

**PROPOSAL  
FOR A  
BACHELOR OF SCIENCE IN CYBERSECURITY**

SPONSORED BY:

COMPUTER SYSTEMS TECHNOLOGY DEPARTMENT

SCHOOL OF TECHNOLOGY AND DESIGN  
NEW YORK CITY COLLEGE OF TECHNOLOGY  
THE CITY UNIVERSITY OF NEW YORK

Anticipated Initiation: Fall 2024

Governance Approval Date: \_\_\_\_\_

**PROGRAM IDENTIFICATION**

COLLEGE	New York City College of Technology The City University of New York
PROGRAM TITLE	Cybersecurity
DEGREE	Bachelor of Science
CONTACT PEOPLE	Dr. Pamela Brown Provost and Vice President of Academic Affairs New York City College of Technology PBrown@citytech.cuny.edu  Dr. Reginald Blake Associate Provost New York City College of Technology RBlake@citytech.cuny.edu  Dr. Gerarda M. Shields Dean of the School of Technology and Design New York City College of Technology GShields@citytech.cuny.edu

## **Table of Content**

Curriculum Modification Proposal Form.....	6
Section 1: Program Introduction.....	9
1.1 Introduction .....	9
1.2 Purpose and Goals .....	10
Section 2: Need and Justification.....	12
2.1 Employment Opportunities After Graduation.....	12
2.1.1 Overview of job market.....	12
2.1.2 Job market growth .....	12
2.1.3 Compensation Potential.....	13
2.2 Cybersecurity Salaries by Position.....	14
2.2.1 Entry-Level Roles.....	14
2.2.2 Intermediate-Level Roles .....	15
2.2.3 Advanced Roles .....	16
2.3 Related Undergrad and Graduate Programs in the NY area (as of 10/23).....	17
2.3.1 Related Programs in CUNY .....	17
2.3.2 Related Programs in SUNY.....	18
Section 3: Student Interest and Anticipated Enrollment.....	19
3.1 Student Interest.....	19
3.2 Current Students.....	20
3.3 Enrollment Outlook.....	21
3.4 Potential Students.....	21
Section 4: Curriculum.....	22
4.1 Overview of the Courses in the Curriculum .....	22
4.2 Anticipated Learning Outcomes .....	23
4.3 Courses Required to Complete the Program.....	24
4.3.1 General Education Required Common Core Courses .....	25
4.3.2 Major Core Requirements .....	26
4.3.3 Cybersecurity Major Electives .....	27
4.4 List of Courses and their Prerequisites.....	28
4.5 Transfer Requirements for BS Cybersecurity Students .....	30
4.6 Progression Requirements for BS Cybersecurity Students .....	30

4.7 Example of a Sequence of CST and MATH Courses .....	31
4.8 Example of a Four-year Course Sequence .....	31
4.9 Time for CST Students to Declared Major in Cybersecurity .....	33
4.10 Catalog Description of the Five New Courses .....	33
4.10.1 CST 3616: Cryptographic Technologies .....	33
4.10.2 CST 4716: Cloud Security .....	34
4.10.3 CST 4726: Mobile Device Security and Privacy .....	34
4.10.4 CST 4816: Cybersecurity and Penetration Testing .....	34
4.10.5 CST 4916: Capstone Cybersecurity Course .....	35
4.11 Proposed Prerequisite and Minor Changes to Existing Courses .....	35
4.11.1 Prerequisites Change for CST 2410: Introduction to Computer Security .....	35
4.12 Mapping Anticipated Learning Outcomes to the Courses .....	35
Section 5: Faculty .....	37
Section 6: Cost Assessment .....	39
Section 7: Acknowledgements .....	41
Section 8: References .....	42
Section 9: New Course and Curriculum Change Proposals .....	43
9.1 New Course Proposal #1: CST 3616 – Cryptographic Technologies .....	44
9.2 New Course Proposal #2: CST 4716 – Cloud Security .....	59
9.3 New Course Proposal #3: CST 4726 – Mobile Device Security and Privacy .....	76
9.4 New Course Proposal #4: CST 4816 – Cybersecurity and Penetration Testing .....	95
9.5 New Course Proposal #5: CST 4916 – Capstone Cybersecurity Course .....	113
9.6 Proposal to Change Prerequisites: CST 2410 – Introduction to Computer Security .....	131
Appendix A: Letters of Support .....	134
Appendix B: Sample Job Postings .....	139
Cybersecurity Analyst Levels 1-7 (Threat Hunting and Automation) .....	139
Cybersecurity Engineer Levels 1-7 (Privileged Access Strategist) .....	140
Information Security Analyst (Entry Level - College Grads) .....	141
Cyber Security Analyst (CyberArk) .....	142
Appendix C: Draft Articulation Agreements .....	143
Appendix D: Colleges Offering Degrees in Cybersecurity .....	148
Sample Certificate in Cybersecurity .....	148
Sample AAS in Cybersecurity Programs .....	149



Samples BS in Cybersecurity Programs .....	150
Sample MS in Cybersecurity Programs.....	151
Appendix E: CST Industry Advisory Board Meeting.....	152
Appendix F: Evidence of Consultation with Other Departments .....	153

# Curriculum Modification Proposal Form

New York City College of Technology, CUNY

## Curriculum Modification Proposal Form

<b>Title of Proposal</b>	Bachelor of Science in Cybersecurity
<b>Date</b>	9/11/2023
<b>Major or Minor</b>	Major
<b>Proposer's Name</b>	Prof. Chen, Yu-Wen Prof. Elhadary, Ossama Prof. Kusyk, Janusz Prof. Meherji, Cyrus Prof. Oudjehane, Badreddine Prof. Pinto, Marcos Prof. Li, Xiangdong
<b>Department</b>	Computer Systems Technology
<b>Date of Departmental Meeting in which proposal was approved</b>	03/17/2023 & 09/08/2023
<b>Department Chair Name</b>	Ashwin Satyanarayana
<b>Department Chair Signature and Date</b>	Ashwin Satyanarayana Digitally signed by Ashwin Satyanarayana Date: 2023.09.12 10:37:37 -04'00' 09/12/2023
<b>Academic Dean Name</b>	Gerarda M. Shields
<b>Academic Dean Signature and Date</b>	Gerarda M. Shields Digitally signed by Gerarda M. Shields Date: 2023.09.14 16:55:23 -04'00'
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body.)	The Department of Computer Systems Technology (CST) at the School of Technology and Design, New York City College of Technology (NYCCT/CityTech), proposes a Bachelor of Science (BS) degree in Cybersecurity. Our program is designed to foster in students the knowledge and skills required to defend computer systems, networks, information, and data from cyberattacks. The proposed curriculum includes selected core and general education courses, foundational computer system topics and specialized cybersecurity courses. Our proposal also includes five new CST courses and a list of major electives provided by the departments of Mathematics, Computer Engineering Technology and CST.

<p><b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).</p>	<p>The proposed Cybersecurity program aims to prepare our graduates to become successful professionals in a broad array of cybersecurity-related careers. Recent studies show that there is a high demand for specialists to fill job openings in the cybersecurity field. Some of the roles our graduates will be well-positioned for in the labor market include security analyst, consultant, architect, and system penetration tester. At the same time, the cybersecurity field is becoming increasingly competitive as more schools seek to introduce related programs. Within CUNY, only Queensborough Community College (AAS in Cybersecurity) and Bronx Community College (AAS in Cybersecurity and Networking) currently offer undergraduate associate degrees focused on cybersecurity. Additionally, two CUNY colleges offer master's level degrees in related fields: City College of New York (MS in Cybersecurity) and John Jay College of Criminal Justice (MS in Digital Forensics and Cybersecurity). The BS degree in Cybersecurity, offered by the CST department of NYCCT, will bridge a vital gap in CUNY education programs, providing students a unique opportunity to either become successful professionals or pursue further academic studies at the Master's level.</p>
<p><b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).</p>	<p>9/11/2023: 1<sup>st</sup> submission of this proposal</p>

**ALL PROPOSAL CHECK LIST**

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	X
Documentation of Advisory Commission views (if applicable).	
Completed <a href="#">Chancellor's Report Form</a> .	X

**EXISTING PROGRAM MODIFICATION PROPOSALS**

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	X
Detailed rationale for each modification (this includes minor modifications)	X

## Section 1: Program Introduction

### 1.1 Introduction

Cybersecurity is the craft of protecting computer systems, computer networks, cloud networks, programs, companies/employee data from digital attacks. Cyberattacks target company's data and try to access, change, destroy, hold hostage sensitive information; ransomware tries to extort money from companies and hold data hostage; and interrupt/disrupt normal business processes.

Students enrolled in the Bachelor of Science (BS) in Cybersecurity program will gain a broad understanding of cybersecurity principles and hone their skills using tools that the computer security industry uses. Graduates of the program can benefit from the abundance of employment opportunities available both in public and private sectors within the tristate area and beyond, with many of these positions available immediately upon graduation. In addition, graduates of the program can pursue graduate studies at several graduate schools including the CUNY John Jay College of Criminal Justice and the CUNY City College of New York.

The BS in Cybersecurity is consistent with the mission of New York City College of Technology in that it will provide students with the educational foundation as well as the command of the technical skills necessary to succeed in the domains where Cybersecurity is applied. The degree will offer a balance of technical and liberal arts courses in an effort to foster intellectual curiosity, an appreciation for the aesthetic dimension of life and work and a respect for cultural diversity. The BS in Cybersecurity is also consistent with the mission of the Computer Systems Technology Department (CST) as courses offered will emphasize both the theoretical and practical foundation in the Cybersecurity domain and will emphasize a "hands-on" approach for maximum learning and retention of concepts and practices.

## 1.2 Purpose and Goals

The purpose and goal of the BS in Cybersecurity program is to prepare graduates with the technical skills necessary to enter careers in the Cybersecurity field, which is one of the fastest-growing fields today.

According to STATISTA [1]

- Revenue in the Cybersecurity market is projected to reach US\$162.00bn in 2023.
- Security Services dominates the market with a projected market volume of US\$85.49bn in 2023.
- Revenue is expected to show an annual growth rate (CAGR 2023-2028) of 9.63%, resulting in a market volume of US\$256.50bn by 2028.
- The average Spend per Employee in the Cybersecurity market is projected to reach US\$46.54 in 2023.
- In global comparison, most revenue will be generated in the United States (US\$68,680.00m in 2023).

Demand for cybersecurity specialists has soared in the last decade due to increasing rates of cybercrime. As a result, careers in cybersecurity bring numerous benefits, including job security and a relatively high income. [2]

The U.S. Bureau of Labor Statistics (BLS) reports that the median annual salary for information security analysts is \$102,600. This salary is more than double the national median earnings of workers across all industries (\$45,760). Cybersecurity salary potential tends to be so high due to the delicate nature of the job and the increasing economic demand for cybersecurity professionals.

The BS in Cybersecurity curriculum focuses on the knowledge and skills required to meet industry's security challenges. Students will also complete the CUNY Pathway general education requirements which provide students with a solid liberal arts education. Students will also be required to complete courses in mathematics including probability, discrete structures and calculus. The courses in the major will consist of key cybersecurity topics such as cryptography, computer networking, cloud security, computer forensics, as well as operating systems and analytical tools which will prepare students to meet the data challenges of the field. A combination

of lecture, hands-on labs, group work and an internship will provide students with the opportunity to learn and become skilled at cybersecurity who can then apply those skills on the job. In the first two years of the program students become well versed in the foundational principles of computer networks, operating systems and analytic tools. In the last two years, courses are designed to cover the breadth and depth of the cybersecurity field.

Consistent with City Tech's educational goals, the BS in Cybersecurity is designed to provide a well-rounded interdisciplinary education for the new generation of Cybersecurity practitioners.

## Section 2: Need and Justification

The proposed Cybersecurity program aims to prepare our graduates to become successful professionals in a broad array of cybersecurity-related careers. Recent studies show that there is a high demand for specialists to fill job openings in the cybersecurity field. Some of the roles our graduates will be well-positioned for in the labor market include security analyst, consultant, architect, and system penetration tester. At the same time, the cybersecurity field is becoming increasingly competitive as more schools seek to introduce related programs. Within CUNY, only Queensborough Community College (AAS in Cybersecurity) and Bronx Community College (AAS in Cybersecurity and Networking) currently offer undergraduate associate degrees focused on cybersecurity. Additionally, two CUNY colleges offer master's level degrees in related fields: City College of New York (MS in Cybersecurity) and John Jay College of Criminal Justice (MS in Digital Forensics and Cybersecurity). The BS degree in Cybersecurity, offered by the CST department of NYCCT, will bridge a vital gap in CUNY education programs, providing students a unique opportunity to either become successful professionals or pursue further academic studies at the Master's level.

### 2.1 Employment Opportunities After Graduation

#### 2.1.1 Overview of job market

Cybersecurity experts expect demand to remain high this year, and the U.S. Bureau of Labor Statistics projects that **the number of cybersecurity jobs will grow by 35% between 2021 and 2031**. Worldwide, there are about 3.5 million open cybersecurity jobs, according to Cybersecurity Ventures. [3]

#### 2.1.2 Job market growth

Cybersecurity experts expect demand to remain high this year, and the U.S. Bureau of Labor Statistics projects that the number of cybersecurity jobs will grow by 35% between 2021 and 2031. Worldwide, there are about 3.5 million open cybersecurity jobs, according to Cybersecurity Ventures. In the U.S. alone, that number is about 770,000, data from Cyberseek, a cybersecurity industry research company, shows. [3]



There is a pressing ongoing need for skilled professionals in cybersecurity. It has been reported that, as of 2022, the US experienced a shortage of more than 400,000 skilled cybersecurity personnel, a number that is likely to increase in the years to come [4]. Also, a study by ISACA confirmed that while the cybersecurity workforce remained largely unaffected by the pandemic's direct impacts, it continues to confront significant hiring challenges. Furthermore, only half of the recent graduates hired in cybersecurity may be adequately prepared to carry out their duties [5, 6].

### 2.1.3 Compensation Potential

#### **Salary by Industry:**

An upside of working as a cybersecurity specialist is getting to choose from a variety of industries. As a cybersecurity professional, the specific industry you work for plays a major role in determining your annual income [7] – [9]. As shown in the following, some top-paying industries where experts in cybersecurity are in demand, according to the BLS.

- **Remediation and other waste management services.** Information security analysts in this sector earn an average annual wage of \$173,250.
- **Other information services.** This IT subsector pays an average of \$149,540 to cybersecurity experts.
- **Computer and peripheral equipment manufacturing.** Cybersecurity professionals in this field earn an average of \$144,040.
- **Securities and other financial investment sectors.** These fields pay an average cybersecurity salary of \$142,070.
- **Motion picture and video industries.** This entertainment subsector pays information security analysts an average annual wage of \$141,070.

#### **Salary by State:**

Aside from industry, geographical location is a crucial determinant of cybersecurity salary. Salaries differ by state because employers often use their state's income tax rate and cost of living to determine salary. It makes sense that the highest cybersecurity salaries are paid in metropolitan areas with relatively high living costs. The list below shows the states where professionals can earn high average cybersecurity salaries, according to the BLS.

- **California:** \$135,200
- **New York:** \$133,210
- **Maryland:** \$126,110
- **Iowa:** \$125,650
- **District of Columbia:** \$124,980

## 2.2 Cybersecurity Salaries by Position

Cybersecurity salaries may also vary depending on experience level and role. Generally speaking, however, the earning potential in this industry is so high that even an entry-level cybersecurity specialist could make a six-figure income. As of August 2022, Cyberseek lists the average income levels of cybersecurity professionals in various positions.

### 2.2.1 Entry-Level Roles

Newbies in this industry typically spend three to five years in entry-level cybersecurity jobs to acquire foundational experience. We can see from the listings below that an entry-level position in cybersecurity doesn't equate to low pay.

- **Cybersecurity Specialist**
  - **Average Annual Salary:** \$104,480
  - **Job Openings:** 11,150
  - **Position Summary:** A cybersecurity specialist searches for network and system threats through regular vulnerability scans. They develop security strategies aimed at protecting their company's data integrity.
  - **Qualifications:** BS in Cybersecurity/CS/IT
- **Cybercrime Analyst**
  - **Average Annual Salary:** \$100,000
  - **Job Openings:** 1,388
  - **Position Summary:** This professional investigates malware attacks, the people behind them and the damages caused. A cybercrime analyst also works to recover sensitive data that may be valuable to a court case.
  - **Qualifications:** BS in Cybersecurity/CS/IT

- **Incident and Intrusion Analyst**
  - **Average Annual Salary:** \$88,230
  - **Job Openings:** 11,169
  - **Position Summary:** An incident and intrusion analyst detect security threats to an organization's network. They also prevent the escalation of those threats and report their findings to senior cybersecurity experts.
  - **Qualifications:** BS in Cybersecurity/CS/IT
- **IT Auditor**
  - **Average Annual Salary:** \$110,000
  - **Job Openings:** 9,639
  - **Position Summary:** This entry-level role involves continuous assessment of a company's IT infrastructure to ensure all-around security and adherence to compliance regulations.
  - **Qualifications:** BS in Cybersecurity/CS/IT

### 2.2.2 Intermediate-Level Roles

After acquiring at least five years of experience in entry-level positions, cybersecurity professionals can move up the corporate ladder. Mid-level positions equate to greater responsibilities and a higher cybersecurity salary. Some examples are presented in the following.

- **Cybersecurity Analyst**
  - **Average Annual Salary:** \$107,500
  - **Job Openings:** 39,629
  - **Position Summary:** This position involves the analysis of cyber attacks, malware and the behavior of cybercriminals. Post-analysis, the cybersecurity analyst develops security measures to prevent the recurrence of such attacks.
  - **Qualifications:** BS in Cybersecurity/CS/IT
- **Cybersecurity Consultant**
  - **Average Annual Salary:** \$92,500
  - **Job Openings:** 27,226

- **Position Summary:** A cybersecurity consultant tests an organization's network security, detects vulnerabilities and designs a better security system.
- **Qualifications:** BS in Cybersecurity/CS/IT
- **Penetration and Vulnerability Tester**
  - **Average Annual Salary:** \$101,090
  - **Job Openings:** 34,505
  - **Position Summary:** This position focuses on ethical hacking. A penetration and vulnerability testers simulate actual cyber attacks on existing systems to detect cracks in security systems before malicious actors can breach.
  - **Qualifications:** BS in Cybersecurity/CS/IT

### 2.2.3 Advanced Roles

Advanced roles are reserved for seasoned professionals with 10 to 15 years of full-time experience in cybersecurity. Cybersecurity experts in senior positions typically manage mid-level and junior analysts.

- **Cybersecurity Manager**
  - **Average Annual Salary:** \$130,000
  - **Job Openings:** 27,633
  - **Position Summary:** This management position involves delegating specific duties to junior cybersecurity professionals. The cybersecurity manager also creates strategies to prevent security breaches.
  - **Qualifications:** BS in Cybersecurity/CS/IT **Certifications:** valuable addition
- **Cybersecurity Engineer**
  - **Average Annual Salary:** \$117,510
  - **Job Openings:** 78,288
  - **Position Summary:** This cybersecurity professional develops high-tech solutions that protect a company's digital assets from ransomware, hackers and insider threats.
  - **Qualifications:** BS in Cybersecurity/CS/IT **Certifications:** valuable addition

- **Cybersecurity Architect**

- **Average Annual Salary:** \$159,750
- **Job Openings:** 9,050
- **Position Summary:** A cybersecurity architect designs, builds and implements enterprise-class security systems. They also guide other cybersecurity team members to implement security protocols efficiently.
- **Qualifications :** BS in Cybersecurity/CS/IT **Certifications:** valuable addition

## 2.3 Related Undergrad and Graduate Programs in the NY area (as of 10/23)

Within CUNY, only two programs align with the proposed Bachelor of Science in Cybersecurity degree from the Computer Systems Technology Department: Queensborough Community College's AAS in Cybersecurity and Bronx Community College's AAS in Cybersecurity and Networking. Both programs offer undergraduate associate degrees centered on security. Furthermore, two other CUNY colleges, namely City College of New York and John Jay College of Criminal Justice, offer master's degrees in related fields with their MS in Cybersecurity and MS in Digital Forensics and Cybersecurity programs, respectively. The BS degree in Cybersecurity, presented by the CST department at NYCCT, fills a crucial gap in CUNY's educational offerings, granting students a distinct pathway to professional success or further academic pursuits at the Master's level. While various CUNY departments may feature courses in networking, programming, IT, or other CS-related areas that include security components, to our understanding, these aren't specifically designed to instruct in cybersecurity as a primary focus.

### 2.3.1 Related Programs in CUNY

Six colleges within CUNY offer exposure to undergraduate/graduate students in the area related to Cybersecurity.

- City College of New York
  - MS in Cybersecurity
- John Jay College of Criminal Justice
  - MS in Digital Forensics' and Cybersecurity
  - BS in Computer Science and Information Security

- Queensborough Community College
  - AAS in Cybersecurity
- Bronx Community College
  - AAS in Cybersecurity and Networking
- La Guardia Community College
  - AAS Network Administration & Information Security
- Guttman Community College
  - AAS in Information Technology (Cybersecurity Track).

### 2.3.2 Related Programs in SUNY

As of the time of writing this document, all SUNY programs are online except for the Adirondack AAS degree that is offered as hybrid.

- SUNY Canton
  - BS in Cybersecurity
- SUNY Herkimer County Community College
  - AS in Cybersecurity and Digital Forensics
- SUNY Monroe Community College
  - AS in Homeland Security (two courses in comp. security and cybersecurity)
- SUNY Finger Lakes Community College
  - AAS in Networking and Cybersecurity
- SUNY Polytechnic Institute
  - MS in Network and Computer Security
- SUNY Empire State University
  - Advanced Certificate in Cybersecurity
- SUNY Fredonia
  - Advanced Certificate in Cybersecurity
- SUNY Westchester Community College
  - Undergraduate Certificate in Cybersecurity
- SUNY Adirondack (hybrid with 50% of lectures online)
  - AAS in Information Technology: Cybersecurity

## Section 3: Student Interest and Anticipated Enrollment

### 3.1 Student Interest

Based on the latest reports and the US Government / Department of Homeland Security (DHS) involvement and encouragement [10]-[13] in increasing the cybersecurity workforce, cybersecurity is a relatively young and growing field with a huge need to train many more to fill these positions. City Tech students, being New York City locals, are aware of this situation and are interested in the cybersecurity careers not only in the Information Technology and Engineering industry, but also in other industries including Finance, Medical, etc. In addition, many City Tech students are interested in continuing their education in the field of Cybersecurity. Several universities in the New York City and its vicinities offer Master of Science degrees in Cybersecurity. However, within CUNY, there is no college offers a Bachelor level degree in cybersecurity, and only a few colleges offer Bachelor level degrees in Cybersecurity related areas. The BS in Cybersecurity degree proposed here will increase the opportunity for students in, around and beyond New York City.

A survey of 129 City Tech CST students (both AAS and BTech) was conducted in the Spring of 2023 after offering the students a brief description of a tentative Cybersecurity program at City Tech. The following results were obtained:

1. How familiar are you with the terms of cybersecurity?

Answer Choice	Responses
This is the first time I see these terms.	<b>10 (7.8%)</b>
I have heard these terms but do not have a good grasp of what they mean.	<b>42 (32.6%)</b>
I am familiar with these terms and have a general understanding of what they mean.	<b>53 (41.1%)</b>
I have a good understanding of these terms	<b>24 (18.6%)</b>
Total	<b>129 (100%)</b>

2. Are you interested in modern and advanced cybersecurity courses, such as Cryptographic Techniques, Cloud Security, Mobile Device Security and Privacy, and Advanced Topics in Cybersecurity?

Answer Choice	Responses
Yes	<b>113 (87.6%)</b>
No	<b>16 (12.4%)</b>
Total	<b>129 (100%)</b>

3. Based on the following program objectives of the Bachelor of Science Degree in Cybersecurity at the CST Department at City Tech, are you interested in:

Answer Choice	Responses
In-depth theoretical knowledge and extensive practical skills to protect and defend computer systems against cybersecurity threats.	<b>18 (14.0%)</b>
The capability of delivering cybersecurity defense in known and emerging situations at various technological platforms.	<b>16 (12.4%)</b>
Both	<b>95 (73.6%)</b>
Total	<b>129 (100%)</b>

### 3.2 Current Students

The Computer Systems Department currently offers an AAS in Computer Information Systems, a BTech in Computer Systems Technology and a BS in Data Science, launched in fall 2020. The department serves over 1500 students each semester, in addition to offering a variety of computer courses for students in other programs. Given student interest and workforce needs, we expect enrollment of BS in Cybersecurity to exceed the BS in Data Science.

Academic Plan	2018 Fall	2019 Fall	2020 Fall	2021 Fall	2022 Fall
<b>CIB-BTECH (Computer Systems)</b>	1,828	1,798	1,578	1,417	1,180
<b>CIS-AAS (Computer Information Systems)</b>	551	487	422	446	405
<b>DSCI-B (Data Science)</b>			15	50	73
<b>Grand Total</b>	<b>2,379</b>	<b>2,285</b>	<b>2,015</b>	<b>1,913</b>	<b>1,658</b>



### 3.3 Enrollment Outlook

We can estimate enrollment outlook for the next five years based on the rate of growth of the CST student population for the last five years (2017-2022). This estimate is partly based on data acquired from Enrollment Trends found in the Assessment and Institutional Research (AIR) website (<http://air.citytech.cuny.edu/data-dashboard/enrollment-trends-fall>), and calculations of the average rate of growth over the five-year period 2017-2022. These calculations show a 19% average growth for new incoming CST freshmen students and a 7% average growth for transfer students coming into the CST department. Based on these average growth rates and the survey results indicating an 87% interest in the BS in Cybersecurity, we can estimate the following growth over the next five-year period 2024- 2028:

<b>Year</b>	<b>No. of CST Students</b>	<b>Estimated no. of students in BS in Cybersecurity</b>	<b>No. of Transfer Students</b>	<b>Estimated no. of transfer students in BS in Cybersecurity</b>
2024	409	36	219	21
2025	437	58	234	32
2026	467	76	250	44
2027	499	128	267	48
2028	499	179	267	52

### 3.4 Potential Students

City Tech students in the Bachelor of Technology (BTech) curriculum with an interest in Cybersecurity and who meet the requirements of the new program will be potential candidates for the Bachelor of Science in Cybersecurity. In addition, students with Associate Degrees in Computer Science, Computer Information Science and Mathematics from any of the CUNY community colleges including Borough of Manhattan, La Guardia, Kingsborough, Bronx Community College, Lehman College, York College, Medgar Evers College and the College of Staten Island would also be potential candidates for this program.

## Section 4: Curriculum

### 4.1 Overview of the Courses in the Curriculum

The curriculum has been designed to provide students with a holistic understanding of the subject matter. It begins with foundational courses that delve into the basics, ensuring that every learner, regardless of their prior knowledge, starts on an even footing. As students progress in the academic program, more advanced topics are introduced. The program includes courses interleaving theoretical knowledge and hands-on practical experiences. Our course structure ensures a deep understanding of the cybersecurity concepts and their real-world application. Specialized elective courses are available, allowing students to tailor their learning journey according to individual cybersecurity interests and career aspirations. Every course has been created with the input from industry experts, ensuring that the content remains relevant and in line with current market demands.

#### **Curriculum courses and number of credits:**

1. General Education Required Core (42-44 credits) including necessary core, flexible core, and college option classes designed to let students obtain a quality education in liberal arts.
2. Program General Education Requirements in mathematics (**19 credits**) allowing students to develop strong foundations in the mathematics and statistics that are necessary to success in cybersecurity courses and as a professional.
3. Computer Systems Fundamentals (24 credits) teaching the essential concepts of computer systems (i.e., CST 1100: *Introduction to Computer Systems*, CST 1101: *Problem Solving with Computer Programming*, CST 1201: *Programming Fundamentals*, CST 1215: *Operating Systems Fundamentals*, CST 2307: *Networking Fundamentals*) and system security administration (i.e., CST 2410: *Introduction to Computer Security*, CST 2405: *System Administration in Windows* and CST 2415: *System Administration Linux*).
4. Cybersecurity Core (27 credits) introducing advanced topics of modern cybersecurity, such as bases of cybersecurity (i.e., CST 3523: *Computer Forensic* and CST 3616: *Cryptographic Techniques*), networking security essentials (i.e., CST 3507: *Advanced Single-LAN Concepts* and CST 3610: *Networking Security Fundamentals*), system administration (i.e., CST 3523:

*Task Automation in System Administration*) and advanced cybersecurity topics (i.e., CST 4716: *Cloud Security*, CST 4726: *Mobile Device Security and Privacy*, CST 4710: *Advanced Security Technologies* and CST 4816: *Cybersecurity and Penetration Testing*).

5. Capstone Course (2 credits) including industry-oriented group projects designed to consolidate knowledge and hands-on experience acquired by the students during the program for solving challenges faced by cybersecurity professionals.
6. Cybersecurity Major Electives (6-8 credits) letting students select two courses further advancing their proficiencies in computer systems (e.g., networking, programming, virtualizations, data science), computer engineering (e.g., Internet of things, AI) and mathematics.

## 4.2 Anticipated Learning Outcomes

Anticipated general learning outcomes include:

- a) An ability to use the knowledge, techniques, skills, and modern tools of the discipline to cybersecurity.
- b) The proficiency in apply a knowledge of mathematics, science, engineering, and technology to cybersecurity defense problems that require application of principles and practical knowledge.
- c) An ability to conduct standard tests and measurements, and to conduct, analyze, and interpret experiments.
- d) An ability to function effectively as a member of a technical team.
- e) Demonstrate proficiency in written, oral, and graphical communication skills in both technical and non-technical environments; and an ability to identify and use appropriate technical literature.
- f) Demonstrate an understanding of the need for and an ability to engage in self-directed continuing professional development.
- g) Demonstrate an understanding of and a commitment to address professional and ethical responsibilities, including a respect for diversity.
- h) A commitment to quality, timeliness, and continuous improvement in professional practice.

Anticipated program-specific learning outcomes:

- i) Know and be proficient in
  - operating systems (Windows, Linux, MacOS)
  - scripting and programming (Bash, Python, Java)
  - computer networking (WAN, LAN, WLAN, PAN, Cellular, etc.)
  - cryptographic methods
- j) Understand challenges in protecting critical assets
  - meet security objectives
  - implement countermeasures to prevent cyberattacks
  - implement countermeasures to mitigate effects of cyberattacks
  - exercise cybersecurity awareness
- k) Understand and be able to respond to cyberattacks
  - identify, assess, and manage cyberthreats
  - measure exposures and vulnerabilities of computer systems
  - identify possible responses to cyberattacks
- l) Understand and be able to implement cybersecurity policies, protocols and regulations
  - cybersecurity standards, policies and best practices implemented by governments and industry
  - cybersecurity documentation
  - cybersecurity auditing procedures
- m) Know real-world applications for cybersecurity
  - ensure Authenticity, Integrity and Availability of electronic assets
  - implement Python, BASH, PowerShell scripts for cybersecurity
- n) Provide broad system security
  - data security (data at rest, data in transit)
  - network security (wired, wireless)
  - cloud security

### 4.3 Courses Required to Complete the Program

The proposed curriculum for the Bachelor of Science in Cybersecurity reflects City Tech's General Education and commonly accepted accreditation requirements. All groups of courses

and the number of credits they contribute towards the degree are as follows:

Course Requirement	Number of Credits
General Education Required Common Core	42-44
Program General Education Requirements	19
Computer Systems Fundamentals	24
Cybersecurity Core	27
Capstone Course	2
Cybersecurity Major Electives	6-8
<b>Total:</b>	<b>120-124</b>

#### 4.3.1 General Education Required Common Core Courses

All General Education requirements are grouped into two blocks: The General Education Core and the Program Specific General Education classes. The General Education Core courses are further divided into three subcategories: Required Core, Flexible Core, and College Option. The respective contributions of all these General Education requirements towards the Bachelor of Science in Cybersecurity program are as follows:

General Education Core <sup>1</sup>	Number	Course Title	Credits
<b>Required Core</b>	ENG 1101	English Composition I	3
	ENG 1121	English Composition II	3
	Any	Quantitative Reasoning <sup>2</sup>	3-4
	Any	Life and Physical Science <sup>2,3</sup>	3-4
<b>Flexible Core</b>	Any	World Culture and Global Issues	3
	Any	US Experience and Diversity	3
	Any	Creative Expression	3
	Any	Individual and Society	3
	Any	Scientific World	3

<sup>1</sup> If the student takes double duty course (i.e., course that fulfils Program General Education Core course and Program General Education Requirement), the student must take another elective course to complete 120-credit requirement.

<sup>2</sup> Some of the Quantitative Literacy and Life and Physical Science courses are 4-credit class.

<sup>3</sup> It is recommended that a student takes MAT 1275 or MAT 1275CO, College Algebra and Trigonometry, as the core elective for Mathematical and Quantitative Reasoning if MAT 1275, or its equivalent, has not been fulfilled by the student.

	Any	Additional 6th course	3
<b>College Option</b>	Any	Speech/Oral Communication	3
	Any	Interdisciplinary Course	3
	Any	Additional Liberal Arts course I	3
	Any	Additional Liberal Arts course II	3
<b>Sub-total:</b>			<b>42-44</b>
<b>Program General Education<sup>4</sup></b>	<b>Number</b>	<b>Course Title</b>	<b>Credits</b>
	MAT 1375	Precalculus	4
	MAT 1475	Calculus I	4
	MAT 1575	Calculus II	4
	MAT 2440	Discrete Struct. and Algorithms I	3
	MAT 2572	Probability and Mat. Statistics I	4
<b>Sub-total:</b>			<b>19</b>
<b>General Education Total:</b>			<b>61-63</b>

### 4.3.2 Major Core Requirements

The Bachelor of Science in Cybersecurity requires finishing of Core Courses that are grouped into two categories: Computer Systems Fundamentals and Cybersecurity Core blocks. Successful completion of all major Core Courses follows a required Capstone Cybersecurity Course. The list of these courses and their contributions towards the degree are as follows:

<b>Computer Systems Fundamentals</b>	<b>Course Number</b>	<b>Course Title</b>	<b>Credits</b>
	CST 1100	Introduction to Computer Systems	3
	CST 1101	Problem Solving with Computer Programming	3
	CST 1201	Programming Fundamentals	3
	CST 1215	OS Fundamentals	3
	CST 2307	Networking Fundamentals	3
	CST 2410	Introduction to Computer Security	3

<sup>4</sup> If a student takes double duty course (i.e., course that fulfills Program General Education Requirement and General Education Required Core), the student must take another elective to complete 120-credit requirements. If a student places higher in the math sequence they will also have additional liberal arts & science elective credits available. i.e. MAT 2572.

	CST 2405	System Administration – Windows	3
	CST 2415	System Administration – UNIX/Linux	3
<b>Sub-total:</b>			<b>24</b>
<b>Cybersecurity Core</b>	<b>Number</b>	<b>Course Title</b>	<b>Credits</b>
	CST 3507	Advanced Single-LAN Concepts	3
	CST 3520	Computer Forensic	3
	CST 3523	Task Automation in System Administration	3
	CST 3610	Networking Security Fundamentals	3
	CST 3616 ‡	Cryptographic Technologies	3
	CST 4710	Advanced Security Technologies	3
	CST 4716 ‡	Cloud Security	3
	CST 4726 ‡	Mobile Device Security and Privacy	3
	CST 4816 ‡	Cybersecurity and Penetration Testing	3
<b>Sub-total:</b>			<b>27</b>
<b>Capstone</b>	<b>Number</b>	<b>Course Title</b>	<b>Credits</b>
	CST 4916 ‡	Capstone Cybersecurity Course	2
<b>Sub-total:</b>			<b>2</b>
<b>BS major core requirements - Total:</b>			<b>53</b>

‡ New course proposed together with the CST Bachelor of Science in Cybersecurity.

### 4.3.3 Cybersecurity Major Electives

Students pursuing BS in Cybersecurity will complete two major elective courses selected from classes listed in the table below. These courses are offered by CST and other CityTech departments. Students can select two courses to further examine in details areas that interest them the most or complement their career or academic goals within Cybersecurity field of study.

<b>Cybersecurity Major Electives</b>	<b>Course Number</b>	<b>Course Title</b>	<b>Credits</b>
	CST 3513	OO Programming	3
	CST 3607	Interconnectivity	3
	CST 4715	Adv. Top. in Sys. Admin.	3
	CST 3605	Virtualization	3
	CST 3650	Data Structure	3

	CST 4900	Internship	3
	CET 4925	Internet of Things	3
	CET 4973	Introduction to AI	3
	MAT 2580	Introduction to Linear Algebra	3
	MAT 2675	Calculus III	4
	MAT 2540	Discrete Struct. and Algorithms II	3
	MAT 3672	Probability and Mat. Statistics II	4
<b>Total:</b>			<b>6-8</b>

## 4.4 List of Courses and their Prerequisites

The table below lists prerequisites for all Program General Education Requirements, Computer Systems Fundamentals, Cybersecurity Core and Cybersecurity Major Elective courses in the program.

Course	Cr.	Name	Prerequisite
<b>Department of Mathematics (19 Credits)</b>			
MAT 1375	4	Precalculus	MAT 1275 or MAT 1275CO or Meet the Math Placement for MAT 1375
MAT 1475	4	Calculus I	MAT 1375 or Meet the Math Placement for MAT 1475
MAT 1575	4	Calculus II	MAT 1475
MAT 2440	3	Discrete Structures and Algorithms I	MAT 1375 or higher and one of: CST1201 or CST2403 or MAT1630
MAT 2572 <sup>5</sup>	4	Probability and Mathematical Statistics I	MAT 1575
<b>Computer Systems Fundamentals (24 Credits)</b>			
CST 1100	3	Introduction to Computer Systems	CUNY Proficiency
CST 1101	3	Problem Solving with Computer Programming	CUNY Proficiency
CST 1201	3	Programming Fundamentals	CST 1100 and CST 1101
CST 1215	3	Operating Systems Fundamentals	CST 1100

<sup>5</sup> Specific courses listed indicate double duty courses, i.e., program degree requirements that also meet general education requirements. Choosing to take advantage of double duty can speed up progress toward graduation and increase elective credits for liberal arts and sciences classes. Placement into a higher course in the math sequence may also increase elective credits for liberal arts and sciences. A minimum of 60 liberal arts and sciences credits is required to earn a Bachelor of Science degree. Consult with an advisor about your options



CST 2307	3	Networking Fundamentals	CST 1215
CST 2410	3	Introduction to Computer Security	CST 2307 as co-requisite / prerequisite
CST 2405	3	System Administration Windows	CST 2307
CST 2415	3	System Administration Linux	CST 2307
<b>Cybersecurity Core (27 Credits)</b>			
CST 3507	3	Advanced Single LAN Concepts	CST 2307
CST 3520	3	Computer Forensic	CST 2410
CST 3523	3	Task Automation in System Administration	CST 2405 and CST 2415
CST 3610	3	Networking Security Fundamentals	CST 2410
CST 3616 ‡	3	Cryptography Technologies	CST 2410 and MAT 2440
CST 4710	3	Advanced Security Technologies	CST 3507 and CST 3610
CST 4716 ‡	3	Cloud Security	CST 2410
CST 4726 ‡	3	Mobile Device Security and Privacy	CST 3507 and CST 3610
CST 4816 ‡	3	Cybersecurity and Penetration Testing	CST 3610
<b>Capstone Cybersecurity Project (2 Credits)</b>			
CST 4916 ‡	2	Capstone Cybersecurity Course	Two CST 35xx level courses, One 36xx level course, Dept. permission
<b>Cybersecurity Major Elective (6-8 Credits)</b>			
CST 3513	3	Object-Oriented Programming	CST 1201
CST 3605	3	Virtualization	CST 3507 and (CST 2405 or CST 2415)
CST 3607	3	Interconnectivity	CST 3507
CST 4715	3	Advanced Topics in System Administration	CST 3523 and CST 3607 and CST 3610
CST 3650	3	Data Structure	CST 3503 or CST 3513
CST 4900	3	Internship	Two CST 35xx level courses, One 36xx level course, Dept. permission
CET 4925	3	Internet of Things	CET 4711 and/or CET Department Permission
CET 4973	3	Introduction to Artificial Intelligence	CET 4711 and/or CET Department Permission
MAT 2540	3	Discrete Structure and Algorithms 2	CST 2440
MAT 2580	3	Introduction to Linear Algebra	MAT 1575
MAT 2675	4	Calculus III	MAT 1575
MAT 3672	3	Probability and Mathematical Statistics II	MAT 2675 and MAT 2572
MAT 4872	4	Probability and Mathematical Statistics III	MAT 3672

‡ New course proposed together with the CST Bachelor of Science in Cybersecurity.

## 4.5 Transfer Requirements for BS Cybersecurity Students

Acceptance into this program will be under the requirements in effect at the time of admission and may be subject to such changes as will be determined by City Tech's academic policies and curricula. To earn a baccalaureate degree, admitted students must earn a minimum of 60 credits, of which 34 must be taken in residence. Certification of graduation is assured upon completion of a minimum of 60 credits with a cumulative index of 2.0. This 2.0 index is also required in the major, the minor and/or interdisciplinary program.

## 4.6 Progression Requirements for BS Cybersecurity Students

To successfully complete the BS in Cybersecurity, students must complete courses from all General Education Core categories outlined in Section 4.3.1 (at least 61-63 credits), all required BS Major courses listed in Section 4.3.2 (53 credits), and at least two cybersecurity Major Electives selected from the courses listed in Section 4.3.3 (at least 6-8 credits). If a student takes a double duty course (i.e., a course that fulfills both a Program General Education Requirement and a General Education Required Core), the student must take another elective to meet the 120-credit requirement. Students must obtain at least a grade of 'C' in all CST courses and a passing grade in all other required courses. The program's structure ensures a balanced and in-depth understanding of both the theoretical and practical aspects of cybersecurity, as well as general education courses, ensuring that graduates are not only proficient in cybersecurity but also equipped with the essential skills and knowledge necessary for lifelong learning.

## 4.7 Example of a Sequence of CST and MATH Courses

The table below presents a curriculum map suggesting CST and MAT courses for subsequent semesters of students as they progress through the Cybersecurity program.

BS in Cybersecurity Curriculum Map (MAT and CST courses)						
Sem.	MAT		CST			Major Elective
1			CST 1101	CST 1100		
2	MAT 1375		CST 1201		CST 1215	<div>Prerequisites: Two CST35xx AND one CST36xx AND Dept permission.</div>
3	MAT 1475		CST 2410	2307 is co-requisite / prerequisite for 2410	CST 2307	
4		MAT 2440		CST 2415	CST 2405	
5	MAT 1575		CST 3520	CST 3523	CST 3507	Major Elective I
6	MAT 2572		CST 3616	CST 3610		
7			CST 4716	CST 4710	CST 4726	Major Elective II
8				CST 4816	CST 4916	

## 4.8 Example of a Four-year Course Sequence

Course	Name	Cr.
<b>First Year</b>		
<b>1<sup>st</sup> Semester</b>		
CST 1100	Introduction to Computer Systems	3
CST 1101	Problem Solving	3
ENG 1101	English Composition 1	3
Quantitative Reasoning (Req. Core) <sup>†</sup>	Any	3-4
Life and Physical Science (Req. Core)	Any	3-4
<b>Semester Total:</b>		<b>15-17</b>
<b>2<sup>nd</sup> Semester</b>		
CST 1201	Programming Fundamentals	3
CST 1215	Operating Systems Fundamentals	3
MAT 3575	Precalculus	4
ENG 11201	English Composition 2	3
World Culture and Local Issues (Flex. Core)	Any	3
<b>Semester Total:</b>		<b>16</b>

Second Year		
3 <sup>rd</sup> Semester		
CST 2410	Introduction to Computer Security	3
CST 2307	Networking Fundamentals	3
MAT 1475	Calculus I	4
US Experience in Diversity (Flex. Core)	Any	3
Speech/Oral Communication (College Opt.)	Any	3
Semester Total:		16
4 <sup>th</sup> Semester		
CST 2405	System Administration (Windows)	3
CST 2415	System Administration (UNIX/Windows)	3
MAT 2440	Discrete Structure and Algorithms	3
Creative Expression (Flex. Core)	Any	3
Individual and Society (Flex. Core)	Any	3
Semester Total:		15
Third Year		
5 <sup>th</sup> Semester		
CST 3507	Advanced Single Lan Concepts	3
CST 3520	Computer Forensic	3
CST 3523	Task Automation in System Administration	3
MAT 1575	Calculus II	4
Scientific World (Flex. Core)	Any	3
Semester Total:		16
6 <sup>th</sup> Semester		
CST 3610	Networking Security Fundamentals	3
CST 3616 ‡	Cryptographic Technologies	3
MAT 2572	Probability and Mathematical Statistics	4
Additional 6 <sup>th</sup> Flexible Core (Flex. Core)	Any	3
Semester Total:		13
Fourth Year		
7 <sup>th</sup> Semester		
CST 4710	Advanced Security Technologies	3
CST 4716 ‡	Cloud Security	3
CST 4726 ‡	Mobile Device Security and Privacy	3
Cybersecurity Major Elective I	Any	3-4
Additional Liberal Art (College Opt.)	Any	3
Semester Total:		15-16
8 <sup>th</sup> Semester		
CST 4816 ‡	Cybersecurity and Penetration Testing	3
CST 4916 ‡	Capstone Cybersecurity Course	2

Cybersecurity Major Elective II	Any	3-4
Interdisciplinary (College Opt.)	Any	3
Additional Liberal Art (College Opt.)	Any	3
<b>Semester Total:</b>		<b>14-15</b>

† It is recommended that a student takes MAT 1275, College Algebra and Trigonometry, as the core elective for Mathematical and Quantitative Reasoning if MAT 1275, or its equivalent, has not been fulfilled by the student.

‡ New course proposed together with the CST Bachelor of Science in Cybersecurity.

## 4.9 Time for CST Students to Declared Major in Cybersecurity

Computer System Fundamentals and General Education Core courses significantly overlap with lower-level classes required for students enrolled in CST's AAS, BTech, and Data Science programs. CST students can complete the first three semesters of any CST program without the risk of taking courses that do not count towards their final degrees. Furthermore, the CST Department can guide AAS and BTech students in their academic paths, ensuring that all courses taken in their initial two years count towards the BS in Cybersecurity requirements. This added flexibility allows students to directly enroll in the BS in Cybersecurity or explore other computer technologies before deciding on the degree that best suits their academic and career goals.

## 4.10 Catalog Description of the Five New Courses

We propose five new core cybersecurity courses to offer the comprehensive curriculum for our Bachelor of Science in Cybersecurity program. Combined with the existing CST classes in security, networking, operating systems, and IT, these courses will ensure that our graduates acquire essential and competitive technical skills by the time they graduate. All courses are offered every semester. The Sections 4.10.1 CST 3616: Cryptographic Technologies - .4.10.5 CST 4916: Capstone Cybersecurity Course provide catalog descriptions for the new courses.

### 4.10.1 CST 3616: Cryptographic Technologies

Cryptographic technologies play a pivotal role in safeguarding sensitive information and ensuring the security and integrity of digital communication. Topics include: fundamentals of cryptography, symmetric and asymmetric encryption, hash functions, digital signatures, certificate authority, and public key infrastructure (PKI). Particular iterative hash constructions, such as Message Digest –

algorithm 5 (MD5) and Secure Hash – algorithm 1 (SHA-1) and their properties, are discussed before we move on to strong encryption algorithms including Advanced Encryption Standard (AES), Cipher Block Chaining (CBC) and its less advanced algorithm, Electronic Code Book (ECB), and Rivest–Shamir–Adleman algorithm (RSA) to secure communication channels.

#### 4.10.2 CST 4716: Cloud Security

Provides the knowledge and technical skills required to design, manage, and secure data, infrastructure and applications in the cloud using best current practices. Exposure to multiple cloud technologies via the course lab exercises. To ensure the course fully aligns with the industry, the textbook used in this course is the official body of knowledge for CCSP (Certified Security Cloud Professional) credential

#### 4.10.3 CST 4726: Mobile Device Security and Privacy

How to diagnose and address network security aspects arise in the challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Exercises include research into the required infrastructure, protocols, and design to secure applications and communications in the mobile space; and applying various tools to assess vulnerabilities and use best practices to secure both applications and services.

#### 4.10.4 CST 4816: Cybersecurity and Penetration Testing

Assessing vulnerabilities of systems and networks of systems in order to learn to protect organizations and adapt their security policies to counter and minimize the effects and risks associated with malicious attacks. An in-depth examination of ethical hacking phases, various attack vectors, and preventative countermeasures including network packet analysis and system penetration testing techniques. Class assignments are hands-on and designed around the principle that the best way to learn is by doing. Practice in an isolated virtual environment and get comfortable in the use of current cyber security tools and methodologies.

#### 4.10.5 CST 4916: Capstone Cybersecurity Course

A one-semester capstone course featuring research into a cybersecurity problem, and design and implementation of a solution to it. Topics include identification of a problem, background research, cybersecurity system design, and solution implementation. Work in teams to demonstrate mastery of modern cybersecurity concepts and technologies as well as teamwork, problem-solving, critical thinking, and communication skills. A project proposal, including a problem outline and the solution design, must be completed during the first half of the semester and a hands-on implementation of cybersecurity system completed in the second part of the semester. Each team will be required to write a report and to make an oral presentation to the class.

### 4.11 Proposed Prerequisite and Minor Changes to Existing Courses

Along with the proposed new courses for the BS Cybersecurity program mentioned above, the CST Department will make minor modifications to CST 2410. These updates are driven by recent advancements in computer and network security, as well as the need to eliminate duplicate content across the program's major courses. Notably, all CST students, including those in the AAS and BTech majors, will benefit from these changes to CST 2410.

#### 4.11.1 Prerequisites Change for CST 2410: Introduction to Computer Security

CST 2307: Networking Fundamentals is now a prerequisite/co-requisite for CST 2410: Introduction to Computer Security. Previously, students had to complete CST 2307 before enrolling in CST 2410. This adjustment is possible because CST 2410 relies only on the most basic networking knowledge, which is covered during the final weeks of the course. By designating CST 2307 as a prerequisite/co-requisite for CST 2410, students gain greater flexibility in course selection while optimizing their academic schedule and enhancing their overall academic experience without compromising any learning objectives.

### 4.12 Mapping Anticipated Learning Outcomes to the Courses

The following table maps CST courses to student outcomes a-n (see above: *section 4.2 Anticipated Student Outcomes*):

Course	General Learning Outcomes								Program Specific Outcomes					
	a	b	c	d	e	f	g	h	i	j	k	l	m	n
CST 1100	X				X	X		X	X					
CST 1101	X				X	X		X	X					
CST 1201			X	X	X	X								
CST 1215	X			X	X				X	X				
CST 2307	X		X		X	X				X	X			
CST 2410	X	X	X	X	X	X	X		X	X	X	X		
CST 2405	X		X		X	X			X	X				
CST 2415	X		X		X	X			X	X				
CST 3507	X	X	X	X	X	X			X	X	X	X	X	X
CST 3520	X	X	X	X	X	X	X	X	X	X		X	X	
CST 3523	X		X	X			X	X	X	X			X	
CST 3610	X					X	X	X	X	X	X	X	X	X
CST 3616	X							X	X	X	X	X	X	
CST 4710	X					X	X	X	X	X	X	X	X	X
CST 4716	X	X	X				X	X			X	X	X	X
CST 4726	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CST 4816	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CST 4916	X	X	X	X	X	X	X	X	X	X	X	X	X	X



## Section 5: Faculty

The Computer Systems Technology departments has 20 full time faculty and 84 adjunct professors and most are qualified to teach all or a portion of the coursework related to the proposed Bachelor of Science in Cybersecurity degree program. Our full-time faculty members have conducted well-published research in the related field and have contributed to the development of the new courses required by the curriculum.

There are faculty members from other departments such as Mathematics, Computer Engineering Technology, who also conduct research in cybersecurity in various domain of interest.

Below is the list of core faculty members involved with the program:

1. Chen, Yu-Wen
  - a. Education: Ph.D. in Computer Engineering, Iowa State University.
  - b. Areas of Interest: AI, networking, cybersecurity, smart grid, large-scale data analysis, and Internet of Things.
2. Elhadary, Ossama
  - a. Education: D.B.A. Maastricht School of Management (The Netherlands)
  - b. Areas of Interest: Biomedical Information Technology and Biomedical Analytics.
3. Kusyk, Janusz
  - a. Education: Ph.D. in Computer Science, The Graduate Center, CUNY.
  - b. Areas of Interest: AI, game theory, autonomous vehicles, networking, cybersecurity.
4. Meherji, Cyrus
  - a. Education: BSEE New York Institute of Technology
  - b. Areas of Interest: Computer Networking, Cybersecurity
5. Oudjehane, Badreddine
  - a. Education: MS in Rice University, writing stage of Ph.D. dissertation in Image Processing at Polytechnic University
  - b. Areas of Interest: Image processing, cybersecurity, computer networking.
6. Pinto, Marcos
  - a. Education: Ph.D. in Computer Science, The Graduate Center, CUNY.
  - b. Areas of Interest: Intelligent networks, semantic Web, and Web services.

7. Li, Xiangdong

- a. Education: Ph.D. in Computer Science, The Graduate Center, CUNY.
- b. Areas of Interest: information security, quantum information and physics.

In addition, there are several faculty members in Computer Systems Technology and other Departments that can provide support and bring their expertise to the proposed curriculum, in particular, the Mathematics and Computer Engineering Technology.

## Section 6: Cost Assessment

Current classroom equipment is sufficient in the time being for instruction delivery of most of Computer Systems Fundamental courses in the proposal. For these courses, other than our regular maintenance and replacement of current existing equipment, no additional equipment will be required.

However, for the newly proposed Cybersecurity Core Courses, specifically CST4726 – Mobile Device Security and Privacy, CST4816 – Cybersecurity and Penetration Testing, and CST4916 – Capstone Cybersecurity Course, advanced hardware equipment and supporting software are essential to successfully deliver their course material. We are currently in the process of identifying, procuring, and deploying the necessary equipment to our Cybersecurity and Networking lab, located in the Namm building, room N-1102.

We will need software licenses for cybersecurity applications that need to be used in the cybersecurity courses. We will also need cloud resources to be made available for classes, where students need to build and deploy VMs on cloud environments. In addition, we will need to have per seat subscription licenses for cybersecurity-based websites that provide an environment to conduct penetration testing and sandboxes for cybersecurity practices.

Semester	Estimated no. of students in BS Cybersecurity	Approximate Cost per student (licenses/apps/subscription) yearly	Total Anticipated Cost
Fall 2024	36	\$ 600	\$ 21,600
Fall 2025	58	\$ 600	\$ 34,800
Fall 2026	76	\$ 600	\$ 45,600
Fall 2027	128	\$ 600	\$ 76,800
Fall 2028	179	\$ 600	\$ 107,400

Successful deployment and operation of advanced hardware and software components must be completed by the time the first lectures of these classes commence. It's important to highlight that continuous technical support for the hardware and software components in Room N-1102 will be crucial. Furthermore, it's worth noting that not only students enrolled in our BS

program in Cybersecurity will benefit from this equipment. For example, students enrolling in CST2410, CST2307, CST3610, CST4710 will immediately experience an improved and more up to date lab environment in their studying experiences.

**Faculty and College Lab Technician (CLT)**

The CST department currently has 20 full time faculty members and 84 adjunct faculty members providing academic support of more than two thousand students. We anticipate the total number of students will increase with the new proposed degree program. The department will need to recruit the following additional positions:

2 Tenure-track Assistant Professors (approximate salary \$100,000 / year)

1 College Laboratory Technician (approximate salary \$70,000 / year)

## Section 7: Acknowledgements

The proposers would like to acknowledge the following for their support of the program:

- Professors Benito Mendoza and Yu Wang, CET, CUNY
- Prof. Ping Ji, GC, CUNY
- Prof. Shweta Jain, John Jay College of Criminal Justice, Chair Cybersecurity and Forensics Program, CUNY
- Robert Magliaro, Education Lead, Google
- Prof. Akira Kawaguchi, CCNY, Cybersecurity Program, CUNY
- Prof. Rosario Gennaro, CCNY, Chair Cybersecurity Program, CUNY
- Mr. Joel Caminer, NYU-Tandon School of Engineering, Cybersecurity Program
- Dr. Curtis Dann-Messier, Dean, Guttman Community College
- Prof. Yao, Chair, Math & Computer Science, Queensborough CC, CUNY
- Prof. Abderrazak Belkharraz, Chairperson, MEC, LAGCC, CUNY
- Prof. Praveen Khethavath, Deputy Chair, CS, LAGCC, CUNY
- Prof. Doyel Pal, CS, LAGCC, CUNY
- Mr. Felix Pretto, Enterprise CTO, Atlantic Tomorrows Office (MSP)
- Mr. Robert Ferrara, CISSP, Director of Enterprise Solutions, VC3 (MSP)
- Mr. Tony Cai, Director, Sales Engineering at Nerdio
- Mr. Harry Srolovitz, Information Security, Atlantic Tomorrows Office (MSP)
- Mr. Stu Sjouwerman, CEO and Founder, KnowBe4 Security Training
- Mr. Roger Grimes, Data Driven Defense Evangelist, KnowBe4 Security Training
- Alexis Chaconis, Director of Admission Services

## Section 8: References

- [1] Cybersecurity – Worldwide, <https://www.statista.com/outlook/tmo/cybersecurity/worldwide> (accessed on 09/09/2023)
- [2] N. Uche, What Is A Typical Cybersecurity Salary, <https://www.forbes.com/advisor/education/cybersecurity-salary-outlook/> (accessed on 09/09/2023)
- [3] N. Lake, The 3 cybersecurity hiring trends experts predict for 2023, Forbes, <https://fortune.com/education/articles/the-3-cybersecurity-hiring-trends-experts-predict-for-2023/> (accessed on 09/09/2023)
- [4] Fitzgerald, Jay. (2022, October 24). Cybersecurity Labor Shortage Grows Worse in U.S. And Worldwide: Report. The Channel Co. CRN. <https://www.crn.com/news/security/report-cybersecurity-labor-shortage-grows-worse-in-u-s-and-worldwide> (accessed on 09/15/2023)
- [5] St. Clair, Nelbert, and John Girard. "Are cybersecurity professionals satisfied with recent cybersecurity graduates?" In Journal of The Colloquium for Information Systems Security Education, vol. 7, no. 1, pp. 7-7. 2020, ISACA., <https://cisse.info/journal/index.php/cisse/article/download/103/103> (accessed on 09/15/2023)
- [6] New ISACA Study Finds Cybersecurity Workforce Minimally Impacted by Pandemic, but Still Grappling with Persistent Hiring Challenges. ISACA. <https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/new-isaca-study-finds-cybersecurity-workforce-minimally-impacted-by-pandemic-but-still-grappling> (accessed on 09/15/2023)
- [7] Information Security Analysts, US Bureau of Labor Statistics, <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#:~:text=Employment%20of%20information%20security%20analysts,on%20average%2C%20over%20the%20decade> (accessed on 09/09/2023)
- [8] Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025, Cybersecurity Magazine, <https://cybersecurityventures.com/jobs/> (accessed on 09/09/2023)
- [9] Cybersecurity Supply/Demand Heat Map, <https://www.cyberseek.org/heatmap.html> (accessed on 09/09/2023)
- [10] Cyberbit SC magazine, <https://www.scmagazine.com/perspective/cybercrime/ransomware-gangs-force-cybersecurity-teams-to-reassess> (accessed on 09/09/2023)
- [11] DICE. One of the best-known IT employment sites, <https://www.dice.com/career-advice/for-recent-grads-cybersecurity-offers-lots-of-career-opportunities> (accessed on 09/09/2023)
- [12] BLS, <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6>, and <https://www.bls.gov/careeroutlook/2018/interview/cybersecurity-consultant.htm> (accessed on 09/09/2023)
- [13] Fortune magazine, <https://fortune.com/education/articles/this-cybersecurity-job-is-one-of-the-fastest-growing-in-the-u-s-and-it-pays-six-figures/> (accessed on 09/09/2023)

## Section 9: New Course and Curriculum Change Proposals

We propose five new core cybersecurity courses to be included in the curriculum for our Bachelor of Science in Cybersecurity program. The new courses are tailored to address the dynamic and rapidly evolving cyber threat landscape. These proposed courses have been designed after extensive market research and consultation with industry experts. When merged with our existing CST classes that cover fundamentals in security, networking, operating systems, and IT, these new inclusions will act as a robust foundation ensuring that our graduates not only acquire essential technical skills but also remain at the forefront of cybersecurity technologies, hence making them competitive in the job market. The subsequent sections list proposals for all the new courses. We also dedicated a specific section to detail a minor, yet pivotal, change we're suggesting for one of our existing class.

## 9.1 New Course Proposal #1: CST 3616 – Cryptographic Technologies

### ***NEW COURSE PROPOSAL***

*Fall 2023*

### **“Cryptographic Technologies”**

Respectfully submitted to College Council Curriculum Committee *by*:

Prof. Marcos S. Pinto, Computer Systems Technology Department



New York City College of Technology, CUNY

## CURRICULUM MODIFICATION PROPOSAL FORM

<b>Title of Proposal</b>	New course: Cryptographic Technologies
<b>Date</b>	09/06/2023
<b>Major or Minor</b>	Major
<b>Proposer's Name</b>	Marcos S. Pinto
<b>Department</b>	Computer Systems Technology
<b>Date of Departmental Meeting in which proposal was approved</b>	03/17/2023
<b>Department Chair Name</b>	Ashwin Satyanarayana
<b>Department Chair Signature and Date</b>	<div> <div>Ashwin Satyanarayana</div> <div> Digitally signed by Ashwin Satyanarayana  Date: 2023.09.12 10:38:04 -04'00' </div> </div> <div>09/12/2023</div>
<b>Academic Dean Name</b>	Gerarda M. Shields
<b>Academic Dean Signature and Date</b>	<div> <div>Gerarda M. Shields</div> <div> Digitally signed by Gerarda M. Shields  Date: 2023.09.14 16:56:50 -04'00' </div> </div>
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body.)	This new course will be offered as a core course in the bachelor's program in cybersecurity.
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	The course will train students with the skills and knowledge needed to address current and future challenges in the cybersecurity domain where cryptography is relied upon to secure sensitive data and IT infrastructure.
<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	New proposal

**ALL PROPOSAL CHECK LIST**

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	X
Documentation of Advisory Commission views (if applicable).	X
Completed <a href="#">Chancellor's Report Form</a> .	X

**EXISTING PROGRAM MODIFICATION PROPOSALS**

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	N/A

New York City College of Technology, CUNY

## NEW COURSE PROPOSAL FORM

<b>Course Title</b>	<b>Cryptographic Technologies</b>
<b>Proposal Date</b>	09/11/2023
<b>Proposer's Name</b>	Marcos S. Pinto
<b>Course Number</b>	CST 3616
<b>Course Credits, Hours</b>	3 credits, 2 lecture hours and 2 lab hours
<b>Course Pre / Co-Requisites</b>	Pre-requisites: CST 2410 Introduction to Computer Security and MAT 2440 Discrete Structures and Algorithms I
<b>Catalog Course Description</b>	Cryptographic technologies play a pivotal role in safeguarding sensitive information and ensuring the security and integrity of digital communication. Topics include: fundamentals of cryptography, symmetric and asymmetric encryption, hash functions, digital signatures, certificate authority, and public key infrastructure (PKI). Particular iterative hash constructions, such as Message Digest – algorithm 5 (MD5) and Secure Hash – algorithm 1 (SHA-1) and their properties, are discussed before we move on to strong encryption algorithms including Advanced Encryption Standard (AES), Cipher Block Chaining (CBC) and its less advanced algorithm, Electronic Code Book (ECB), and Rivest–Shamir–Adleman algorithm (RSA) to secure communication channels.
<b>Brief Rationale</b> Provide a concise summary of why this course is important to the department, school or college.	The course will train students with the skills and knowledge needed to address current and future challenges in the cybersecurity domain where cryptography is relied upon to secure sensitive data and IT infrastructure.
<b>CUNY – Course Equivalencies</b> Provide information about equivalent courses within CUNY, if any.	CSCI 352 – Cryptography (Queens College) CSC I4950 – Modern Cryptography (City College – graduate) CISC 3240 – Cryptography and Cryptanalysis (Brooklyn College) MTH 4250 – Introduction to Cryptography (Baruch College) CSCI 39539 – Introduction to Cryptography (Hunter College)
<b>Intent to Submit as Common Core</b> If this course is intended to fulfill one of the requirements in the common core, then indicate which area.	No. This course is necessarily in constant evolution due to its nature which is related to protection of internet-connected systems such as hardware, software and data from cyberthreats.
<b>For Interdisciplinary Courses:</b>	N/A

Date submitted to ID Committee for review	N/A
Date ID recommendation received - Will all sections be offered as ID? Y/N	N/A
<b>Intent to Submit as a Writing Intensive Course</b>	No

## NEW COURSE PROPOSAL CHECK LIST

Use this checklist to ensure that all required documentation has been included. You may wish to use this checklist as a table of contents within the new course proposal.

<b>Completed NEW COURSE PROPOSAL FORM</b>	
• Title, Number, Credits, Hours, Catalog course description	X
• Brief Rationale	X
• CUNY – Course Equivalencies	X
Completed <a href="#">Library Resources and Information Literacy Form</a>	X
<b>Course Outline</b> Include within the outline the following.	X
Hours and Credits for Lecture and Labs If hours exceed mandated Carnegie Hours, then rationale for this	X
Prerequisites/Co- requisites	X
Detailed Course Description	X
Course Specific Learning Outcome and Assessment Tables • Discipline Specific • General Education Specific Learning Outcome and Assessment Tables	X
Example Weekly Course outline	X
Grade Policy and Procedure	X
Recommended Instructional Materials (Textbooks, lab supplies, etc)	X
Library resources and bibliography	X
<b>Course Need Assessment.</b> Describe the need for this course. Include in your statement the following information.	
Target Students who will take this course. Which programs or departments, and how many anticipated? Documentation of student views (if applicable, e.g. non-required elective).	X
Projected headcounts (fall/spring and day/evening) for each new or modified course.	X
If additional physical resources are required (new space, modifications, equipment), description of these requirements. If applicable, Memo or email from the VP for	X

Finance and Administration with written comments regarding additional and/or new facilities, renovations or construction.	
Where does this course overlap with other courses, both within and outside of the department?	X
Does the Department currently have full time faculty qualified to teach this course? If not, then what plans are there to cover this?	X
If needs assessment states that this course is required by an accrediting body, then provide documentation indicating that need.	X
<b>Course Design</b> Describe how this course is designed.	
Course Context (e.g. required, elective, capstone)	X
Course Structure: how the course will be offered (e.g. lecture, seminar, tutorial, fieldtrip)?	X
Anticipated pedagogical strategies and instructional design (e.g. Group Work, Case Study, Team Project, Lecture)	X
How does this course support Programmatic Learning Outcomes?	X
Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.	X
<b>Additional Forms for Specific Course Categories</b>	
<a href="#">Interdisciplinary Form</a> (if applicable)	N/A
Interdisciplinary Committee Recommendation (if applicable and if received)* *Recommendation must be received before consideration by full Curriculum Committee	N/A
<a href="#">Common Core (Liberal Arts) Intent to Submit</a> (if applicable)	N/A
Writing Intensive Form if course is intended to be a WIC (under development)	N/A
If course originated as an experimental course, then results of evaluation plan as developed with director of assessment.	N/A
<b>(Additional materials for Curricular Experiments)</b>	
Plan and process for evaluation developed in consultation with the director of assessment. (Contact Director of Assessment for more information).	N/A
Established Timeline for Curricular Experiment	N/A

### LIBRARY RESOURCES & INFORMATION LITERACY: MAJOR CURRICULUM MODIFICATION

Please complete for all major curriculum modifications. This information will assist the library in planning for new courses/programs. Consult with your library faculty subject specialist (<http://cityte.ch/dir>) 3 weeks before the proposal deadline. Course proposer: please complete boxes 1-4. Library faculty subject specialist: please complete box 5.

1	<p>Title of proposal New course: CST 3616 Cryptographic Technologies</p>	<p>Department/Program Computer Systems Technology</p>
	<p>Proposed by (include email &amp; phone) Marcos S. Pinto <a href="mailto:mpinto@citytech.cuny.edu">mpinto@citytech.cuny.edu</a> (718) 260-5100</p>	<p>Expected date course(s) will be offered Fall 2024 # of students 24</p>

2	<p>The library cannot purchase reserve textbooks for every course at the college, nor copies for all students. Consult our website (<a href="http://cityte.ch/curriculum">http://cityte.ch/curriculum</a>) for articles and ebooks for your courses, or our open educational resources (OER) guide (<a href="http://cityte.ch/oer">http://cityte.ch/oer</a>). Have you considered using a freely-available OER or an open textbook in this course? Yes, there is the alternative of using a freely downloadable earlier book (2015) by Sebastian Raschka from the same publishing company, Packt, of the suggested textbook.</p>
---	--

3	<p>Beyond the required course materials, are City Tech library resources sufficient for course assignments? If additional resources are needed, please provide format details (e.g. ebook, journal, DVD, etc.), full citation (author, title, publisher, edition, date), price, and product link. Yes. The library subscribes to sufficient number of journals and databases in which students will find information and instructions on how to complete the courses' assignments.</p>
---	--

4	<p>Library faculty focus on strengthening students' <b>information literacy</b> skills in finding, critically evaluating, and ethically using information. We collaborate on developing assignments and customized instruction and research guides. When this course is offered, how do you plan to consult with the library faculty subject specialist for your area? Please elaborate. Most definitely so. This course is a very important area of IT, <a href="#">cryptographic technologies</a>, which is constantly changing. As new research papers on this subject are being published we will contact the library for the availability of these papers and in case necessary request for the possibility of having them accessible for our students.</p>
---	--

5	<p>Library Faculty Subject Specialist Prof. Junior Tidal     Anne Leonard for Junior Tidal</p> <p>Comments and Recommendations Once this proposal has been approved, communicating about required readings and texts will be important. The subject selector will use the required readings and bibliography to</p> <p>Date 9/25/2023 inform collection development in support of the new course.</p>
---	---

## **Course Overview & Rationale**

The proposed course is designed to explore the mathematical foundations, cryptographic algorithms, protocols, and practical implementations that underpin secure communication and data protection. Students will gain hands-on experience in designing, implementing, and evaluating cryptographic solutions to address real-world security challenges. This new course is proposed based on the following considerations:

1. Cryptographic technologies are at the forefront of protecting digital assets, sensitive information, and critical infrastructure from cyber threats.
2. Understanding cryptography is essential for individuals and organizations to safeguard personal and sensitive data.
3. Cryptography is a sought-after skill in the job market. Professionals with expertise in cryptographic technologies are in high demand in industries such as finance, healthcare, technology, and government.
4. Finally, CST students gain a practical experience in implementing cryptographic solutions which ensures that they are not only knowledgeable in theory but also capable of applying cryptography in real-world scenarios.

## **Course Outline**

### **New York City College of Technology/CUNY Computer Systems Technology Department**

#### **CST3616 – Cryptographic Technologies**

3 credits

2 class hours, 2 lab hours

#### **1. Course Description:**

This course is designed to explore the mathematical foundations, cryptographic algorithms, protocols, and practical implementations that underpin secure communication and data protection. Students will gain hands-on experience in designing, implementing, and evaluating cryptographic solutions to address real-world security challenges. It emphasizes real-world use of mathematics to encrypt and decrypt data. Students learn cryptography and cryptographic procedures through lectures and hands-on lab experimentations. The topics in this course include fundamentals of cryptography, symmetric and asymmetric encryption, hash functions, digital signatures, certificate authority, and public key infrastructure (PKI). Particular iterative hash constructions, such as Message Digest – algorithm 5 (MD5) and Secure Hash – algorithm 1 (SHA-1) and their properties, are discussed before we move on to strong encryption algorithms including Advanced Encryption Standard (AES), Cipher Block Chaining (CBC) and its less advanced algorithm, Electronic Code Book (ECB), and Rivest–Shamir–Adleman algorithm (RSA) to secure communication channels.

#### **2. Course Objectives:**

Upon successful completion of the course, the student should be able to:

1. Understand what Cryptography is and why we need to study it
2. Learn and describe the basics of cryptography and its most important methods
3. Execute cryptographic applications to illustrate how real-world problems can be solved with cryptography technologies.
4. Implement simple cryptographic applications using Python scripting language.

#### **3. Prerequisite:**

CST 2410 Introduction to Computer Security and MAT 2440 Discrete Structures and Algorithms.

#### **4. Required Text:**

Required: Hands-On Cryptography with Python, Sam Bowne, Packt Publishing Co., 2018, ISBN: 978-1789534443

Reference: Foundations of Cryptography, Oded Goldreich, Cambridge University Press, Vol. 1, 2001, ISBN: 0-521-79172-3

#### **5. Evaluation and Grading\*:**

Midterm	35%
Final	35%
Project**	20%
Participation, Tests, Homework	10%



\* No late submissions of assignments will be accepted if there is no reasonable excuse.

\*\* Project – Individual, online submission. A typical project will include forecasting the outcome of a current problem in the big data field, such as dynamic learning programs (Education), wearable devices and sensor (Healthcare), cybersecurity (Government), etc.

## 6. Grade System\*:

Grade	A	A-	B+	B	B-	C+	C	D	F
Range	93-100	90-92.9	87-89.9	83-86.9	80-82.9	77-79.9	70-76.9	60-69.0	<= 59.9

\* All CST students must attain a grade of C or better in all CST courses

## 7. Academic Integrity:

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using, crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. Please review City Tech's Academic Integrity Policy Manual found at <https://openlab.citytech.cuny.edu/academicintegrity/files/2016/10/Academic-Integrity-Policy-Manual-2017.pdf>, and in the City Tech catalog at <http://www.citytech.cuny.edu/catalog/docs/catalog.pdf> which outlines the college's Academic Integrity Policy.

## 8. Diversity Statement

The Computer Systems Technology Department complies with the college wide nondiscrimination policy and seeks to foster a safe and inclusive learning environment that celebrates diversity in its many forms and enhances our students' ability to be informed, global citizens. Through our example, we demonstrate an appreciation of the rich diversity of world cultures and the unique forms of expression that make us human.

## 9. Disability/Medical Accommodations Statement

City Tech is committed to supporting the educational goals of enrolled students with disabilities in the areas of enrollment, academic advisement, tutoring, assistive technologies and testing accommodations. If you have or think you may have a disability, you may be eligible for reasonable accommodations or academic adjustments as provided under applicable federal, state and city laws. You may also request services for temporary conditions or medical issues under certain circumstances. If you have questions about your eligibility or would like to seek accommodation services or academic adjustments, please contact the Center for Student Accessibility at 300 Jay Street room L-237, (718) 260-5143 or <http://www.citytech.cuny.edu/accessibility/>. Students who miss a scheduled presentation or exam due to illness or medically-related emergencies will be referred to the Center for Students Accessibility. The CSA will review any documentation requested and give the student a letter to share with the relevant instructor if accommodations need to be made.

**10. Course Outline**

Week	TOPIC
1	History and fundamentals of cryptography
2, 3	Obfuscation, Symmetric and asymmetric encryption
4	Caesar cipher and ROT13, base64 encoding
5	XOR, the Caesar cipher, base64, XOR
6	Hashing, MD5 and SHA hashes
7	Windows password hashes, Linux password hashes, Ch 7
7	Midterm
8, 9	Cracking Windows/Linux hashes, Cracking many-round hashes
10, 11	Digital signature, digital certificate and their implementation using Public Key Infrastructure (PKI)
12	Strong (Asymmetric) Encryption: AES (Advanced Encryption Standard)
13	Strong (Asymmetric) Encryption: ECB and CBC models, Padding oracle attack
14, 15	Strong encryption with RSA, Cracking RSA with similar factors, What's next?
15	FINAL

**11. Course Assessment:**

For the successful completion of this course a student should be able to:	Evaluation methods and criteria
Describe the challenges, opportunities and constraints when working with Python, to develop cryptography applications.	Students will develop/modify programs that illustrate principles of cryptography applications
Identify societal challenges that can potentially be tackled by cryptography methods and determine which these methods can be applied	Students' ability to create applications that solve real-world problems.
Model the societal challenges as mathematical problems that cryptography techniques can be applied and propose how to adjust these techniques to fit the problems.	Students will use algorithms and cryptography techniques to turn mathematical models into problem solving applications.
Build efficient security and process modules in order to search, make security adjustments, and user and self-controlled attacking entities.	Students will document/answer questions on issues of security and cryptography applications
Appreciate the challenges of developing cryptography applications	Students will address the following potential issues in their developed cryptography applications: jobs, bias, responsibility, and privacy.

**12. General Education Outcomes and Assessment:**

<b>Learning Outcomes</b>	<b>Assessment Method</b>
<b>SKILLS/Inquiry/Analysis</b> Students will employ scientific reasoning and logical thinking.	Students will describe problem, identify inputs, processes and desired outcomes in assignments, class work and tests. Students will solve problems in assignments, class work and tests. Students will identify coding paradigms in assignments, class work and tests
<b>SKILLS/Communication</b> Students will communicate in diverse settings and groups, using written (both reading and writing), oral (both speaking and listening), and visual means	Students will present their analysis of cryptography applications in written/oral form.
<b>Values, Ethics, Relationships/Professional/Personal Development</b> Students will work with teams, including those of diverse composition. Build consensus. Respect and use creativity.	Students will demonstrate creativity in modifying cryptography apps to meet the user needs.

**13. Bibliography**

1. W. T. Lawrence, C. Washington, Introduction to Cryptography with Coding Theory, 3rd edition, Pearson, 2021.
2. D. Wong, Real-World Cryptography, Manning, 2021.
3. J. Katz, Y. Lindell, Introduction to Modern Cryptography: Third Edition, Chapman and Hall/CRC, 2020.
4. J. P. Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, The Starch Press, 2017.
5. C. Paar, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.
6. N. Ferguson, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

### **Course Need**

**Students who would take this class:** students in the BS Cybersecurity program

**Department:** Computer Systems Technology

**Program:** Bachelors of Science in Cybersecurity

**The number of section (s) anticipated:** one section for the first year

**Projected headcount:** 24 students

**Physical Resources required:** Basic smart room set-up: a screen, and an overhead projector/a TV set that is run by and connected to a computer

**Course overlap:** None

**Faculty qualified for teaching this course:** Yes, there are faculty members who have doctoral degrees in Computer Science with the concentration in computer application development for various domains.

### **Course Design**

**Course context:** This course will be offered as a core course in the BS in Cybersecurity degree. Students are required to develop an independent project at the end of the semester.

**Course structure:** This course will be offered in a lecture style/format.

**Anticipated Pedagogical Strategies and Instructional Design:** This class will be run in a lecture-activity style/format. Any CST department classroom seats 24 students and it provides a computer workstation for each one of them. The class will start with a lecture, and then move on to create in-class activities, such as developing a cryptographic puzzle challenge where students (groups or individuals) are required to decrypt an encrypted message given the encryption method used.

**Providing Support to Programmatic Learning Outcomes:** This course requires satisfactory completion of individual assignments, two major exams and a final term project. These activities will give students tools and knowledge to tackle current and future adventures in Cryptographic Technologies.

CHANCELLOR'S REPORT FORM***NEW COURSE PROPOSAL: "Cryptographic Technologies Course"***

<b>Department(s)</b>	Computer Systems Technology
<b>Academic Level</b>	<input checked="" type="checkbox"/> Regular <input type="checkbox"/> Compensatory <input type="checkbox"/> Developmental <input type="checkbox"/> Remedial
<b>Subject Area</b>	Cybersecurity
<b>Course Prefix</b>	CST
<b>Course Number</b>	3616
<b>Course Title</b>	Cryptographic Technologies
<b>Catalog Description</b>	Cryptographic technologies play a pivotal role in safeguarding sensitive information and ensuring the security and integrity of digital communication. Topics include: fundamentals of cryptography, symmetric and asymmetric encryption, hash functions, digital signatures, certificate authority, and public key infrastructure (PKI). Particular iterative hash constructions, such as Message Digest – algorithm 5 (MD5) and Secure Hash – algorithm 1 (SHA-1) and their properties, are discussed before we move on to strong encryption algorithms including Advanced Encryption Standard (AES), Cipher Block Chaining (CBC) and its less advanced algorithm, Electronic Code Book (ECB), and Rivest–Shamir–Adleman algorithm (RSA) to secure communication channels.
<b>Prerequisite</b>	CST 2410, MAT 2440
<b>Corequisite</b>	None
<b>Pre- or corequisite</b>	None
<b>Credits</b>	3
<b>Contact Hours</b>	4 (2 lecture and 2 lab hours)
<b>Liberal Arts</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>Course Attribute (e.g. Writing Intensive, etc.)</b>	Hands-on coding in programming language
<b>Course Applicability</b>	<input checked="" type="checkbox"/> Major <input type="checkbox"/> Gen Ed Required <input type="checkbox"/> Gen Ed – Flexible <input type="checkbox"/> Gen Ed - College Option <input type="checkbox"/> English Composition <input type="checkbox"/> World Cultures <input type="checkbox"/> Speech <input type="checkbox"/> Mathematics <input type="checkbox"/> US Experience in its Diversity <input type="checkbox"/> Interdisciplinary <input type="checkbox"/> Science <input type="checkbox"/> Creative Expression <input type="checkbox"/> Advanced Liberal Arts <input type="checkbox"/> Individual and Society <input type="checkbox"/> Scientific World
<b>Effective Term</b>	Fall 2024

### **Rationale**

The rationale is one or two sentences explaining where the course fits into the curriculum and why it is being introduced. Must include at least one title and IRP code of a program to which the new course is applicable, as per SED regulation.

This proposed course, CST3616, is a major course for students in the BS in Cybersecurity program. Suggesting a course in cryptographic technologies is well-founded due to its critical role in securing digital information, protecting privacy, and addressing cybersecurity challenges. Moreover, it offers valuable skills and career opportunities in a rapidly evolving digital landscape. CST3616 with its examples supports all the department's four bachelor-level tracks: Database, Networking & Security, IT Operations, and Software Development.

## 9.2 New Course Proposal #2: CST 4716 – Cloud Security

### ***NEW COURSE PROPOSAL***

*Fall 2023*

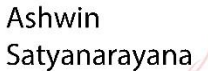

#### **“Cloud Security”**

Respectfully submitted to College Council Curriculum Committee *by*:

Dr. Ossama Elhadary, Computer Systems Technology Department

New York City College of Technology, CUNY

**CURRICULUM MODIFICATION PROPOSAL FORM**

<b>Title of Proposal</b>	New Course: Cloud Security		
<b>Date</b>	09/11/2023		
<b>Major or Minor</b>	Major		
<b>Proposer's Name</b>	Dr. Ossama Elhadary		
<b>Department</b>	Computer Systems Technology		
<b>Date of Departmental Meeting in which proposal was approved</b>	03/17/2023		
<b>Department Chair Name</b>	Ashwin Satyanarayana		
<b>Department Chair Signature and Date</b>	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">             Ashwin Satyanarayana         </div> <div style="font-size: small;">           Digitally signed by Ashwin Satyanarayana            Date: 2023.09.12 10:40:25 -04'00'         </div> <div style="text-align: right;">           9/12/2023         </div> </div>		
<b>Academic Dean Name</b>	Gerarda M. Shields		
<b>Academic Dean Signature and Date</b>	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">             Gerarda M. Shields         </div> <div style="font-size: small;">           Digitally signed by Gerarda M. Shields            Date: 2023.09.14 16:59:02 -04'00'         </div> </div>		
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body).	Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments. This course attempts to fill this gap by providing students with the knowledge and technical skills required to design, manage and secure data, infrastructure and applications in the cloud using best current practices. This course will cover cloud in general without restricting itself to certain cloud technologies like AWS and Azure. Exposure to multiple cloud technologies though will be achieved via the course lab exercises.		
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments.		
<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	This is a new proposal.		



**ALL PROPOSAL CHECK LIST**

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	X
Documentation of Advisory Commission views (if applicable).	X
Completed <a href="#">Chancellor's Report Form</a> .	X

**EXISTING PROGRAM MODIFICATION PROPOSALS**

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	N/A

New York City College of Technology, CUNY

## NEW COURSE PROPOSAL FORM

<b>Course Title</b>	<b>Cloud Security</b>
<b>Proposal Date</b>	Sep. 11, 2023
<b>Proposer's Name</b>	Dr. Ossama Elhadary
<b>Course Number</b>	CST4716
<b>Course Credits, Hours</b>	3 credits, 2 class hours, 2 lab hours
<b>Course Pre / Co-Requisites</b>	CST3610 and CST3507
<b>Catalog Course Description</b>	Provides the knowledge and technical skills required to design, manage, and secure data, infrastructure and applications in the cloud using best current practices. Exposure to multiple cloud technologies via the course lab exercises. To ensure the course fully aligns with the industry, the textbook used in this course is the official body of knowledge for CCSP (Certified Security Cloud Professional) credential.
<b>Brief Rationale</b> Provide a concise summary of why this course is important to the department, school or college.	Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments.
<b>CUNY – Course Equivalencies</b> Provide information about equivalent courses within CUNY, if any.	N/A
<b>Intent to Submit as Common Core</b> If this course is intended to fulfill one of the requirements in the common core, then indicate which area.	N/A
<b>For Interdisciplinary Courses:</b> - Date submitted to ID Committee for review. - Date ID recommendation received - Will all sections be offered as ID? Y/N	N/A
	N/A
	N/A
<b>Intent to Submit as a Writing Intensive Course</b>	N/A

## NEW COURSE PROPOSAL CHECK LIST

<b>Completed NEW COURSE PROPOSAL FORM</b>	
• Title, Number, Credits, Hours, Catalog course description	X
• Brief Rationale	X
• CUNY – Course Equivalencies	X
Completed <a href="#">Library Resources and Information Literacy Form</a>	X
<b>Course Outline</b> Include within the outline the following.	X
Hours and Credits for Lecture and Labs If hours exceed mandated Carnegie Hours, then rationale for this	X
Prerequisites/Co- requisites	X
Detailed Course Description	X
Course Specific Learning Outcome and Assessment Tables • Discipline Specific • General Education Specific Learning Outcome and Assessment Tables	X
Example Weekly Course outline	X
Grade Policy and Procedure	X
Recommended Instructional Materials (Textbooks, lab supplies, etc)	X
Library resources and bibliography	X
<b>Course Need Assessment.</b> Describe the need for this course. Include in your statement the following information.	
Target Students who will take this course. Which programs or departments, and how many anticipated? Documentation of student views (if applicable, e.g. non-required elective).	X
Projected headcounts (fall/spring and day/evening) for each new or modified course.	X
If additional physical resources are required (new space, modifications, equipment), description of these requirements. If applicable, Memo or email from the VP for Finance and Administration with written comments regarding additional and/or new facilities, renovations or construction.	X
Where does this course overlap with other courses, both within and outside of the department?	X
Does the Department currently have full time faculty qualified to teach this course? If not, then what plans are there to cover this?	X
If needs assessment states that this course is required by an accrediting body, then provide documentation indicating that need.	X
<b>Course Design</b>	

Describe how this course is designed.	
Course Context (e.g. required, elective, capstone)	X
Course Structure: how the course will be offered (e.g. lecture, seminar, tutorial, fieldtrip)?	X
Anticipated pedagogical strategies and instructional design (e.g. Group Work, Case Study, Team Project, Lecture)	X
How does this course support Programmatic Learning Outcomes?	X
Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.	X
<b>Additional Forms for Specific Course Categories</b>	
<a href="#">Interdisciplinary Form</a> (if applicable)	N/A
Interdisciplinary Committee Recommendation (if applicable and if received)* *Recommendation must be received before consideration by full Curriculum Committee	N/A
<a href="#">Common Core (Liberal Arts) Intent to Submit</a> (if applicable)	N/A
Writing Intensive Form if course is intended to be a WIC (under development)	N/A
If course originated as an experimental course, then results of evaluation plan as developed with director of assessment.	N/A
<b>(Additional materials for Curricular Experiments)</b>	
Plan and process for evaluation developed in consultation with the director of assessment. (Contact Director of Assessment for more information).	N/A
Established Timeline for Curricular Experiment	N/A

## LIBRARY RESOURCES & INFORMATION LITERACY: MAJOR CURRICULUM MODIFICATION

<b>1 Title of proposal</b> CST4716 – Cloud Security	<b>Department/Program</b> Computer Systems Technology / BS in Cybersecurity
<b>Proposed by</b> (include email & phone) Dr. Ossama Elhadary <a href="mailto:oeelhadary@citytech.cuny.edu">oeelhadary@citytech.cuny.edu</a>	<b>Expected date course(s) will be offered</b> Fall 2024  <b># of students:</b> 24

**2 The library cannot purchase reserve textbooks for every course at the college, nor copies for all students. Consult our website (<http://cityte.ch/curriculum>) for articles and ebooks for your courses, or our open educational resources (OER) guide (<http://cityte.ch/oer>). Have you considered using a freely-available OER or an open textbook in this course?**

Yes, this course will also use some of the freely available OER or resources as partial selective readings.

**3 Beyond the required course materials, are City Tech library resources sufficient for course assignments? If additional resources are needed, please provide format details (e.g. ebook, journal, DVD, etc.), full citation (author, title, publisher, edition, date), price, and product link.**


Yes, City Tech Library resources are sufficient for the proposed course assignments because the main readings for the course are a required textbook and journal articles that will be assigned by instructor. Students should be able to locate the selected journal articles in library.

**4 Library faculty focus on strengthening students' information literacy skills in finding, critically evaluating, and ethically using information. We collaborate on developing assignments and customized instruction and research guides. When this course is offered, how do you plan to consult with the library faculty subject specialist for your area? Please elaborate.**

I will reach out to the library subject specialist via email to arrange an information session in which the library subject specialist can present to the students of this course, the use of library databases, citation convention and discuss copyright issues.

**5 Library Faculty Subject Specialist** \_\_\_\_\_ **Prof. Junior Tidal** **Anne Leonard for Junior Tidal**  **Comments and Recommendations**

comments and recommendations: Anticipating the approval of this degree, I look forward to working with the instructor to create an information literacy lesson that addresses copyright. I will use the course outline, bibliography, and assigned readings to inform collection development of print and electronic resources to support the

**Date** 9/25/2023 course.

---

## **Course Overview & Rationale**

Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments.

This course attempts to fill this gap by providing students with the knowledge and technical skills required to design, manage, and secure data, infrastructure and applications in the cloud using best current practices. This course will cover cloud in general without restricting itself to certain cloud technologies like AWS and Azure. Exposure to multiple cloud technologies though will be achieved via the course lab exercises.

To ensure the course fully aligns with the industry, the textbook used in this course is the official body of knowledge for CCSP (Certified Security Cloud Professional) credential.

## **Course Outline**

### **New York City College of Technology/CUNY Computer Systems Technology Department**

#### **CST4716 – Cloud Security**

3 credits

2 class hours, 2 lab hours

#### **Course Description:**

Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments. This course attempts to fill this gap by providing students with the knowledge and technical skills required to design, manage and secure data, infrastructure and applications in the cloud using best current practices. This course will cover cloud in general without restricting itself to certain cloud technologies like AWS and Azure. Exposure to multiple cloud technologies though will be achieved via the course lab exercises. To ensure the course fully aligns with the industry, the text book used in this course is the official body of knowledge for CCSP (Certified Security Cloud Professional) credential.

#### **Course Objectives:**

Upon successful completion of the course, the student should be able to:

1. Demonstrate knowledge of the core concepts of cloud computing
2. Demonstrate knowledge of the core concepts of cloud security
3. Design and Apply basic Cloud Security technologies and strategies
4. Demonstrate the ability to perform basic cloud security operation tasks

#### **Required Materials:**

The Official (ISC) 2 CCSP CBK Reference, 3rd Edition. June 2021

Leslie Fife, Aaron Kraus, Bryan Lewis, ISBN: 978-1-119-60346-7

The course is divided into 6 domains in line with the CSSP structure.

- Domain 1. Cloud Concepts, Architecture and Design
- Domain 2. Cloud Data Security
- Domain 3. Cloud Platform & Infrastructure Security
- Domain 4. Cloud Application Security
- Domain 5. Cloud Security Operations
- Domain 6. Legal, Risk and Compliance

**Prerequisites:** CST2410

#### **Academic Integrity Standards:**

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using,



crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. The complete text of the College policy on Academic Integrity may be found in the catalog.

The instructor of the course has the authority to give a grade of F if the student submits the work of another person in a manner that represents his/her work, or knowingly permits one's work to be submitted by another person without the instructor's permission (see College Catalog).

### Progression Requirements

Students majoring in CIB must earn a grade of "C" or better in this course in order to progress to the next level courses. If grade earned is less than "C", the course must be repeated.

### Homework Assignments

All assignment are to be submitted by the due date on SafeAssign. Late assignments, as well as assignments not submitted through SafeAssign will not be accepted.

### Grading Procedure:

Exams	40%
Assignments	40%
Labs	20%
	===
TOTAL	100%

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numerical Grade	93-100	90-92.9	87-89.9	83-86.9	80-82.9	77-79.9	70-76.9	60-69.9	<=59.9

### Course Outline:

Week	Topics	Reading
1	<b>Understand Cloud Computing Concepts:</b> Cloud Computing Definitions and roles Key Cloud Computing Characteristics Building Block Technologies <b>Cloud Reference Architecture</b> Cloud Computing Activities, and Capabilities Cloud Service Categories and Deployment Models Cloud Shared Considerations	Pages 1-22
2	<b>Security Concepts Relevant to Cloud Computing</b> Cryptography and Key Management Access Control Data and Media Sanitization	Pages 23-40

	Network Security Virtualization Security Common Threats <b>Understand Design Principles of Secure Cloud Computing</b> Cloud Secure Data Lifecycle Cloud-Based Disaster Recovery and Business Continuity Planning Functional Security Requirements and Security Considerations for Different Cloud Categories <b>Lab 1</b>	
3	<b>Cloud Data Security</b> Cloud Data Concepts and Lifecycle Phases Data Dispersion <b>Design and Implement Cloud Data Storage Architectures</b> Storage Types Threats to Storage Types <b>Design and Apply Data Security Technologies and Strategies</b> Encryption and Key Management Hashing, Masking, and Tokenization Data Loss Prevention, Obfuscation, and De-identification <b>Implement Data Discovery</b> <b>Exam 1</b>	Pages 40-69
4	Design and Implement Information Rights Management Plan. Implement Data Retention, Deletion, and Archiving Policies Design and Implement Auditability, Traceability, and Accountability of Data Events	Pages 70-85
5	<b>Cloud Platform and Infrastructure Security</b> Design a Secure Data Center Analyze Risks Associated with Cloud Infrastructure Design and Plan Security Controls Identification, Authentication, and Authorization in Cloud Infrastructure Plan Disaster Recovery and Business Continuity <b>Lab 2</b>	Pages 85-116
6	<b>Cloud Application Security</b> Cloud Development Basics and Common Cloud Vulnerabilities Secure Software Development Lifecycle Process NIST Secure Software Development Framework OWASP Software Assurance Security Model Cloud-Specific Risks, Quality Assurance, and Threat Modeling Software Configuration Management and Versioning Secure Testing Methodologies <b>Exam 2</b>	Pages 117-132
7	<b>Cloud Application Security - Continued</b> Cryptography, Sandboxing, and Application Virtualization and Orchestration <b>Identity and Access Management Solutions</b>	Pages 133-144

	Federated Identity Identity Providers Single Sign-On Multifactor Authentication Cloud Access Security Broker <b>Lab 3</b>	
8	<b>Cloud Security Operations</b> Hardware-Specific Security Configuration Requirements Installation and Configuration of Virtualization Management Tools Virtual Hardware–Specific Security Configuration Requirements Installation of Guest Operating System Virtualization Toolsets Configure Access Control for Local and Remote Access Secure Network Configuration Operating System Hardening through the Application of Baselines	Pages 145-165
9	<b>Cloud Security Operations</b> Operating System Baseline Compliance Monitoring and Remediation Patch Management Performance and Capacity Monitoring Hardware Monitoring Configuration of Host and Guest Operating System Backup and Restore Functions Network Security Controls and Management Plane <b>Exam 4</b>	165-181
10	<b>Implement Operational Controls and Standards</b> Change Management, and Continuity Management Information Security Management Continual Service Improvement Management Incident, Problem, Release, Deployment, Configuration, Service Level, Availability, and Capacity Management <b>Lab 4</b>	182-197
11	<b>Forensics</b> Forensic Data Collection Methodologies, and Evidence Management Collect, Acquire, and Preserve Digital Evidence Manage Communication with Relevant Parties Shared Responsibility Model Stakeholders <b>Manage Security Operations</b> Security Operations Center Monitoring of Security Controls Log Capture and Analysis Incident Management	198-220
12	<b>Evaluation of Legal Risks Specific to Cloud Computing</b> <b>Understanding Audit Process, Methodologies, and Required Adaptations for a Cloud Environment</b> <b>Lab 5</b>	221-250

13	<b>Understand Implications of Cloud to Enterprise Risk Management</b> Assess Providers Risk Management Programs 266 Differences Between Data Owner/Controller vs. Data Custodian/Processor Risk Treatment and Risk Frameworks Metrics for Risk Management Assessment of Risk Environment	251-285
14	<b>Final Review</b>	
15	<b>Exam 5</b>	

#### Assessment Criteria:

<b>For the successful completion of this course a student should be able to:</b>	<b>Evaluation methods and criteria</b>
Demonstrate knowledge of the core concepts of cloud computing	Exams, and assignments
Demonstrate knowledge of the core concepts of cloud security	Exams, and assignments
Design and Apply basic Cloud Security Technologies and Strategies	Exams, and assignments
Demonstrate the ability to perform basic cloud security operation tasks	Labs

## **Course Need**

**Students who would take this class:** students who intend to major in Cybersecurity

**Department:** Computer Systems Technology

**Program:** Bachelors in Cybersecurity

**The number of section (s) anticipated:** one section for the first year

**Projected headcount:** 24 students

**Physical Resources required:** Basic smart room set-up: a screen, and an overhead projector/a TV set that is run by and connected to a computer

**Course overlap:** None

**Faculty qualified for teaching this course:** Yes, there are faculty members who have doctoral degrees in Computer Science with the concentration in Cybersecurity for various domains.

## **Course Design**

**Course context:** This course will be required of Cybersecurity major students.

**Course structure:** This course will be offered in a lecture style/format.

**Anticipated Pedagogical Strategies and Instructional Design:** This class will be run in a lecture-activity style/format. The class will start with a lecture, and involve the in-class activities, such as group discussion, hands-on exercises, and hands-on labs.

**Providing Support to Programmatic Learning Outcomes:** This course requires satisfactory completion of individual assignments, quizzes, and exams.

**Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.** Not online; all in-person.

## CHANCELLOR'S REPORT FORM

### **NEW COURSE PROPOSAL: " Cloud Security"**

<b>Department(s)</b>	Computer Systems Technology
<b>Academic Level</b>	<input checked="" type="checkbox"/> Regular <input type="checkbox"/> Compensatory <input type="checkbox"/> Developmental <input type="checkbox"/> Remedial
<b>Subject Area</b>	Cybersecurity
<b>Course Prefix</b>	CST
<b>Course No.</b>	4716
<b>Course Title</b>	Cloud Security
<b>Catalog Description</b>	Provides the knowledge and technical skills required to design, manage, and secure data, infrastructure and applications in the cloud using best current practices. Exposure to multiple cloud technologies via the course lab exercises. To ensure the course fully aligns with the industry, the textbook used in this course is the official body of knowledge for CCSP (Certified Security Cloud Professional) credential.
<b>Prerequisites</b>	CST2410
<b>Credits</b>	3
<b>Contact Hours</b>	4 (2 lecture and 2 lab hours)
<b>Liberal Arts</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>Course Attribute</b>	It is not a writing intensive course
<b>Course Applicability</b>	<input checked="" type="checkbox"/> Major <input type="checkbox"/> Gen Ed Required <input type="checkbox"/> Gen Ed - Flexible <input type="checkbox"/> Gen Ed - College Option <input type="checkbox"/> English Composition <input type="checkbox"/> World Cultures <input type="checkbox"/> Speech <input type="checkbox"/> Mathematics <input type="checkbox"/> US Experience in its Diversity <input type="checkbox"/> Interdisciplinary <input type="checkbox"/> Science <input type="checkbox"/> Creative Expression <input type="checkbox"/> Advanced Liberal Arts <input type="checkbox"/> Individual and Society <input type="checkbox"/> Scientific World
<b>Effective Term</b>	Fall 2024

### **Rationale**

Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who

understand how to secure such environments. This course attempts to fill this gap by providing students with the knowledge and technical skills required to design, manage, and secure data, infrastructure and applications in the cloud using best current practices.

### 9.3 New Course Proposal #3: CST 4726 – Mobile Device Security and Privacy

#### ***NEW COURSE PROPOSAL***

*Fall 2023*

#### **“Mobile Device Security and Privacy”**

Respectfully submitted to College Council Curriculum Committee *by*:

Dr. Yu-Wen Chen, Computer Systems Technology Department



## CURRICULUM MODIFICATION PROPOSAL FORM

<b>Title of Proposal</b>	New Course: Mobile Device Security and Privacy		
<b>Date</b>	08/31/2023		
<b>Major or Minor</b>	Major		
<b>Proposer's Name</b>	Dr. Yu-Wen Chen,		
<b>Department</b>	Computer Systems Technology		
<b>Date of Departmental Meeting in which proposal was approved</b>	03/17/2023		
<b>Department Chair Name</b>	Ashwin Satyanarayana		
<b>Department Chair Signature and Date</b>	Ashwin Satyanarayana	 Digitally signed by Ashwin Satyanarayana Date: 2023.09.12 10:40:45 -04'00'	09/12/2023
<b>Academic Dean Name</b>	Gerarda M. Shields		
<b>Academic Dean Signature and Date</b>	Gerarda M. Shields  Digitally signed by Gerarda M. Shields Date: 2023.09.14 16:59:28 -04'00'		
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body).	This course focuses on information and network security aspects that arise in this challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. This course covers standards and research challenges in deployed and future systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Students acquire knowledge of security and privacy in mobile systems. Students study and research the required infrastructure, protocols, and design to secure applications and communications in the mobile space. Students also apply various tools to assess the vulnerabilities and use the best practices to secure the applications and services.		
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	In today's world, mobile devices play an essential role in our daily routines, yet the significance of mobile security is often underestimated. These devices hold valuable information - from our contact lists, passwords, emails, texts, and more. Therefore, secure access to mobile devices is crucial for maintaining cybersecurity. As mobile devices are being utilized more frequently for remote work, it is imperative that we prioritize both privacy and usability while ensuring top-notch security. The proposed CST4726 provides complete knowledge and hands-on skills in mobile device security and privacy to the students in the BS Cybersecurity program.		

<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	This is a new proposal.
--	-------------------------

**ALL PROPOSAL CHECK LIST**

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	X
Documentation of Advisory Commission views (if applicable).	X
Completed <a href="#">Chancellor's Report Form</a> .	X

**EXISTING PROGRAM MODIFICATION PROPOSALS**

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	N/A

## NEW COURSE PROPOSAL FORM

<b>Course Title</b>	<b>Mobile Device Security and Privacy</b>
<b>Proposal Date</b>	Aug. 31, 2023
<b>Proposer's Name</b>	Dr. Yu-Wen Chen
<b>Course Number</b>	CST4726
<b>Course Credits, Hours</b>	3 credits, 2 class hours, 2 lab hours
<b>Course Pre / Co-Requisites</b>	CST3610 and CST3507
<b>Catalog Course Description</b>	How to diagnose and address network security aspects arise in the challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Exercises include research into the required infrastructure, protocols, and design to secure applications and communications in the mobile space; and applying various tools to assess vulnerabilities and use best practices to secure both applications and services.
<b>Brief Rationale</b> Provide a concise summary of why this course is important to the department, school or college.	In today's world, mobile devices play an essential role in our daily routines, yet the significance of mobile security is often underestimated. These devices hold valuable information - from our contact lists, passwords, emails, texts, and more. Therefore, secure access to mobile devices is crucial for maintaining cybersecurity. As mobile devices are being utilized more frequently for remote work, it is imperative that we prioritize both privacy and usability while ensuring top-notch security. The proposed CST4726 provides complete knowledge and hands-on skills in mobile device security and privacy to the students in the BS Cybersecurity program.
<b>CUNY – Course Equivalencies</b> Provide information about equivalent courses within CUNY, if any.	N/A
<b>Intent to Submit as Common Core</b> If this course is intended to fulfill one of the requirements in the common core, then indicate which area.	N/A
<b>For Interdisciplinary Courses:</b>	N/A
- Date submitted to ID Committee for review	N/A
- Date ID recommendation received	N/A
- Will all sections be offered as ID? Y/N	N/A
<b>Intent to Submit as a Writing Intensive Course</b>	N/A

## NEW COURSE PROPOSAL CHECK LIST

<b>Completed NEW COURSE PROPOSAL FORM</b>	
• Title, Number, Credits, Hours, Catalog course description	X
• Brief Rationale	X
• CUNY – Course Equivalencies	X
Completed <a href="#">Library Resources and Information Literacy Form</a>	X
<b>Course Outline</b> Include within the outline the following.	X
Hours and Credits for Lecture and Labs If hours exceed mandated Carnegie Hours, then rationale for this	X
Prerequisites/Co- requisites	X
Detailed Course Description	X
Course Specific Learning Outcome and Assessment Tables • Discipline Specific • General Education Specific Learning Outcome and Assessment Tables	X
Example Weekly Course outline	X
Grade Policy and Procedure	X
Recommended Instructional Materials (Textbooks, lab supplies, etc)	X
Library resources and bibliography	X
<b>Course Need Assessment.</b> Describe the need for this course. Include in your statement the following information.	
Target Students who will take this course. Which programs or departments, and how many anticipated? Documentation of student views (if applicable, e.g. non-required elective).	X
Projected headcounts (fall/spring and day/evening) for each new or modified course.	X
If additional physical resources are required (new space, modifications, equipment), description of these requirements. If applicable, Memo or email from the VP for Finance and Administration with written comments regarding additional and/or new facilities, renovations or construction.	X
Where does this course overlap with other courses, both within and outside of the department?	X
Does the Department currently have full time faculty qualified to teach this course? If not, then what plans are there to cover this?	X
If needs assessment states that this course is required by an accrediting body, then provide documentation indicating that need.	X
<b>Course Design</b>	

Describe how this course is designed.	
Course Context (e.g. required, elective, capstone)	X
Course Structure: how the course will be offered (e.g. lecture, seminar, tutorial, fieldtrip)?	X
Anticipated pedagogical strategies and instructional design (e.g. Group Work, Case Study, Team Project, Lecture)	X
How does this course support Programmatic Learning Outcomes?	X
Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.	X
<b>Additional Forms for Specific Course Categories</b>	
<a href="#">Interdisciplinary Form</a> (if applicable)	N/A
Interdisciplinary Committee Recommendation (if applicable and if received)* *Recommendation must be received before consideration by full Curriculum Committee	N/A
<a href="#">Common Core (Liberal Arts) Intent to Submit</a> (if applicable)	N/A
Writing Intensive Form if course is intended to be a WIC (under development)	N/A
If course originated as an experimental course, then results of evaluation plan as developed with director of assessment.	N/A
<b>(Additional materials for Curricular Experiments)</b>	
Plan and process for evaluation developed in consultation with the director of assessment. (Contact Director of Assessment for more information).	N/A
Established Timeline for Curricular Experiment	N/A

## LIBRARY RESOURCES & INFORMATION LITERACY: MAJOR CURRICULUM MODIFICATION

<b>1 Title of proposal</b> CST4726 - Mobile Device Security and Privacy	<b>Department/Program</b> Computer Systems Technology / BS in Cybersecurity
<b>Proposed by</b> (include email & phone) Dr. Yu-Wen Chen <a href="mailto:YWChen@citytech.cuny.edu">YWChen@citytech.cuny.edu</a> 718-260-5325	<b>Expected date course(s) will be offered</b> Fall 2024  <b># of students:</b> 24

- 2 The library cannot purchase reserve textbooks for every course at the college, nor copies for all students. Consult our website (<http://cityte.ch/curriculum>) for articles and ebooks for your courses, or our open educational resources (OER) guide (<http://cityte.ch/oer>). Have you considered using a freely-available OER or an open textbook in this course?**

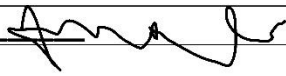
Yes, this course will also use some of the freely available OER or resources as partial selective readings.

- 3 Beyond the required course materials, are City Tech library resources sufficient for course assignments? If additional resources are needed, please provide format details (e.g. ebook, journal, DVD, etc.), full citation (author, title, publisher, edition, date), price, and product link.**

Yes, City Tech Library resources are sufficient for the proposed course assignments because the main readings for the course are a required textbook and journal articles that will be assigned by instructor. Students should be able to locate the selected journal articles in library.

- 4 Library faculty focus on strengthening students' information literacy skills in finding, critically evaluating, and ethically using information. We collaborate on developing assignments and customized instruction and research guides. When this course is offered, how do you plan to consult with the library faculty subject specialist for your area? Please elaborate.**

I will reach out to the library subject specialist via email to arrange an information session in which the library subject specialist can present to the students of this course, the use of library databases, citation convention and discuss copyright issues.

- 5 Library Faculty Subject Specialist** Prof. Junior Tidal   
Anne Leonard signing for Junior Tidal

**Comments and Recommendations** The topic of mobile device security is an especially apt one for an information literacy orientation, since there is a lot of popular, professional, and scholarly information on the topic. A collaboration between the instructor and librarian subject specialist will be important to develop this lesson. Access to the syllabus, reading list, and bibliography will help the library develop the print and

**Date** 9/25/2023 online collection in support of this topic.

---



## **Course Overview & Rationale**

Mobile devices continue to evolve and penetrate our everyday lives, leading to the increased importance of mobile security - a topic of wireless communication, mobile computing, and computer security. Many underestimate the value a phone truly holds when it comes to the information it stores. For example, cell phones, tablets, computers, and more have become a dominant part of our everyday lives, and these devices store information such as our contact list, passwords, emails, texts, and so on. Information that needs to be protected from those who seek to access it without our knowing.

Secure mobile access is an important component of a cybersecurity strategy. As mobile devices become a more widely used option for remote work, the data, applications, and systems they access are at increased risk of being compromised by infected devices. At the same time, mobile security needs to prioritize the needs of the device users, including privacy and usability.

This course focuses on information and network security aspects that arise in this challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. This course covers standards and research challenges in deployed and future systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Students acquire knowledge of security and privacy in mobile systems. Students study and research the required infrastructure, protocols, and design to secure applications and communications in the mobile space. Students also apply various tools to assess the vulnerabilities and use the best practices to secure the applications and services.

## **Course Outline**

**New York City College of Technology/CUNY  
Computer Systems Technology Department**

### **CST 4726 – Mobile Device Security and Privacy**

3 credits

2 class hours, 2 lab hours

#### **Course Description:**

Mobile devices continue to evolve and penetrate our everyday lives, leading to the increased importance of mobile security - a topic of wireless communication, mobile computing, and computer security. This course focuses on information and network security aspects that arise in this challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. This course covers standards and research challenges in deployed and future systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Students acquire knowledge of security and privacy in mobile systems. Students study and research the required infrastructure, protocols, and design to secure applications and communications in the mobile space. Students also apply various tools to assess the vulnerabilities and use the best practices to secure the applications and services.

#### **Course Objectives:**

This course fosters in students' knowledge of security and privacy needs in mobile systems. This course also teaches students how to identify and assess vulnerabilities, analyze, and apply the best practices to secure applications and services in the mobile space.

#### **Learning Outcomes:**

1. Understand and able to describe the evolution of data, wireless, and mobile networks.
2. Identify and examine security and privacy issues in mobile systems.
3. Identify, and analyze mobile attacks and be able to select and apply cybersecurity safeguards.
4. Assess the vulnerabilities and analyze them with various tools.
5. Recognize and design secure applications, protocols, and services in the mobile space.

#### **General Education Learning Outcomes:**

1. Demonstrate the ability to work collaboratively and independently on assignments in and outside a classroom setting.
2. Understand and employ both quantitative and qualitative analysis to solve problems.
3. Develop reading, writing competencies, and listening skills.
4. Work with teams. Build consensus. Use creativity.

**Prerequisites:** CST3610 and CST3507

**Required textbook:**

Security of Mobile Communications by Nouredine Boudriga, 2010.

Recommended: Doherty, Jim. *Wireless and Mobile Device Security*, Second Edition, Burlington, MA: Jones & Bartlett Learning, 2022 (ISBN 9781284211726)

**Other References:**

- Android Security: Attacks and Defenses by Abhishek Dubey and Anmol Misra, 2013.
- Hacking Android, S. R. Kotipalli and M. A. Imran, PacktPublishing Co., 2016, ISBN: 978-1785888007
- The Mobile Application Hacker's Handbook 1st Edition, D. Chell, T. Erasmus, S. Colley, O. Whitehouse, John Wiley & Sons, 2015, ISBN: 978-1118958506
- Mobile Application Security by Himanshu Dwivedi, Chris Clark, and David Thiel, 2010.
- Security for Telecommunications Networks by Patrick Traynor, Patrick McDaniel, and Thomas La Porta, 2008.
- Fundamentals of Wireless Communication by David Tse and Pramod Viswanath, 2005. (Available online: [https://web.stanford.edu/~dntse/wireless\\_book.html](https://web.stanford.edu/~dntse/wireless_book.html))
- Cryptography and Network Security: Principles and Practices by William Stallings (ISBN: 0-13-091429-0)
- Wireless Security: Models, Threats, and Solutions by R. K. Nichols and P. C. Lekkas (ISBN 0071380388)

**Assignments and Labs:** Assignments and labs will be based on the related readings and other selected practices.

**Project:** The term project requires students to conduct a thoughtful study on a specific course-related topic (selected by students and approved by the instructor). Students need to present in class with PowerPoint slides and submit a formal project report at the end of the semester. More details will be discussed throughout the semester.

**Online Certificate:** Students are required to complete the certificate “AWR385 Mobile Device Security and Privacy” offered by the TEEX. The URL for registering the online certificate: <https://teex.org/class/AWR385/>

**Grade Requirement:** Students must complete the term project, online certificate, exams, assignments, and quizzes, and participate in the class.

**Course grading formula:**

Assignments/Labs	25%
Projects	15%
Certificates	15%

Participation & Quizzes	15%
Midterm Exam	15%
Final Exam	15%
	100%

### **Grading Policy:**

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numeric Grade	100-93	92.9-90	89.9-87	86.9-83	82.9-80	79.9-77	76.9-70	69.9-60	59 and below

**Progression Requirements:** Students majoring in CST must earn a “C” or better grade in this course.

### **Topics and Schedule:**

Week	Topics	Reading
1	Mobile Devices and general security challenges	Ch1, Ch2
2	Telecom Systems, Protocols, and Security; Telcom Systems Security Issues	Ch3, Selected readings [1], [2]
3 – 4	WiFi Security and WiFi Privacy Issues	Ch7, Selected readings [3], [4]
4 – 5	Personal Area Networks	Selected readings [5], [6]
6 – 7	NFC and Mobile Payment	Ch13, Selected readings [7]-[9]
7	Midterm Exam	
8	Introduction of Mobile Sensing and Context; Location Services, and Mobile Sensing Risks	Ch10, Ch11
9	Security Values of Sensor Data	Ch11
10	Mobile Apps & Analysis Tools	Ch13, Ch14, Ch15
11	Mobile OS & App Security	Selected readings [10]-[13]
12	Mobile Devices Policies & Best Practices; From Mobile to IoT	Selected reading [14]
13	IoT Security & Privacy	Selected reading [15]
14	Mobile Devices in Enterprise & Other Systems (Cyber-Physical Systems, Smart Vehicles, etc.,)	Selected readings [16], [17]
15	Project Presentation & Final Exam	

### **Selected Readings:**

- [1] <https://www.cise.ufl.edu/~traynor/papers/jcs08.pdf>
- [2] [https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat\\_DC\\_2011\\_Perez-Pico\\_Mobile\\_Attacks-wp.pdf](https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf)
- [3] [https://www.interlinknetworks.com/whitepapers/Layer2\\_Layer3\\_whitepaper\\_03\\_2006.pdf](https://www.interlinknetworks.com/whitepapers/Layer2_Layer3_whitepaper_03_2006.pdf)
- [4] [https://www.usenix.org/legacy/event/hotos07/tech/full\\_papers/greenstein/greenstein.pdf](https://www.usenix.org/legacy/event/hotos07/tech/full_papers/greenstein/greenstein.pdf)
- [5] <https://ieeexplore.ieee.org/document/5447506>
- [6] <https://ieeexplore.ieee.org/document/5396321>
- [7] [https://members.nfc-forum.org/resources/white\\_papers/Innovision\\_whitePaper1.pdf](https://members.nfc-forum.org/resources/white_papers/Innovision_whitePaper1.pdf)
- [8] <https://www.semanticscholar.org/paper/Security-in-Near-Field-Communication-%28-NFC-%29-and-Haselsteiner/cbe90ce9e3b721dc2429a82618bb9ce06cfae283?p2df>

- [9] <https://wnss.sv.cmu.edu/papers/wowmom-12p.pdf>  
 [10] <https://dl.acm.org/doi/10.1145/2046614.2046618>  
 [11] <https://dl.acm.org/doi/10.1145/2435349.2435378>  
 [12] <https://dl.acm.org/doi/10.1145/2185448.2185464>  
 [13] [https://faculty.cc.gatech.edu/~pearce/papers/addroid\\_asiacs\\_2012.pdf](https://faculty.cc.gatech.edu/~pearce/papers/addroid_asiacs_2012.pdf)  
 [14] <https://mews.sv.cmu.edu/papers/usenixSec-17.pdf>  
 [15] <https://ieeexplore-ieee-org.central.ezproxy.cuny.edu/stamp/stamp.jsp?tp=&arnumber=9187908>  
 [16] [https://www.usenix.org/legacy/events/sec10/tech/full\\_papers/Rouf.pdf](https://www.usenix.org/legacy/events/sec10/tech/full_papers/Rouf.pdf)  
 [17] <https://eprint.iacr.org/2010/332.pdf>

### Course Assessment:

Course-specific outcomes	Assessment methods
1. Understand and able to describe the evolution of data, wireless, and mobile networks. 2. Identify and examine security and privacy issues in mobile systems.	<ul style="list-style-type: none"> <li>• Quizzes</li> <li>• Assignments/Labs</li> <li>• Certificate</li> <li>• Participation</li> <li>• Exams</li> </ul>
3. Identify, and analyze mobile attacks and be able to select and apply cybersecurity safeguards. 4. Assess the vulnerabilities and analyze them with various tools.	<ul style="list-style-type: none"> <li>• Quizzes</li> <li>• Assignments/Labs</li> <li>• Participation</li> <li>• Exams</li> </ul>
5. Recognize and design secure applications, protocols, and services in the mobile space.	<ul style="list-style-type: none"> <li>• Term Project</li> <li>• Assignments/Labs</li> <li>• Certificate</li> <li>• Participation</li> </ul>

General Education Learning Outcomes	Assessment Methods
1. Demonstrate the ability to work collaboratively and independently on assignments in and outside a classroom setting.	<ul style="list-style-type: none"> <li>• Classroom discussions,</li> <li>• Term project</li> </ul>
2. Understand and employ both quantitative and qualitative analysis to solve problems.	<ul style="list-style-type: none"> <li>• Classroom discussion</li> <li>• Group in-class activities</li> <li>• Term project</li> <li>• Quizzes</li> <li>• Exams</li> </ul>
3. Develop reading, writing competencies, and listening skills.	<ul style="list-style-type: none"> <li>• Writing assignments (Each assignment requires writing)</li> <li>• Term project report</li> <li>• Classroom discussion.</li> </ul>

4. Work with teams. Build consensus. Use creativity.	• Term project and presentation
--	---------------------------------

### **New York City College of Technology Policy on Academic Integrity:**

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using, crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. The complete text of the College policy on Academic Integrity may be found in the catalog.

New York City College of Technology, like all academic institutions, encourages and thrives on the open exchange of ideas. At City Tech, we expect everyone to conduct their intellectual work with honesty and integrity. With this goal in mind, and in response to the Report of the CUNY Committee on Academic Integrity (<http://web.cuny.edu/academics/info-central/policies/academic-integrity-report.pdf>) the NYCCT College Council approved a new academic integrity policy in May 2007. City Tech's academic integrity policy aims to deter academic dishonesty by students and allow the college to process cases of academic dishonesty more effectively. This policy has been in effect as of August 27, 2008.

### **Accessibility Statement:**

Accessibility Statement City Tech is committed to supporting the educational goals of enrolled students with disabilities in the areas of enrollment, academic advisement, tutoring, assistive technologies, and testing accommodations. If you have or think you may have a disability, you may be eligible for reasonable accommodations or academic adjustments as provided under applicable federal, state, and/or city laws. You may also request services for temporary conditions or medical issues under certain circumstances. If you have questions about your eligibility and/or would like to seek accommodation services and/or academic adjustments, please contact the Student Accessibility Center (SAC) at 300 Jay Street. Room L-237; telephone: 718-260-5143; WWW: <http://www.citytech.cuny.edu/accessibility/>.

### **City Tech Computer Systems Technology Department Commitment to Student Diversity:**

This course welcomes students from all backgrounds, experiences and perspectives. In accordance with the City Tech and CUNY missions, this course intends to provide an atmosphere of inclusion, respect, and the mutual appreciation of differences so that together we can create an environment in which all students can flourish. It is the instructor's goal to provide materials and activities that are welcoming and accommodating of diversity in all of its forms, including race, gender identity and presentation, ethnicity, national origin, religion, cultural identity, socioeconomic background, sexuality and sexual orientation, ability, neurodivergence, age, and etc. Your instructor is committed to equity and actively seeks ways to challenge institutional racism, sexism, ableism and other forms of prejudice. Your

input is encouraged and appreciated. If a dynamic that you observe or experience in the course concerns you, you may respectfully inform your instructor without fear of how your concerns will affect your grade. Let your instructor know how to improve the effectiveness of the course for you personally, or for other students or student groups. We acknowledge that NYCCT is located on the traditional homelands of the Canarsie and Lenape peoples.

## **Course Need**

**Students who would take this class:** students who intend to major in Cybersecurity

**Department:** Computer Systems Technology

**Program:** Bachelors in Cybersecurity

**The number of section (s) anticipated:** one section for the first year

**Projected headcount:** 24 students

**Physical Resources required:** Basic smart room set-up: a screen, and an overhead projector/a TV set that is run by and connected to a computer.

**Course overlap:** None

**Faculty qualified for teaching this course:** Yes, there are faculty members who have doctoral degrees in Computer Science with the concentration in Cybersecurity for various domains.

## **Course Design**

**Course context:** This course will be required of Cybersecurity major students. Students are required to develop an independent project at the end of the semester.

**Course structure:** This course will be offered in a lecture style/format.

**Anticipated Pedagogical Strategies and Instructional Design:** This class will be run in a lecture-activity style/format. The class will start with a lecture, and involve the in-class activities, such as group discussion, hands-on exercises, and hands-on labs.

**Providing Support to Programmatic Learning Outcomes:** This course requires satisfactory completion of individual assignments, quizzes, on-line certificate, exams and the final group project.

**Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.** Not online; all in-person.



## CHANCELLOR'S REPORT FORM

### ***NEW COURSE PROPOSAL: "Capstone Cybersecurity Course "***

<b>Department(s)</b>	Computer Systems Technology
<b>Academic Level</b>	<input checked="" type="checkbox"/> Regular <input type="checkbox"/> Compensatory <input type="checkbox"/> Developmental <input type="checkbox"/> Remedial
<b>Subject Area</b>	Cybersecurity
<b>Course Prefix</b>	CST
<b>Course No.</b>	4726
<b>Course Title</b>	Mobile Device Security and Privacy
<b>Catalog Description</b>	How to diagnose and address network security aspects arise in the challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and mobile telecommunication systems. Topics include but are not limited to telecom vulnerabilities, security, and privacy in the smartphone, mobile internet, mobile app, and Internet of Things (IoT). Exercises include research into the required infrastructure, protocols, and design to secure applications and communications in the mobile space; and applying various tools to assess vulnerabilities and use best practices to secure both applications and services.
<b>Prerequisites</b>	CST3610 and CST3507
<b>Credits</b>	3
<b>Contact Hours</b>	4 (2 lecture and 2 lab hours)
<b>Liberal Arts</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>Course Attribute</b>	It is not a writing intensive course
<b>Course Applicability</b>	<input checked="" type="checkbox"/> Major <input type="checkbox"/> Gen Ed Required <input type="checkbox"/> Gen Ed - Flexible <input type="checkbox"/> Gen Ed - College Option <input type="checkbox"/> English Composition <input type="checkbox"/> World Cultures <input type="checkbox"/> Speech <input type="checkbox"/> Mathematics <input type="checkbox"/> US Experience in its Diversity <input type="checkbox"/> Interdisciplinary <input type="checkbox"/> Science <input type="checkbox"/> Creative Expression <input type="checkbox"/> Advanced Liberal Arts <input type="checkbox"/> Individual and Society <input type="checkbox"/> Scientific World
<b>Effective Term</b>	Fall 2024

## **Rationale**

Mobile devices continue to evolve and penetrate our everyday lives, leading to the increased importance of mobile security - a topic of wireless communication, mobile computing, and computer security. Many underestimate the value a phone truly holds when it comes to the information it stores. For example, cell phones, tablets, computers, and more have become a dominant part of our everyday lives, and these devices store information such as our contact list, passwords, emails, texts, and so on. Information that needs to be protected from those who seek to access it without our knowing.

Secure mobile access is an important component of a cybersecurity strategy. As mobile devices become a more widely used option for remote work, the data, applications, and systems they access are at increased risk of being compromised by infected devices. At the same time, mobile security needs to prioritize the needs of the device users, including privacy and usability.

## 9.4 New Course Proposal #4: CST 4816 – Cybersecurity and Penetration Testing

### ***NEW COURSE PROPOSAL***

*Fall 2023*

#### **“Cybersecurity and Penetration Testing”**

Respectfully submitted to College Council Curriculum Committee *by*:

Prof. Badreddine Oudjehane, Computer Systems Technology Department

CURRICULUM MODIFICATION PROPOSAL FORM

<b>Title of Proposal</b>	<b>Cybersecurity and Penetration Testing</b>
<b>Date</b>	<b>September 10, 2023</b>
<b>Major or Minor</b>	<b>Major</b>
<b>Proposer's Name</b>	<b>Badreddine Oudjehane</b>
<b>Department</b>	<b>Computer Systems Technology</b>
<b>Date of Departmental Meeting in which proposal was approved</b>	<b>09/08/2023</b>
<b>Department Chair Name</b>	<b>Ashwin Satyanarayana</b>
<b>Department Chair Signature and Date</b>	Ashwin Satyanarayana <small>Digitally signed by Ashwin Satyanarayana Date: 2023.09.12 10:41:03 -04'00'</small> <b>09/12/2023</b>
<b>Academic Dean Name</b>	<b>Gerarda M. Shields</b>
<b>Academic Dean Signature and Date</b>	<b>Gerarda M. Shields</b> <small>Digitally signed by Gerarda M. Shields Date: 2023.09.14 16:59:52 -04'00'</small>
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body).	The "Cybersecurity and Penetration Testing" course is an advanced class within our new CST Bachelor of Science in Cybersecurity program. This course offers a hands-on exploration of advanced cybersecurity concepts using penetration testing methods. It emphasizes assessing system vulnerabilities and implementing protective measures against both current and emerging malicious threats. Students will explore ethical hacking, attack vectors, and effective countermeasures for threats against government institutions and industries. The curriculum of this course encompasses network packet analysis, system penetration testing techniques, and practical exercises in a virtual environment, providing students with experience with modern cybersecurity tools and approaches.
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	The course is essential for integrating the knowledge students acquire in lower and mid-level cybersecurity courses with modern tools for detecting, identifying, and counteracting cyber-threats. It enhances the CST Bachelor of Science in Cybersecurity program by engaging students in hands-on labs and class projects to address contemporary cyber threats. The course underscores the importance of the cybersecurity specialist role in today's world and examines their responsibilities in various organizational contexts. Neither CST Department nor other CUNY institutions offer a similar course.
<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	New proposal.

**ALL PROPOSAL CHECK LIST**

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	N/A
Documentation of Advisory Commission views (if applicable).	N/A
Completed <a href="#">Chancellor's Report Form</a> .	X

**EXISTING PROGRAM MODIFICATION PROPOSALS**

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	N/A

## NEW COURSE PROPOSAL FORM

<b>Course Title</b>	<b>Cybersecurity and Penetration Testing</b>
<b>Proposal Date</b>	September 12, 2023
<b>Proposer's Name</b>	Badreddine Oudjehane
<b>Course Number</b>	CST 4816
<b>Course Credits, Hours</b>	3 credits, 2 class hours, 2 lab hours
<b>Course Pre / Co-Requisites</b>	CST 3610
<b>Catalog Course Description</b>	Assessing vulnerabilities of systems and networks of systems in order to learn to protect organizations and adapt their security policies to counter and minimize the effects and risks associated with malicious attacks. An in-depth examination of ethical hacking phases, various attack vectors, and preventative countermeasures including network packet analysis and system penetration testing techniques. Class assignments are hands-on and designed around the principle that the best way to learn is by doing. Practice in an isolated virtual environment and get comfortable in the use of current cyber security tools and methodologies.
<b>Brief Rationale</b> Provide a concise summary of why this course is important to the department, school or college.	Given the evolving nature of cybersecurity-related threats and the growing need for robust digital defenses, hands-on, project-based learning is essential. The course highlights the significance of the cybersecurity specialist role in today's world and explores their responsibilities in various organizational contexts. It also improves students' problem-solving, teamwork, and communication skills, which are vital in the collaborative field of cybersecurity. The course is crucial for bridging the gap between academic learning and practical application, ensuring graduates are industry-ready and properly equipped to address novel challenges of the cybersecurity world.
<b>CUNY – Course Equivalencies</b> Provide information about equivalent courses within CUNY, if any.	N/A
<b>Intent to Submit as Common Core</b> If this course is intended to fulfill one of the requirements in the common core, then indicate which area.	N/A
<b>For Interdisciplinary Courses:</b> - Date submitted to ID Committee for review	N/A
- Date ID recommendation received	N/A
- Will all sections be offered as ID? Y/N	N/A
<b>Intent to Submit as a Writing Intensive Course</b>	N/A

## NEW COURSE PROPOSAL CHECK LIST

<b>Completed NEW COURSE PROPOSAL FORM</b>	
• Title, Number, Credits, Hours, Catalog course description	X
• Brief Rationale	X
• CUNY – Course Equivalencies	X
Completed <a href="#">Library Resources and Information Literacy Form</a>	
<b>Course Outline</b> Include within the outline the following.	
Hours and Credits for Lecture and Labs If hours exceed mandated Carnegie Hours, then rationale for this	X
Prerequisites/Co- requisites	X
Detailed Course Description	
Course Specific Learning Outcome and Assessment Tables • Discipline Specific • General Education Specific Learning Outcome and Assessment Tables	X
Example Weekly Course outline	X
Grade Policy and Procedure	X
Recommended Instructional Materials (Textbooks, lab supplies, etc.)	X
Library resources and bibliography	X
<b>Course Need Assessment.</b> Describe the need for this course. Include in your statement the following information.	
Target Students who will take this course. Which programs or departments, and how many anticipated? Documentation of student views (if applicable, e.g. non-required elective).	X
Projected headcounts (fall/spring and day/evening) for each new or modified course.	X
If additional physical resources are required (new space, modifications, equipment), description of these requirements. If applicable, Memo or email from the VP for Finance and Administration with written comments regarding additional and/or new facilities, renovations or construction.	X
Where does this course overlap with other courses, both within and outside of the department?	X
Does the Department currently have full time faculty qualified to teach this course? If not, then what plans are there to cover this?	X
If needs assessment states that this course is required by an accrediting body, then provide documentation indicating that need.	N/A
<b>Course Design</b> Describe how this course is designed.	

Course Context (e.g. required, elective, capstone)	X
Course Structure: how the course will be offered (e.g. lecture, seminar, tutorial, fieldtrip)?	X
Anticipated pedagogical strategies and instructional design (e.g. Group Work, Case Study, Team Project, Lecture)	X
How does this course support Programmatic Learning Outcomes?	X
Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.	X
<b>Additional Forms for Specific Course Categories</b>	
<a href="#">Interdisciplinary Form</a> (if applicable)	N/A
Interdisciplinary Committee Recommendation (if applicable and if received)* *Recommendation must be received before consideration by full Curriculum Committee	N/A
<a href="#">Common Core (Liberal Arts) Intent to Submit</a> (if applicable)	N/A
Writing Intensive Form if course is intended to be a WIC (under development)	N/A
If course originated as an experimental course, then results of evaluation plan as developed with director of assessment.	N/A
<b>(Additional materials for Curricular Experiments)</b>	
Plan and process for evaluation developed in consultation with the director of assessment. (Contact Director of Assessment for more information).	N/A
Established Timeline for Curricular Experiment	N/A



## LIBRARY RESOURCES & INFORMATION LITERACY: MAJOR CURRICULUM MODIFICATION

<b>1</b>	<b>Title of proposal</b> CST 4816 – Cybersecurity and Penetration Testing	<b>Department/Program</b> Computer Systems Technology / BS in Cybersecurity
	<b>Proposed by</b> (include email & phone) Badreddine Oudjehane <a href="mailto:BOudjehane@citytech.cuny.edu">BOudjehane@citytech.cuny.edu</a> 718-260-5122	<b>Expected date course(s) will be offered</b> Fall 2024  <b># of students:</b> 24

- 2** The library cannot purchase reserve textbooks for every course at the college, nor copies for all students. Consult our website (<http://cityte.ch/curriculum>) for articles and eBooks for your courses, or our open educational resources (OER) guide (<http://cityte.ch/oer>). Have you considered using a freely-available OER or an open textbook in this course?

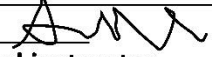
Yes, this course will also use some of the freely available OER or resources as partial selective readings.

- 3** Beyond the required course materials, are City Tech library resources sufficient for course assignments? If additional resources are needed, please provide format details (e.g. eBook, journal, DVD, etc.), full citation (author, title, publisher, edition, date), price, and product link.

Yes, City Tech Library resources are sufficient for the proposed course assignments because the main readings for the course are a required textbook and journal articles that will be assigned by instructor. Students should be able to locate the selected journal articles in library.

- 4** Library faculty focus on strengthening students' information literacy skills in finding, critically evaluating, and ethically using information. We collaborate on developing assignments and customized instruction and research guides. When this course is offered, how do you plan to consult with the library faculty subject specialist for your area? Please elaborate.

I will reach out to the library subject specialist via email to arrange an information session in which the library subject specialist can present to the students of this course, the use of library databases, citation convention and discuss copyright issues.

- 5 **Library Faculty Subject Specialist** Anne Leonard for Prof. Junior Tidal   
**Comments and Recommendations:** The librarian subject specialist and instructor should collaborate on an information literacy lesson to support students' abilities to find and evaluate relevant information. The use of journal articles as assigned readings is a good entry point to help students develop this information literacy skill. As always, access to the course syllabus, reading list, and bibliography helps the  
**Date** librarian subject specialist develop the print & online collection in support of the course.

**Date** 9 25 2023

## **Course Overview & Rationale**

The "Cybersecurity and Penetration Testing" course is an integral part of our new CST Bachelor of Science in Cybersecurity program. It provides students with a comprehensive, hands-on exploration of evolving cybersecurity challenges. It is emphasizing the assessment of system vulnerabilities to prepare students to effectively counter both present and emerging threats. Students are engaging into ethical hacking, diverse attack vectors, and proactive countermeasures that are essential for safeguarding government institutions and businesses. A significant emphasis is placed on understanding the ever-changing threat landscape, given the increasing damages from known cybersecurity issues. The course stresses experiential learning while covering network packet analysis and system penetration testing techniques. The structure of this course ensures that students not only grasp advanced concepts but also gain practical experience with contemporary cybersecurity tools and methodologies, equipping them to adapt and respond to real-world challenges.

The rapidly changing landscape of cybersecurity threats demands a deep, practical approach to education. The escalating frequency, sophistication, and potential damage of these threats make it crucial for aspiring cybersecurity professionals to undergo hands-on, project-based learning. Our "Cybersecurity and Penetration Testing" course addresses contemporary challenges, grooming students to become cybersecurity specialists. These specialists will not only comprehend threats and deploy appropriate defenses but will also excel in collaboration, strategy, and clear communication, fostering a comprehensive cyber defense. This course seamlessly integrates theory and practice to shape graduates who are not only knowledgeable in theory but are also skilled practitioners. After completing this course, students will be equipped with the skills, experience, and insight needed to address and mitigate the constantly evolving challenges of the cybersecurity space.

## **Couse Outline**

### **New York City College of Technology/CUNY Computer Systems Technology Department**

#### **CST 4816 – Cybersecurity and Penetration Testing**

3 credits

2 class hours, 2 lab hours

#### **Course Description:**

This course will teach students to understand and learn how to assess vulnerabilities of a system and network of systems to learn to protect organizations and adapt their security policies to counter and minimize the effects and risks associated with malicious attacks. We live in a world where threats are constantly evolving, while many known issues have been responsible for inflicting significant cybersecurity related damages to businesses and institutions. An in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures will provide students with a strong foundation that they can build upon. Students will learn network packet analysis and system penetration testing techniques. This course is hands-on oriented and is designed around the principle that students *learn by doing*. Students will practice in an isolated virtual environment and get comfortable in the use of the current cyber security tools and methodologies.

#### **Prerequisites:**

CST3610

#### **Progression Requirements:**

Students majoring in CST must earn a “C” or better grade in this course.

#### **Required Textbook:**

CompTIA PenTest+ Study Guide: Exam PT0-002, 2nd Edition, Mike Chapple, David Seidl  
ISBN: 978-1-119-82381-0 November 2021

#### **Course Objectives:**

This course fosters in students a better appreciation of the role of a cybersecurity specialist in our modern world. This course teaches students how to identify and assess cyber vulnerabilities and analyze and apply the best practices to secure computer systems. This course also teaches students to understand what is expected from a cybersecurity specialist and functions of a cybersecurity specialist in different company settings. Students will experience working in groups, which is typical in an enterprise.

#### **Course Format:**

The course will be delivered through a combination of lectures, discussions and hands-on activities. Students study security incidents and vulnerability. They will assess systems, scan them for possible vulnerabilities and will apply techniques to control those vulnerabilities. Students will work individually and in teams in many labs to cover the different aspects of cyber security.

