# CYBERSECURITY, M.S.

New Jersey City University (NJCU) is proposing a Master of Science (M.S.) in Cybersecurity hybrid program (face-to-face and online) in order to prepare students for careers in the rapidly growing field of Cybersecurity. The Master of Science in Cybersecurity will be offered in the Department of Professional Security Studies.

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 across the globe seek to protect their networks and data. 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 aims to equip the students with the mathematical, technical and business tools to secure an organization's information systems. 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.

The program will require 12 months and ten courses of 30 credits in total. The program will have two optional Cybersecurity pathways within the M.S. in Cybersecurity: Information Security and Technology. For the Information Security path: There will be 4 core subjects of 12 credits, 2 fundamental elective courses of 6 credits, 2 specialized courses in Information Security of 6 credits, and 2 optional capstone project/ fieldwork or thesis 1&2 for 6 credits. For the Technology path: There will be 4 core subjects of 12 credits, 2 fundamental elective courses of 6 credits, 3 specialized courses in Technology of 9 credits, and 1 optional Project or Thesis of 3 credits.

Core courses in computer network & network security, cybersecurity, ethics and information security, and intrusion detection and prevention systems provide the theoretical basis for understanding the source of vulnerabilities in computation and information systems. The 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. With this broad theoretical foundation, students can select courses from domain areas that provide both foundation and core of coverage across a wide variety of topics in Cybersecurity. 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 guideline and knowledge units. These courses will enable learning about local area network (LAN) security, cryptography, the advanced encryption standard, smartcards, biometrics, ethical hacking and information systems risk management.

The overall 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 will focus 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. This program is expected best in the state of New Jersey to be designated as a National Center of Academic Excellence by the National Security Agency (NSA) and the Department of Homeland Security (DHS).

| 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 6XX - COMP | | 3 |
| SECU 610 | Cyber Security | 3 |
| SECU 6XX - ETHIC | | 3 |
| SECU 6XX - INTRUSION DETECTION AND PREVENTION SYSTEMS | | 3 |

| Code | Title | Credits |
|---|---|---|
| Fundamental courses(Electives): 6 Credits | | |
| SECU 6XX - OPER/ | | 3 |
| SECU 6XX - BIG DATA ANALYSIS AND SECURITY | | 3 |
| SECU 6XX - MALW | | 3 |
| SECU 665 | Information Security Strategy and Policy Development | 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 |

| Code | Title | Credits |
|---|---|---|
| For Technology Path: Technology Specialized Courses: 9 credits | | |
| CS 508: CRYPTOG | | 3 |
| CS 540: CLOUD COMPUTING WITH ARTIFICIAL INTELLIGENCE | | 3 |
| CS 506 - MACHINE | | 3 |

| Code | Title | Credits |
|---|---|---|
| Capstone and Internship/Fieldwork: 3 credits | | |
| CS 59X - MS CAPS | | 3 |
| CS 599 - MS THESIS IN CYBERSECURITY TECHNOLOGY | | 3 |

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)