CYBERSECURITY, B.S.

The Bachelor of Science in Cybersecurity program provides students with the necessary knowledge, skills, and professional training to pursue careers in the rapidly growing field of Cybersecurity. The program offers a balance between the theoretical and deep technical skills of Cybersecurity. The program is suitable for students who have received an Associate's degree in Business, Homeland Security, Criminal Justice, Computer Science or a related major and have a desire to join the Cybersecurity workforce or conduct Cybersecurity research. The program prepares our graduates to face the futuristic security-related challenges emerging from our internet-connected world, the rapid adoption of mobile devices, and the ever-increasing role of software applications in our daily life. Our curriculum for the Bachelor in Cybersecurity program blends contemporary knowledge with advanced research concepts to deliver a cutting-edge program mapped with the NSA/DHS guidelines and knowledge units.

The requirement for admission to this degree track is a minimum cumulative grade point average (CGPA) of 2.25.

Code	Title	Credits
Prerequisites (15 credits)		
CS 101	Computer Science I	3
CS 206	Concepts of Operating Systems	3
CS 407	Introduction to Unix/Linux System Administration and Shell Programming	3
SECU 210	Introduction to Intelligence	3
SECU 222	Computer Security I	3
Core Courses (27)		
CS 252	TEMP Programming for All in Python and Computer Science Principles	3
CS 410	Telecommunications & Networks	3
SECU 221	Contemporary International Security Topics	3
SECU 224	Ethics in National Security	3
SECU TBD-5	Introduction to Computer & Network Security	3
SECU 345	Computer Forensics I	3
SECU 322	Computer Security II	3
SECU TBD-3	Computer Hacking Forensic Investigator	3
SECU 460	Security & Privacy of Information and Information Systems	3
Security Studies Track Courses (21)		
SECU 422	Computer Security III	3
SECU 3XX	Cyber Incident Handling	3
SECU 3XX	Cybersecurity & Event Management	3
SECU 323	Risk Management	3
SECU 340	Ethical Hacking I	3
SECU TBD-4	Intrusion Detection and Prevention Systems	3
SECU 154	Careers in Professional Security Studies	3
Business Security Track Courses (21)		
FINC XXX	Cybersecurity for Financial Markets and Institutions	3
FINC 305	Introduction to Data Science	3
FINC 430	Principles of Machine Learning	3
MKTG 422	E-commerce	3
ACCT XXX	Intro to Macro Fraud Concepts	3
ECON 220	Understanding Business/Economic Data	3
MKTG 231	Principles of Marketing	3
Computer Science Track Courses (21)		
CS 304	Operating System Design Security	3
CS 350	Software Engineering I	3
CS 306	Data Base Design	3
CS 407	Introduction to Unix/Linux System Administration and Shell Programming	3
CS 252	TEMP Programming for All in Python and Computer Science Principles	3
CS 552	Computer Networks-Architectures, Protocols and Standards	3
CS 307	Microcomputer Maintenance and Repair	3
Electives (12 credits) Take at least four courses		
SECU 151	Security Systems & Design	3
SECU 152	Loss Prevention Technique	3
SECU 153	Occupational Safety and Health	3
SECU 155	Introduction to International Security	3
SECU 214	Crime Scene Investigation	3
SECU 215	Behavioral Analysis & Criminal Profiling	3
SECU 220	Current Security Problems	3
SECU 280	Security Organization & Administration	3
SECU 310	Forensic Investigations	3
SECU TBD-7	Bloodstain Pattern Analysis	3
SECU 315	Big Data in U.S. National Security	3
SECU 321	Seminar on National Security	3
SECU 465	Resource Manangement in Security	3
SECU 398	Research Methods in Professional Security Studies	3
SECU 1305	Special Topics: Intelligence Analysis and National Security	3
SECU 3305	Special Topics: Executive Communications for National Security	3
SECU 2305	Special Topics: National Security Policy	3
SECU 4305	Special Topics: Domestic Terrorism	3
SECU 5305	Special Topics: Extremist Groups	3
SECU 6305	Special Topics: Critical Thinking	3
SECU 7305	Special Topics: Security Fraud	3

Freshman

Semester 1		**Credits**
ENGL 101	English Composition I	4
MATH 165	Pre Calculus	3
General Education Course Tier I		3
General Education Course Tier II		3
General Education Course Tier II		3
	Credits	16
Semester 2		
ENGL 102	English Composition II	4
MATH 140	Statistics I	3
General Education Course Tier I		3

General Education Course Tier II		3
General Education Course Tier II		3
	Credits	16
Sophomore		
Semester 1		
CS 101	Computer Science I	3
General Education Course Tier I		3
General Education Course Tier II		3
General Education Course Tier II		3
CS 408	Introduction to Cryptography	3
	Credits	15
Semester 2		
SECU 222	Computer Security I	3
CS 206	Concepts of Operating Systems	3
SECU 210	Introduction to Intelligence	3
CS 407	Introduction to Unix/Linux System Administration and Shell Programming	3
General Education Course		3
	Credits	15
Junior		
Semester 1		
CS 252	TEMP Programming for All in Python and Computer Science Principles	3
CS 401	Introduction to Algorithms	3
CS 410	Telecommunications & Networks	3
SECU TBD-3	Computer Hacking Forensic Investigator	3
SECU 460	Security and Privacy of Information and Information Systems	3
	Credits	15
Semester 2		
SECU 221	Contemporary International Security Topics	3
SECU 224	Ethics in National Security	3
SECU 322	Computer Security II	3
SECU 345	Computer Forensics I	3
SECU TBD-5	Introduction to Computer & Network Security	3
	Credits	15
Senior		
Semester 1		
Select Specialization Track Course		3
Select Specialization Track Course		3
Select Specialization Track Course		3
Select Specialization Track Course		3
Select Specialization Track Course		3
	Credits	15
Semester 2		
Select Specialization Track Course		3
Select Specialization Track Course		3
Select Specialization Track Course		3
Open Elective		3
Open Elective		3
	Credits	15
	Total Credits	122

STUDENT LEARNING OUTCOMES

In addition to goals and objectives, the proposed B.S. in Cybersecurity program includes two sets of student learning outcomes: (1) institutional (i.e., NJCU) and (2) National Centers of Academic Excellence in Cyber Defense (CAE-CD) (i.e., NSA/DHS). Students earning a Bachelor of Science in Cybersecurity from the New Jersey City University will demonstrate proficiency in their abilities to:

NJCU'S GENERAL EDUCATION REQUIREMENT (GER) LEARNING OUTCOMES

1. Effectively communicate ideas orally and in writing, as informed by the tenets of a liberal
arts education (Liberal Arts Literacy) [GER1]

2. Use logical reasoning and a scientific approach to support conclusions based on empirical evidence (Scientific Literacy) [GER2]
3. Form conclusions that are supported logically by the principles of qualitative and quantitative reasoning, probability, and statistics (Quantitative Literacy) [GER3]
4. Demonstrate the ability to use computing systems in order to access, store, process and analyze the information as an essential aspect of critical thinking and problem solving (Computing Literacy) [GER4]
5. Identify and articulate the multifaceted relationships between the economic, social, and political forces that inform and structure society as well as an individual's place within it (Social Science Literacy) [GER5]

CYBER DEFENSE (CD) KNOWLEDGE UNITS LEARNING OUTCOMES

1. Understand the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems). [CAE-CD 1]
2. Evaluate leadership, theory, tools, skills, and practices as they apply to safeguard the security and privacy of today and tomorrow's cyberinfrastructure. [CAE-CD 2]
3. Design solutions for complex problems in a secure and robust manner using a programming language. [CAE-CD 3]
4. Identify and articulate potential system attacks and the actors that might perform them.
[CAE-CD 4]
5. Identify and articulate appropriate measures to be taken should a system compromise occur. [CAE-CD 5]
6. Identify and articulate cyber defense tools, methods and components. [CAE-CD 6]
7. Understand cyber defense methods to prepare a system to repel attacks. [CAE-CD 7]
8. Demonstrate proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks). [CAE-CD 8]
9. Identify and compare/contrast bad actors in cyberspace, including their resources, capabilities/techniques, motivations, and aversion to risk. [CAE-CD 9]
10. Describe different types of attacks and their characteristics [CAE-CD 10]
11. Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies. [CAE-CD 11]

12. Understand the interaction between security and system usability and the importance of minimizing the effects of security mechanisms [CAE-CD 12]
13. Evaluate the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed. [CAE-CD 13]
14. Identify the elements of a cryptographic system. [CAE-CD 14]
15. Describe how various cryptographic algorithms and protocols work. [CAE-CD 15]
16. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation. [CAE-CD 16]
17. Describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in implementation (e.g., key management), etc. [CAE-CD 17]
18. Apply and analyze hardware components of modern computing environments and their individual functions. [CAE-CD 18]
19. Describe the fundamental concepts, technologies, components and issues related to communications and data networks. [CAE-CD 19]
20. Describe a basic network architecture given a specific need and set of hosts/clients. [CAECD 20]
21. Describe the responsibilities related to the handling of information about vulnerabilities. [CAE-CD 21]
22. Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup.
[CAE-CD 22]
23. Apply security principles to the design and development of database systems and database structures. [CAE-CD 23]
24. Apply the knowledge of network technologies to design and construct a working network. [CAE-CD 24]
25. Analyze a trace of packets to identify the establishment of a TCP connection. [CAE-CD 25]