**Learning Outcomes:**

1. Apply principles of science, and technology to solve complex cybersecurity problems.
2. Ability to evaluate security vulnerability and assess a risk level score.
3. Ability to properly use methods and tools to evaluate, assess and secure systems.
4. Ability to test security levels of a system through the use of penetration testing techniques.
5. Ability to identify potential threat and use the proper tools to assess the risk level.
6. Ability to use the current tools used in the field of cyber security.
7. Ability to test current defensive implementation and propose solutions.

**General Education Learning Outcomes:**

1. An ability to use the knowledge, techniques, skills, and modern tools of the discipline to cybersecurity.
2. An ability to apply knowledge of mathematics, science, engineering, and technology to cybersecurity defense problems that require application of principles and practical knowledge.
3. An ability to conduct standard tests and measurements, and to conduct, analyze, and interpret experiments.
4. An ability to function effectively as a member of a technical team.

**Grade Requirement:**

Students must participate in team meetings and project development.

**Course grading formula:**

Labs: 35%

Tests/Projects: 35%

Final Exam: 30%

**Grading Policy:**

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numeric Grade	100-93	92.9-90	89.9-87	86.9-83	82.9-80	79.9-77	76.9-70	69.9-60	59-0

**Accessibility Statement:**

Accessibility Statement City Tech is committed to supporting the educational goals of enrolled students with disabilities in the areas of enrollment, academic advisement, tutoring, assistive technologies, and testing accommodations. If you have or think you may have a disability, you may be eligible for reasonable accommodations or academic adjustments as provided under applicable federal, state, and/or city laws. You may also request services for temporary conditions or medical issues under certain circumstances. If you have questions about your eligibility and/or would like to seek accommodation services and/or academic adjustments, please contact the Student Accessibility Center (SAC) at 300 Jay Street. Room L-237; telephone: 718-260-5143; WWW: <http://www.citytech.cuny.edu/accessibility/>.

**Diversity and Inclusive Education Syllabus Statement:**

This course welcomes students from all backgrounds, experiences and perspectives. In accordance with the City Tech and CUNY missions, this course intends to provide an atmosphere of inclusion, respect, and the mutual appreciation of differences so that together we can create an environment in which all students can flourish. It is the instructor's goal to provide materials and activities that are welcoming and accommodating of diversity in all of its forms, including race, gender identity and presentation, ethnicity, national origin, religion, cultural identity, socioeconomic background, sexuality and sexual orientation, ability, neurodivergence, age, and etc. Your instructor is committed to equity and actively seeks ways to challenge institutional racism, sexism, ableism and other forms of prejudice. Your input is encouraged and appreciated. If a dynamic that you observe or experience in the course concerns you, you may respectfully inform your instructor without fear of how your concerns will affect your grade. Let your instructor know how to improve the effectiveness of the course for you personally, or for other students or student groups. We acknowledge that NYCCT is located on the traditional homelands of the Canarsie and Lenape peoples.

**New York City College of Technology Policy on Academic Integrity:**

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using, crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. The complete text of the College policy on Academic Integrity may be found in the catalog.

New York City College of Technology, like all academic institutions, encourages and thrives on the open exchange of ideas. At City Tech, we expect everyone to conduct their intellectual work with honesty and integrity. With this goal in mind, and in response to the Report of the CUNY Committee on Academic Integrity (<http://web.cuny.edu/academics/info-central/policies/academic-integrity-report.pdf>) the NYCCT College Council approved a new academic integrity policy in May 2007. City Tech's academic integrity policy aims to deter academic dishonesty by students and allow the college to process cases of academic dishonesty more effectively. This policy has been in effect as of August 27, 2008.

**Course Schedule:**

<b>Week</b>	<b>Topics</b>	
<b>1</b>	What is cybersecurity? What is ethical hacking?	Chapter 1
	Review of TCP/IP protocols, Operating Systems and Databases	
	Lab: Creating a testing environment.	
<b>2</b>	Planning and Scoping Penetration Tests	Chapter 2
	Information Gathering	Chapter 3
	Lab: Tools of the Trade Project 1: System Scan Report	
<b>3,4,5</b>	Vulnerabilities assessment and Scanning	Chapter 4
	Scans Assessments.	Chapter 5
	Project 1: System Scan Report Lab: OSINT, Shodan	
	Test	
<b>6,7,8</b>	Exploiting Vulnerabilities: Pivoting	Chapter 6
	Exploiting Network Vulnerabilities, Physical and social Lab: NSS Project 2: Metasploit	Chapter 7
	Test	
<b>9,10</b>	Exploiting Application Vulnerabilities	Chapter 8 Chapter 9
	Lab: Security and network Analyzers	
<b>11,12</b>	Systems Attacks Project 3: Replicating and understanding an exploit	Chapter 10
<b>13</b>	Communication and reporting	Chapter 11
	Security and Cloud Technologies Scripting	Chapter 12
	Test	
<b>14,15</b>	Project 3 testing and Presentation Final Exam	

**Course Assessment:**

<b>Course-specific outcomes</b>	<b>Assessment methods</b>
1. Apply principles of science, mathematics, and technology to solve complex cybersecurity problems.	<ul style="list-style-type: none"> <li>• Labs</li> <li>• Projects</li> <li>• Final Exam</li> </ul>

2. Ability to break down a complex cybersecurity problem into components that can be addressed by known cybersecurity tools. 3. Ability to create a solution strategy for a complex cybersecurity problem based on information about the problem. 4. Ability to delineate the scope of the solution strategy and ability to execute the strategy to solve a cybersecurity problem	<ul style="list-style-type: none"> <li>• Projects</li> <li>• Quizzes</li> <li>• Projects</li> <li>• Final Exam</li> </ul>
---	---

<b>General Education Learning Outcomes</b>	<b>Assessment Methods</b>
1. Demonstrate the ability to work collaboratively and independently on assignments in and outside a classroom setting.	<ul style="list-style-type: none"> <li>• Projects</li> <li>• Labs</li> </ul>
2. Understand and employ both quantitative and qualitative analysis to solve problems.	<ul style="list-style-type: none"> <li>• Quizzes</li> <li>• Projects</li> <li>• Final Exam</li> </ul>
3. Develop reading, writing competencies, and listening skills.	<ul style="list-style-type: none"> <li>• Projects</li> </ul>
5. Work with teams. Build consensus. Use creativity.	<ul style="list-style-type: none"> <li>• Projects</li> <li>• Labs</li> </ul>



## **Course Need**

**Students who would take this class:** students who intend to major in Cybersecurity

**Department:** Computer Systems Technology

**Program:** Bachelors in Cybersecurity

**The number of section (s) anticipated:** one to two sections for the first year

**Projected headcount:** 24 students per section

**Physical Resources required:** There are additional requirements to basic smart room set-up in a form of a screen, and an overhead projector/a TV set that is run by and connected to a computer. In addition, advanced hardware equipment and supporting software are needed to successfully deliver their course material. We are currently in the process of identifying, procuring, and deploying the necessary equipment to our Cybersecurity and Networking lab, located in the Namm building, room N-1102. Successful deployment and operation of advanced hardware and software components must be completed by the time the first lectures of these classes commence. It's important to highlight that continuous technical support for the hardware and software components in Room N-1102 will be crucial. Furthermore, it's worth noting that not only students enrolled in our BS program in Cybersecurity will benefit from this equipment. For example, students enrolling in CST2410, CST2307, CST3610, CST4710 will immediately experience improved and more up to date lab environment in their studying experiences

**Course overlap:** None

**Faculty qualified for teaching this course:** Yes, there are faculty members who have doctoral degrees in Computer Science with the concentration in Information Security for various domains.

## **Course Design**

**Course context:** This course will be required of Cybersecurity major students. Students must participate in team meetings, both with and without the course instructor, and in project development and presentation.

**Course structure:** This course will be offered in a lecture style/format.

**Anticipated Pedagogical Strategies and Instructional Design:** This class will be run in a lecture-activity style/format. The class will start with a lecture, and involve the in-class activities, such as group discussion, hands-on exercises and hands-on implementations using available cybersecurity tools.

**Providing Support to Programmatic Learning Outcomes:** This course requires satisfactory completion of labs, projects and tests.

**Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.** Not fully online, all in-person or can be hybrid (with students working in groups on developing their solutions)

## CHANCELLOR'S REPORT FORM

### **NEW COURSE PROPOSAL: " Cybersecurity and Penetration Testing "**

<b>Department(s)</b>	Computer Systems Technology
<b>Academic Level</b>	<input checked="" type="checkbox"/> Regular <input type="checkbox"/> Compensatory <input type="checkbox"/> Developmental <input type="checkbox"/> Remedial
<b>Subject Area</b>	Cybersecurity
<b>Course Prefix</b>	CST
<b>Course No.</b>	4816
<b>Course Title</b>	Cybersecurity and Penetration Testing
<b>Catalog Description</b>	Assessing vulnerabilities of systems and networks of systems in order to learn to protect organizations and adapt their security policies to counter and minimize the effects and risks associated with malicious attacks. An in-depth examination of ethical hacking phases, various attack vectors, and preventative countermeasures including network packet analysis and system penetration testing techniques. Class assignments are hands-on and designed around the principle that the best way to learn is by doing. Practice in an isolated virtual environment and get comfortable in the use of current cyber security tools and methodologies.
<b>Prerequisites</b>	Two CST 36xx courses
<b>Credits</b>	3
<b>Contact Hours</b>	4 (2 lecture and 2 lab hours)
<b>Liberal Arts</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>Course Attribute</b>	It is not a writing intensive course
<b>Course Applicability</b>	<input checked="" type="checkbox"/> Major <input type="checkbox"/> Gen Ed Required <input type="checkbox"/> Gen Ed - Flexible <input type="checkbox"/> Gen Ed - College Option <input type="checkbox"/> English Composition <input type="checkbox"/> World Cultures <input type="checkbox"/> Speech <input type="checkbox"/> Mathematics <input type="checkbox"/> US Experience in its Diversity <input type="checkbox"/> Interdisciplinary <input type="checkbox"/> Science <input type="checkbox"/> Creative Expression <input type="checkbox"/> Advanced Liberal Arts <input type="checkbox"/> Individual and Society <input type="checkbox"/> Scientific World
<b>Effective Term</b>	Spring 2024

## **Rationale**

The rapidly changing landscape of cybersecurity threats demands a deep, practical approach to education. The escalating frequency, sophistication, and potential damage of these threats make it crucial for aspiring cybersecurity professionals to undergo hands-on, project-based learning. Our "Cybersecurity and Penetration Testing" course addresses contemporary challenges, grooming students to become cybersecurity specialists. These specialists will not only comprehend threats and deploy appropriate defenses but will also excel in collaboration, strategy, and clear communication, fostering a comprehensive cyber defense. This course seamlessly integrates theory and practice to shape graduates who are not only knowledgeable in theory but are also skilled practitioners. After completing this course, students will be equipped with the skills, experience, and insight needed to address and mitigate the constantly evolving challenges of the cybersecurity space.

## 9.5 New Course Proposal #5: CST 4916 – Capstone Cybersecurity Course

### ***NEW COURSE PROPOSAL***

*Fall 2023*

#### **“Capstone Cybersecurity Course”**

Respectfully submitted to College Council Curriculum Committee *by*:

Prof. Janusz Kusk, Computer Systems Technology Department

**CURRICULUM MODIFICATION PROPOSAL FORM**

<b>Title of Proposal</b>	Capstone Cybersecurity Course	
<b>Date</b>	Aug. 31, 2023	
<b>Major or Minor</b>	Major	
<b>Proposer's Name</b>	Dr. Janusz Kusiak	
<b>Department</b>	Computer Systems Technology	
<b>Date of Departmental Meeting in which proposal was approved</b>	3/17/2023	
<b>Department Chair Name</b>	Ashwin Satyanarayana	
<b>Department Chair Signature and Date</b>	Ashwin Satyanarayana <small>Digitally signed by Ashwin Satyanarayana Date: 2023.09.12 10:41:24 -04'00'</small>	09/12/2023
<b>Academic Dean Name</b>	Gerarda M. Shields	
<b>Academic Dean Signature and Date</b>	Gerarda M. Shields <small>Digitally signed by Gerarda M. Shields Date: 2023.09.14 17:00:20 -04'00'</small>	
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body).	In this one-semester, two-credit capstone course, students identify and address a cybersecurity issue, with a focus on research, system design, and hands-on implementation. Prioritizing teamwork, teams submit a project proposal in the first half of the semester and conclude with a system demonstration. They will also provide a written report and deliver an oral presentation by the end of the semester.	
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	The final core curriculum course in the new CST Bachelor of Science program in Cybersecurity. Given the evolving nature of cybersecurity-related threats and the growing need for robust digital defenses, hands-on, project-based learning is essential. This course allows students to synthesize and apply their accumulated academic and practical knowledge in a real-world context. It also sharpens students' problem-solving, teamwork, and communication skills, which are vital in the collaborative field of cybersecurity. The course is crucial for bridging the gap between academic learning and practical application, ensuring graduates are industry-ready and equipped to address the dynamic challenges of the cybersecurity world when working in groups and facing novel challenges.	
<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	New proposal.	

## All Proposal Check List

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	N/A
Documentation of Advisory Commission views (if applicable).	N/A
Completed <a href="#">Chancellor's Report Form</a> .	X

## EXISTING PROGRAM MODIFICATION PROPOSALS

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	N/A

**NEW COURSE PROPOSAL FORM**

<b>Course Title</b>	<b>Capstone Cybersecurity Course</b>
<b>Proposal Date</b>	September 12, 2023
<b>Proposer's Name</b>	Janusz Kusyk
<b>Course Number</b>	CST 4916
<b>Course Credits, Hours</b>	2 credits, 1 class hours, 2 lab hours
<b>Course Pre / Co-Requisites</b>	Two CST 35xx and One 36xx Level and Dept Permission
<b>Catalog Course Description</b>	A one-semester capstone course featuring research into a cybersecurity problem, and design and implementation of a solution to it. Topics include identification of a problem, background research, cybersecurity system design, and solution implementation. Work in teams to demonstrate mastery of modern cybersecurity concepts and technologies as well as teamwork, problem-solving, critical thinking, and communication skills. A project proposal, including a problem outline and the solution design, must be completed during the first half of the semester and a hands-on implementation of cybersecurity system completed in the second part of the semester. Each team will be required to write a report and to make an oral presentation to the class.
<b>Brief Rationale</b> Provide a concise summary of why this course is important to the department, school or college.	The capstone course is the final core curriculum course in the new CST Bachelor of Science program in Cybersecurity. Given the evolving nature of cybersecurity-related threats and the growing need for robust digital defenses, hands-on, project-based learning is essential. This course allows students to synthesize and apply their accumulated academic and practical knowledge in a real-world context. It also sharpens students' problem-solving, teamwork, and communication skills, which are vital in the collaborative field of cybersecurity. The course is crucial for bridging the gap between academic learning and practical application, ensuring graduates are industry-ready and equipped to address the dynamic challenges of the cybersecurity world, especially when working in groups and facing new challenges.
<b>CUNY – Course Equivalencies</b> Provide information about equivalent courses within CUNY, if any.	N/A
<b>Intent to Submit as Common Core</b> If this course is intended to fulfill one of the requirements in the common core, then indicate which area.	N/A
<b>For Interdisciplinary Courses:</b>	N/A



- Date submitted to ID Committee for review	N/A
- Date ID recommendation received	N/A
- Will all sections be offered as ID? Y/N	
<b>Intent to Submit as a Writing Intensive Course</b>	Yes

## NEW COURSE PROPOSAL CHECK LIST

<b>Completed NEW COURSE PROPOSAL FORM</b>	
• Title, Number, Credits, Hours, Catalog course description	X
• Brief Rationale	X
• CUNY – Course Equivalencies	X
Completed <a href="#">Library Resources and Information Literacy Form</a>	
<b>Course Outline</b> Include within the outline the following.	
Hours and Credits for Lecture and Labs If hours exceed mandated Carnegie Hours, then rationale for this	X
Prerequisites/Co- requisites	X
Detailed Course Description	
Course Specific Learning Outcome and Assessment Tables • Discipline Specific • General Education Specific Learning Outcome and Assessment Tables	X
Example Weekly Course outline	X
Grade Policy and Procedure	X
Recommended Instructional Materials (Textbooks, lab supplies, etc.)	X
Library resources and bibliography	X
<b>Course Need Assessment.</b> Describe the need for this course. Include in your statement the following information.	
Target Students who will take this course. Which programs or departments, and how many anticipated? Documentation of student views (if applicable, e.g. non-required elective).	X
Projected headcounts (fall/spring and day/evening) for each new or modified course.	X
If additional physical resources are required (new space, modifications, equipment), description of these requirements. If applicable, Memo or email from the VP for Finance and Administration with written comments regarding additional and/or new facilities, renovations or construction.	X
Where does this course overlap with other courses, both within and outside of the department?	X
Does the Department currently have full time faculty qualified to teach this course? If not, then what plans are there to cover this?	X
If needs assessment states that this course is required by an accrediting body, then provide documentation indicating that need.	N/A
<b>Course Design</b> Describe how this course is designed.	

Course Context (e.g. required, elective, capstone)	X
Course Structure: how the course will be offered (e.g. lecture, seminar, tutorial, fieldtrip)?	X
Anticipated pedagogical strategies and instructional design (e.g. Group Work, Case Study, Team Project, Lecture)	X
How does this course support Programmatic Learning Outcomes?	X
Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.	X
<b>Additional Forms for Specific Course Categories</b>	
<a href="#">Interdisciplinary Form</a> (if applicable)	N/A
Interdisciplinary Committee Recommendation (if applicable and if received)* *Recommendation must be received before consideration by full Curriculum Committee	N/A
<a href="#">Common Core (Liberal Arts) Intent to Submit</a> (if applicable)	N/A
Writing Intensive Form if course is intended to be a WIC (under development)	X
If course originated as an experimental course, then results of evaluation plan as developed with director of assessment.	N/A
<b>(Additional materials for Curricular Experiments)</b>	
Plan and process for evaluation developed in consultation with the director of assessment. (Contact Director of Assessment for more information).	N/A
Established Timeline for Curricular Experiment	N/A

## LIBRARY RESOURCES & INFORMATION LITERACY: MAJOR CURRICULUM MODIFICATION

Please complete for **all** major curriculum modifications. This information will assist the library in planning for new courses/programs.

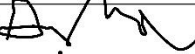
Consult with your library faculty subject specialist (<http://cityte.ch/dir>) **3 weeks before the proposal deadline**.

**Course proposer:** please complete boxes 1-4. **Library faculty subject specialist:** please complete box 5.

- |   |   |
|---|---|
| <b>1 Title of proposal</b><br>CST 4916 – Capstone Course  | <b>Department/Program</b><br>Computer Systems Technology / BS in Cybersecurity              |
| <b>Proposed by</b> (include email & phone)<br>Dr. Janusz Kusk<br><a href="mailto:jkusk@citytech.cuny.edu">jkusk@citytech.cuny.edu</a><br>718-260-5164 | <b>Expected date course(s) will be offered</b><br>Fall 2024<br><br><b># of students:</b> 15 |
- 2 The library cannot purchase reserve textbooks for every course at the college, nor copies for all students. Consult our website (<http://cityte.ch/curriculum>) for articles and eBooks for your courses, or our open educational resources (OER) guide (<http://cityte.ch/oer>). Have you considered using a freely-available OER or an open textbook in this course?**
- Yes, this course will also use some of the freely available OER or resources as partial selective readings.
- 3 Beyond the required course materials, are City Tech library resources sufficient for course assignments? If additional resources are needed, please provide format details (e.g. eBook, journal, DVD, etc.), full citation (author, title, publisher, edition, date), price, and product link.**
- Yes, City Tech Library resources are sufficient for the proposed course assignments because the main readings for the course are a required textbook and journal articles that will be assigned by instructor. Students should be able to locate the selected journal articles in library.
- 4 Library faculty focus on strengthening students' information literacy skills in finding, critically evaluating, and ethically using information. We collaborate on developing**

**assignments and customized instruction and research guides. When this course is offered, how do you plan to consult with the library faculty subject specialist for your area? Please elaborate.**

I will reach out to the library subject specialist via email to arrange an information session in which the library subject specialist can present to the students of this course, the use of library databases, citation convention and discuss copyright issues.

- 5 Library Faculty Subject Specialist Anne Leonard for Prof. Junior Tidal** 
- Comments and Recommendations:** Collaborating with the instructor, and couse coordinator and chair as needed, to plan an information literacy session to support students' research in the course will be a priority, since students identify a relevant issue for a significant research project. Supporting students' discipline-specific information literacy is important to career readiness.

**Date** 9/25/2023

## **Course Overview & Rationale**

With the surge in digital proliferation and the increasing sophistication of cyber threats, there is a need for professionals who are not only technically savvy but also practically prepared to confront real-world cybersecurity challenges. This capstone course offers students a holistic approach by intertwining theory in cybersecurity with its proactive implementation. It allows students to apply their accumulated academic and practical knowledge to solve relevant tasks. Beyond technical skills in cybersecurity, the course emphasizes critical thinking, effective communication, and teamwork, hence all essential skills for a successful cybersecurity career. Upon completion of this course, students will be well-versed in both the conceptual and practical facets of cybersecurity.

This Capstone Cybersecurity Course is for students who are already well-versed in the key concepts of cybersecurity threats and countermeasures but need to learn how to extend and apply their knowledge to a topic of their interest. This course teaches students to identify and assess cyber vulnerabilities and to apply best practices to secure computer systems. Additionally, it provides students with a deeper appreciation of the role of a cybersecurity specialist in the modern world, helping them understand the expectations and functions of such specialists in various company settings. Students will also gain experience working in teams, as is typical in an enterprise environment.

The Capstone Cybersecurity Course is vital for bridging the gap between academic learning and practical application, ensuring graduates are industry-ready and properly equipped to address the dynamic challenges of the cybersecurity world, especially when working in groups and facing previously unknown challenges. This course is the final core curriculum offering in the new Bachelor of Science program in Cybersecurity, provided by the Computer Systems Technology department at New York City College of Technology.

## **Couse Outline**

**New York City College of Technology/CUNY  
Computer Systems Technology Department**

### **CST 4916 – Capstone Cybersecurity Course**

2 credits

1 lecture hour, 2 lab hours

#### **Course Description:**

This is a one-semester capstone course. Students will be required to research a cybersecurity problem and design and implement a solution to it. Topics include identification of a problem, background research, cybersecurity system design and implementation of a solution for the problem. The students will work in teams to demonstrate mastery of modern cybersecurity concepts and technologies as well as teamwork, problem-solving, critical thinking, and communication skills. A project proposal, including a problem outline and the solution design, must be completed during the first half of the semester and a hands-on implementation of cybersecurity system is to be completed in the second part of the semester. Each team will be required to write a report and to make an oral presentation to the class, with each student taking parts in these activities.

#### **Course Prerequisites:**

Two CST 35xx and one CST 36xx level and Dept. permission.

#### **Progression Requirements:**

Students majoring in CST must earn a “C” or better grade in this course.

#### **Required Textbook:**

No particular textbook is required for this course. However, students may be asked to read and reference academic publications, technical documentations, and other materials relevant to their project.

#### **Course Objectives:**

This course teaches students how to identify and assess cyber vulnerabilities and apply the best practices to secure computer systems. This course also equips students with a better appreciation of the role of a cybersecurity specialist in our modern world, enabling them to understand the expectations and functions of such a cybersecurity specialist in different company settings. Students will experience working in a team, which is typical in an enterprise environment. This is a designated writing intensive course that will include writing a project proposal, project report and a project presentation.

#### **Course Format:**

The course will be delivered through a combination of lectures, discussions and hands-on activities. Students will work in teams to develop a project proposal to be approved by a course instructor. Each team will work on its project throughout the semester under the

guidance of the course instructor. Each team will have regular meeting with the course instructor to ensure progress of the project. The course will culminate with a final project presentation.

### **Learning Outcomes:**

1. Apply principles of science, mathematics, and technology to solve complex cybersecurity problems.
2. Ability to break down a complex cybersecurity problem into components that can be addressed by known cybersecurity tools.
3. Ability to create a solution strategy for a complex cybersecurity problem based on information about the problem.
4. Ability to delineate the scope of the solution strategy and ability to execute the strategy to solve a cybersecurity problem.

### **General Education Learning Outcomes:**

1. Demonstrate the ability to work collaboratively and independently on assignments in and outside a classroom setting.
2. Understand and employ both quantitative and qualitative analysis to solve problems.
3. Develop and demonstrate reading, writing competencies, and listening skills.
4. Work with teams. Build consensus. Use creativity.

### **Grade Requirement:**

Students must participate in team meetings, both with and without the course instructor, and in project development.

### **Course Grading Formula:**

Project proposal	10%
Implementation and testing	30%
Midterm project report	10%
Final project report	20%
Project presentation	10%
Participation in project development and team meetings	20%

---

Total: 100%

### **Grading Policy:**

<b>Letter Grade</b>	<b>A</b>	<b>A-</b>	<b>B+</b>	<b>B</b>	<b>B-</b>	<b>C+</b>	<b>C</b>	<b>D</b>	<b>F</b>
<b>Numeric Grade</b>	100-93	92.9-90	89.9-87	86.9-83	82.9-80	79.9-77	76.9-70	69.9-60	59-0

### **Accessibility Statement:**

Accessibility Statement City Tech is committed to supporting the educational goals of enrolled students with disabilities in the areas of enrollment, academic advisement, tutoring,



assistive technologies, and testing accommodations. If you have or think you may have a disability, you may be eligible for reasonable accommodations or academic adjustments as provided under applicable federal, state, and/or city laws. You may also request services for temporary conditions or medical issues under certain circumstances. If you have questions about your eligibility and/or would like to seek accommodation services and/or academic adjustments, please contact the Student Accessibility Center (SAC) at 300 Jay Street. Room L-237; telephone: 718-260-5143; WWW: <http://www.citytech.cuny.edu/accessibility/>.

### **Diversity and Inclusive Education Syllabus Statement:**

This course welcomes students from all backgrounds, experiences and perspectives. In accordance with the City Tech and CUNY missions, this course intends to provide an atmosphere of inclusion, respect, and the mutual appreciation of differences so that together we can create an environment in which all students can flourish. It is the instructor's goal to provide materials and activities that are welcoming and accommodating of diversity in all of its forms, including race, gender identity and presentation, ethnicity, national origin, religion, cultural identity, socioeconomic background, sexuality and sexual orientation, ability, neurodivergence, age, and etc. Your instructor is committed to equity and actively seeks ways to challenge institutional racism, sexism, ableism and other forms of prejudice. Your input is encouraged and appreciated. If a dynamic that you observe or experience in the course concerns you, you may respectfully inform your instructor without fear of how your concerns will affect your grade. Let your instructor know how to improve the effectiveness of the course for you personally, or for other students or student groups. We acknowledge that NYCCT is located on the traditional homelands of the Canarsie and Lenape peoples.

### **New York City College of Technology Policy on Academic Integrity:**

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using, crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. The complete text of the College policy on Academic Integrity may be found in the catalog.

New York City College of Technology, like all academic institutions, encourages and thrives on the open exchange of ideas. At City Tech, we expect everyone to conduct their intellectual work with honesty and integrity. With this goal in mind, and in response to the Report of the CUNY Committee on Academic Integrity (<http://web.cuny.edu/academics/info-central/policies/academic-integrity-report.pdf>) the NYCCT College Council approved a new academic integrity policy in May 2007. City Tech's academic integrity policy aims to deter academic dishonesty by students and allow the college to process cases of academic dishonesty more effectively. This policy has been in effect as of August 27, 2008.

**Course Schedule:**

<b>Week</b>	<b>Topics</b>
<b>1</b>	Introduction to Capstone Cybersecurity Course and Team Formation
	Overview of the capstone course
	Team formation and project selection
<b>2</b>	Project Planning Scope, and Requirements
	Identify the scope of the project
	Prepare a project plan and schedule
	Identify the requirements of the project
<b>3 - 6</b>	Project Design
	Identify cybersecurity measures to be explored
	Start developing the project
<b>7</b>	Revise an initial project scope, and requirements if needed
	Midterm project report
<b>8 - 13</b>	Project Implementation
	Implement cybersecurity tools, protocols and countermeasures
<b>12 - 13</b>	Test and validate cybersecurity measures
	Identify potential issues and problems, if any
	Identify potential limitations in meeting requirements, if any
	Asses effectiveness of the cybersecurity measures
<b>14</b>	Project Deliverables
	Finalize project report
	Prepare project presentation
<b>15</b>	Project Presentation and Report submission

**Course Assessment:**

<b>Course-specific outcomes</b>	<b>Assessment methods</b>
1. Apply principles of science, mathematics, and technology to solve complex cybersecurity problems.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Midterm project report</li> <li>• Final project report</li> </ul>
2. Ability to break down a complex cybersecurity problem into components that can be addressed by known cybersecurity tools.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Project proposal</li> <li>• Midterm project report</li> <li>• Final project report</li> </ul>
3. Ability to create a solution strategy for a complex cybersecurity problem based on information about the problem.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Project proposal</li> <li>• Midterm project report</li> <li>• Final project report</li> <li>• Project presentation</li> </ul>
4. Ability to delineate the scope of the solution strategy and ability to execute the strategy to solve a cybersecurity problem	

General Education Learning Outcomes	Assessment Methods
1. Demonstrate the ability to work collaboratively and independently on assignments in and outside a classroom setting.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Final project report</li> <li>• Project presentation</li> </ul>
2. Understand and employ both quantitative and qualitative analysis to solve problems.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Final project report</li> </ul>
3. Develop reading, writing competencies, and listening skills.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Final project report</li> </ul>
5. Work with teams. Build consensus. Use creativity.	<ul style="list-style-type: none"> <li>• Team meetings</li> <li>• Project participation</li> <li>• Project presentation</li> <li>• Final project report</li> </ul>

## **Course Need Assessment**

**Students who would take this class:** students who intend to major in Cybersecurity.

**Department:** Computer Systems Technology

**Program:** Bachelors in Cybersecurity

**The number of section (s) anticipated:** one to two sections for the first year

**Projected headcount:** 15 students per section

**Physical Resources required:** Basic smart room set-up: a screen, and an overhead projector/a TV set that is run by and connected to a computer.

**Course overlap:** None

**Faculty qualified for teaching this course:** Yes, there are faculty members who have doctoral degrees in Computer Science with the concentration in Information Security for various domains.

## **Course Design**

**Course context:** This course will be required of Cybersecurity major students. Students must participate in team meetings, both with and without the course instructor, and in project development and presentation.

**Course structure:** This course will be offered in a lecture style/format.

**Anticipated Pedagogical Strategies and Instructional Design:** This class will be run in a lecture-activity style/format. The class will start with a lecture, and involve the in-class activities, such as group discussion, hands-on exercises and hands-on implementations using available cybersecurity tools.

**Providing Support to Programmatic Learning Outcomes:** This course requires satisfactory completion of (i) project proposal, (ii) implementation and testing, (iii) midterm project report (iv) final project report, (v) project presentation and (vi) active participation in project development and team meetings.

**Is this course designed to be partially or fully online? If so, describe how this benefits students and/or program.** Not fully online, all in-person or can be hybrid (with students working in groups on developing their solutions)

## CHANCELLOR'S REPORT FORM

### ***NEW COURSE PROPOSAL: "Capstone Cybersecurity Course "***

<b>Department(s)</b>	Computer Systems Technology
<b>Academic Level</b>	<input checked="" type="checkbox"/> Regular <input type="checkbox"/> Compensatory <input type="checkbox"/> Developmental <input type="checkbox"/> Remedial
<b>Subject Area</b>	Cybersecurity
<b>Course Prefix</b>	CST
<b>Course No.</b>	4916
<b>Course Title</b>	Capstone Cybersecurity Course
<b>Catalog Description</b>	A one-semester capstone course featuring research into a cybersecurity problem, and design and implementation of a solution to it. Topics include identification of a problem, background research, cybersecurity system design, and solution implementation. Work in teams to demonstrate mastery of modern cybersecurity concepts and technologies as well as teamwork, problem-solving, critical thinking, and communication skills. A project proposal, including a problem outline and the solution design, must be completed during the first half of the semester and a hands-on implementation of cybersecurity system completed in the second part of the semester. Each team will be required to write a report and to make an oral presentation to the class.
<b>Prerequisites</b>	Two CST 3500 and One 3600 Level and Dept Permission.
<b>Credits</b>	2
<b>Contact Hours</b>	3 (1 lecture and 2 lab hours)
<b>Liberal Arts</b>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>Course Attribute</b>	Writing intensive course
<b>Course Applicability</b>	<input checked="" type="checkbox"/> Major <input type="checkbox"/> Gen Ed Required <input type="checkbox"/> Gen Ed - Flexible <input type="checkbox"/> Gen Ed - College Option <input type="checkbox"/> English Composition <input type="checkbox"/> World Cultures <input type="checkbox"/> Speech <input type="checkbox"/> Mathematics <input type="checkbox"/> US Experience in its Diversity <input type="checkbox"/> Interdisciplinary <input type="checkbox"/> Science <input type="checkbox"/> Creative Expression <input type="checkbox"/> Advanced Liberal Arts <input type="checkbox"/> Individual and Society <input type="checkbox"/> Scientific World
<b>Effective Term</b>	Fall 2024

## **Rationale**

With the surge in digital proliferation and the increasing sophistication of cyber threats, there is a need for professionals who are not only technically savvy but also practically prepared to confront real-world cybersecurity challenges. This capstone course offers students a holistic approach by intertwining theory in cybersecurity with its proactive implementation. It allows students to apply their accumulated academic and practical knowledge to solve relevant tasks. Beyond technical skills in cybersecurity, the course emphasizes critical thinking, effective communication, and teamwork, hence all essential skills for a successful cybersecurity career. Upon completion of this course, students will be well-versed in both the conceptual and practical facets of cybersecurity.

This Capstone Cybersecurity Course is for students who are already well-versed in the key concepts of cybersecurity threats and countermeasures but need to learn how to extend and apply their knowledge to a topic of their interest. This course teaches students to identify and assess cyber vulnerabilities and to apply best practices to secure computer systems. Additionally, it provides students with a deeper appreciation of the role of a cybersecurity specialist in the modern world, helping them understand the expectations and functions of such specialists in various company settings. Students will also gain experience working in teams, as is typical in an enterprise environment.

The Capstone Cybersecurity Course is vital for bridging the gap between academic learning and practical application, ensuring graduates are industry-ready and properly equipped to address the dynamic challenges of the cybersecurity world, especially when working in groups and facing previously unknown challenges. This course is the final core curriculum offering in the new Bachelor of Science program in Cybersecurity, provided by the Computer Systems Technology department at New York City College of Technology.

## 9.6 Proposal to Change Prerequisites: CST 2410 – Introduction to Computer Security

New York City College of Technology, CUNY	
<b>CURRICULUM MODIFICATION PROPOSAL FORM</b>	
<b>Title of Proposal</b>	<b>Modification of Course Title and Prerequisite for CST 2410</b>
<b>Date</b>	09/11/2023
<b>Major or Minor</b>	Minor
<b>Proposer's Name</b>	Dr. Yu-Wen Chen
<b>Department</b>	Computer Systems Technology
<b>Date of Departmental Meeting in which proposal was approved</b>	03/17/2023
<b>Department Chair Name</b>	Ashwin Satyanarayana
<b>Department Chair Signature and Date</b>	<div> <div>Ashwin Satyanarayana</div> <div> Digitally signed by Ashwin Satyanarayana  Date: 2023.09.12 10:41:47 -04'00' </div> </div> <div>09/12/2023</div>
<b>Academic Dean Name</b>	Gerarda M. Shields
<b>Academic Dean Signature and Date</b>	<div> <div>Gerarda M. Shields</div> <div> Digitally signed by Gerarda M. Shields  Date: 2023.09.14 17:00:44 -04'00' </div> </div>
<b>Brief Description of Proposal</b> (Describe the modifications contained within this proposal in a succinct summary. More detailed content will be provided in the proposal body.)	A change of prerequisite from CST 2307 to corequisite or prerequisite "CST2307"
<b>Brief Rationale for Proposal</b> (Provide a concise summary of why this proposed change is important to the department. More detailed content will be provided in the proposal body).	<p>This change aims to accommodate students in the proposed Cybersecurity program, allowing them to take CST 2410: Introduction to Computer Security either concurrently with or after CST 2307: Networking Fundamentals. The subjects covered in CST1215: Operating System Fundamentals, a prerequisite for CST 2307, provide a robust intellectual foundation that equips students well to fully grasp the concepts in CST 2410. Consequently, enrolling in CST 2410 alongside or after CST 2307 offers students flexibility in planning their academic schedules without hindering their comprehension of CST 2410's content. Notably, all CST students, including those pursuing AAS and BTech majors, will gain from these modifications to CST 2410. These revisions are also prompted by the latest developments in computer and network security and the goal of avoiding redundancy within the program's primary courses.</p>

<b>Proposal History</b> (Please provide history of this proposal: is this a resubmission? An updated version? This may most easily be expressed as a list).	This is a new submission
--	--------------------------

### ALL PROPOSAL CHECK LIST

Completed CURRICULUM MODIFICATION FORM including:	
• Brief description of proposal	X
• Rationale for proposal	X
• Date of department meeting approving the modification	X
• Chair's Signature	X
• Dean's Signature	X
Evidence of consultation with affected departments List of the programs that use this course as required or elective, and courses that use this as a prerequisite.	N/A
Documentation of Advisory Commission views (if applicable).	N/A
Completed <a href="#">Chancellor's Report Form</a> .	X

### EXISTING PROGRAM MODIFICATION PROPOSALS

Documentation indicating core curriculum requirements have been met for new programs/options or program changes.	N/A
Detailed rationale for each modification (this includes minor modifications)	X



## CHANCELLOR'S REPORT FORM

### Section AV: Changes in Existing Courses

#### AV.1. CST2410 Introduction to Computer Security

Effective term: Fall 2024

From		To	
Course Subject & Number	CST2410	Course Subject & Number	CST2410
Course Name	Introduction to Computer Security	Course Name	Introduction to Computer Security
Prerequisite	<del>CST2307</del>	Co-requisite or Prerequisite	CST 2307
Corequisite		Corequisite	
Credits	3	Credits	3
Hours	4	Hours	4
Rationale	<p>This change aims to accommodate students in the proposed Cybersecurity program, allowing them to take CST 2410: Introduction to Computer Security either concurrently with or after CST 2307: Networking Fundamentals. The subjects covered in CST1215: Operating System Fundamentals, a prerequisite for CST 2307, provide a robust intellectual foundation that prepares students well to fully grasp the concepts in CST 2410. Consequently, enrolling in CST 2410 alongside or after CST 2307 offers students flexibility in planning their academic schedules without hindering their comprehension of CST 2410's content. Notably, all CST students, including those pursuing AAS and BTech majors, will gain from these modifications to CST 2410. These revisions are also prompted by the latest developments in computer and network security and the goal of avoiding redundancy within the program's primary courses.</p>		

# Appendix A: Letters of Support

## 1. NUY Tandon School of Engineering



**NYU**

**TANDON SCHOOL  
OF ENGINEERING**

**Tandon School of Engineering**  
1 MetroTech Center  
Brooklyn, NY 11201  
646-997-3600  
[engineering.nyu.edu](http://engineering.nyu.edu)

September 8, 2023

To:

Computer Systems Technology Department  
New York City College of Technology  
City University of New York  
300 Jay Street, Brooklyn, NY 11201

Dear Sir/Madam,

I am writing to express my support for your plans to develop a new Bachelor of Science degree program in the field of Cybersecurity.

I was given the opportunity to review the proposed curriculum. I am comfortable that as proposed it represents a balanced program that can adequately prepare graduates to enter the cybersecurity industry. I am particularly pleased that it covers various courses in cybersecurity at the appropriate level for undergraduates.

There is a high demand for cybersecurity trained individuals and the industry needs qualified candidates with a solid understanding of basic concepts. This degree program will prepare them with the knowledge and tools used in the cybersecurity industry and will also prepare them to undertake graduate level work in cybersecurity.

Your proposed program should help address the gap, and I deem it will be beneficial both to your students and to the industry.

Please do not hesitate to contact me if you need any further discussion.

Sincerely,

Joel Caminer

Senior Director, NYU Center for Cybersecurity  
370 Jay St, Brooklyn, NY 11201

E-mail: [joel.caminer@nyu.edu](mailto:joel.caminer@nyu.edu) | Office: 646-997-3351

Leading invention, innovation and entrepreneurship

## 2. CUNY - Queensborough Community College



### DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

September 6, 2023

**Computer Systems Technology Department**

New York City College of Technology  
City University of New York  
300 Jay Street,  
Brooklyn, NY 11201

Dear Sir/Madam,

I am writing to express my support for your plans to develop a new Bachelor of Science degree program in the field of Cybersecurity.

I was given the opportunity to review the proposed curriculum. I am comfortable that as proposed it represents a balanced program that can adequately prepare graduates to enter the cybersecurity industry. I am particularly pleased that it covers various courses in cybersecurity at the appropriate level for undergraduates.

There is a high demand for cybersecurity trained individuals and the industry needs qualified candidates with a solid understanding of basic concepts. This degree program will prepare them with the knowledge and tools used in the cybersecurity industry and will also prepare them to undertake graduate level work in cybersecurity.

Your proposed program should help address the gap, and I deem it will be beneficial both to your students and to the industry.

Please do not hesitate to contact me if you need any further discussion.

Sincerely,

A handwritten signature in black ink that reads 'Haishen Yao'.

Haishen Yao, Ph.D  
Professor and Chairperson  
CUNY QCC Math and CS

718-631-6361  
FAX 718-631-6290  
Science, Room 245  
222-05 56<sup>th</sup> Avenue  
Bayside, NY 11364-1497

ONE COMMUNITY. INFINITE POSSIBILITIES.

### 3. KnowBe4 Security Awareness and Training Solutions



September 8, 2023

Computer Systems Technology Department  
New York City College of Technology  
City University of New York  
300 Jay Street,  
Brooklyn, NY 11201

Dear Sir/Madam,

I am a 35-year career cybersecurity practitioner and author of 13 books and over 1300 articles on computer security. I am writing to express my support for your plans to develop a new Bachelor of Science degree program in the field of Cybersecurity.

I was given the opportunity to review the proposed curriculum. I am comfortable that as proposed, it represents a balanced program that can adequately prepare graduates to enter the cybersecurity industry. I am particularly pleased that it covers various courses in cybersecurity at the appropriate level for undergraduates.

There is a high demand for cybersecurity-trained individuals and the industry needs qualified candidates with a solid understanding of basic concepts. This degree program will prepare them with the knowledge and tools used in the cybersecurity industry and will also prepare them to undertake graduate-level work in cybersecurity.

Your proposed program should help address the gap, and I deem it will be beneficial both to your students and to the industry.

Please do not hesitate to contact me if you need any further discussion.

Sincerely,

A handwritten signature in blue ink, appearing to read "Roger A. Grimes". The signature is fluid and cursive, with the first name "Roger" and last name "Grimes" clearly distinguishable.

Roger A. Grimes  
Data-Driven Defense Evangelist  
KnowBe4, Inc.  
33 N. Garden Avenue, Suite 1200  
Clearwater, FL 33755  
E: rogerg@knowbe4.com.

#### 4. KnowBe4 Security Awareness and Training Solutions



September 20, 2023

To,  
Computer Systems Technology Department  
New York City College of Technology  
City University of New York  
300 Jay Street,  
Brooklyn, NY 11201

Dear Sir/Madam,

I am writing to express my support for your plans to develop a new Bachelor of Science degree program in the field of Cybersecurity.

I was given the opportunity to review the proposed curriculum. I am comfortable that as proposed it represents a balanced program that can adequately prepare graduates to enter the cybersecurity industry. I am particularly pleased that it covers various courses in cybersecurity at the appropriate level for undergraduates.

There is a high demand for cybersecurity trained individuals and the industry needs qualified candidates with a solid understanding of basic concepts. This degree program will prepare them with the knowledge and tools used in the cybersecurity industry and will also prepare them to undertake graduate level work in cybersecurity.

Your proposed program should help address the gap, and I deem it will be beneficial both to your students and to the industry.

Please do not hesitate to contact me if you need any further discussion.

Sincerely,  
Stu Sjouerman  
CEO, KnowBe4

KnowBe4, Inc. | 33 N Garden Ave | Suite 1200 | Clearwater, Florida 33755  
HR@KnowBe4.com | www.KnowBe4.com | 855-566-9234

5. CUNY - John Jay College of Criminal Justice



Shweta Jain  
Professor  
Graduate Program Director  
Department Chair  
Mathematics and Computer Science  
John Jay College of Criminal Justice  
email: [sjain@jjay.cuny.edu](mailto:sjain@jjay.cuny.edu)

September 14, 2023

To:

Computer Systems Technology Department  
New York City College of Technology  
City University of New York  
300 Jay Street,  
Brooklyn, NY 11201

RE: Letter of support for New York City College of Technology's new BS degree program

Dear Sir/Madam

I am writing to express my support for your plans to develop a new Bachelor of Science degree program in the field of Cybersecurity.

I was given the opportunity to review the proposed curriculum. I am comfortable that as proposed it represents a balanced program that can adequately prepare graduates to enter the cybersecurity industry. I am particularly pleased that it covers various courses in cybersecurity at the appropriate level for undergraduates.

There is a high demand for cybersecurity trained individuals and the industry needs qualified candidates with a solid understanding of basic concepts. This degree program will prepare them with the knowledge and tools used in the cybersecurity industry and will also prepare them to undertake graduate level work in cybersecurity.

Your proposed program should help address the gap, and I deem it will be beneficial both to your students and to the industry.

Please do not hesitate to contact me if you need any further discussion.

Sincerely

A handwritten signature in black ink, appearing to read "Shweta Jain", with a stylized flourish at the end.

Shweta Jain

## Appendix B: Sample Job Postings

### Cybersecurity Analyst Levels 1-7 (Threat Hunting and Automation)



Metropolitan Transportation Authority  
New York, NY

#### Job description

DEPT/DIV: MTA Information Technology/ Office of IT Cyber Security Services

SUPERVISOR: Cyber Security Office Manager

LOCATION: 2 Broadway, New York, NY 10004

HOURS OF WORK: 9:00am-530pm (7.5 hours/day) or as required.

<https://tinyurl.com/3v4hna3f>

The purpose of this position is to provide critical technical expertise in threat hunting and automation functions. Cybersecurity Analyst will be tasked with remaining up to date on the latest risks and threats to the MTA as the threat landscape gradually evolves. This position will work in conjunction with the MTA's SOC, MSSP, and other cybersecurity partners to perform effective threat hunting and anticipation. