Covers essential cybersecurity concepts.
- Fundamental Electives (6 credits): Builds foundational knowledge.
- Specialized Courses in Information Security (6 credits): Focuses on advanced security strategies.
- Capstone/Fieldwork or Thesis (6 credits): Practical application or research-based study.

The curriculum for the M.S. in Cybersecurity program blends contemporary knowledge with advanced research concepts to deliver a cutting-edge program, and it is mapped with the NSA/DHS guidelines and knowledge units. Students are exposed to state-of-the-art tools and techniques for identifying threats to networking infrastructure, computer systems, as well as data and information systems.

The goal of the M.S. in Cybersecurity program is to provide students with the advanced knowledge in theory and practice to understand current cybersecurity threats, but more importantly to be able to understand, adapt, and develop new techniques to confront emerging threats. The program focuses on a critical understanding of information governance and assurance, combined with technology risk management practices. The elective research component (embodied in the culminating thesis) requires students to expand their resourcefulness by exploring new and creative approaches to address emerging threats.

Code	Title	Credits
Pre-Requisites: 9 Credits (All undergraduate majors are welcomed. Professional knowledge or experience equivalent to the following three courses is required:		
CS 252	Programming for All in Python and Computer Science Principles	3
MATH 140	Statistics I	3
CS 401	Introduction to Algorithms	3

Code	Title	Credits
Major Core Courses: 12 Credits		
SECU 610	Cyber Security	3
SECU 611	Intrusion Detection and Prevention Systems	3
SECU 612	Computer Network & Network Security	3
SECU 6XX - ETHICS AND INFORMATION SECURITY		3

Code	Title	Credits
Fundamental courses(Electives): 6 Credits		
SECU 613	Operating System Security	3
SECU 665	Information Security Strategy and Policy Development	3
SECU 6XX - BIG D/		3
SECU 6XX - MALWARE AND SOFTWARE SECURITY		3

Code	Title	Credits
For Information Security Path: Information Security/ Specialized Courses: 6 credits		
SECU 660	Security, Privacy of Information and Information Systems	3
SECU 665	Information Security Strategy and Policy Development	3

Code	Title	Credits
Capstone and Internship/Fieldwork: 6 credits		
SECU 680	Specialized Field Project	6
SECU 670	Thesis I	6
SECU 675	Thesis II	3

Code	Title	Credits
For Technology Path: Technology Specialized Courses: 9 credits		

Code	Title	Credits
Capstone and Internship/Fieldwork: 3 credits		

The primary program objectives are to confer degrees to students exhibiting the ability to:

1. Demonstrate complex and specialized knowledge and skills in the field of Cybersecurity. (PO1)
2. Appreciate innovations, advances and major issues at the frontiers of Cybersecurity and their implications. (PO2)
3. Deal with complex issues both creatively and systematically, and show originality in tackling and solving problems. (PO3)
4. Perform information security risk assessments, identify potential threats, and develop threat mitigation strategies. (PO4)
5. Use and evaluate a variety of software, tools and techniques relevant to Cybersecurity practices. (PO5)
6. Implement security defense technologies. (PO6)
7. Identify malicious activities and attacks and then evaluate and recommend appropriate response capabilities (PO7)
8. Execute incident response activities and help solve cyber-crime investigations. (PO8)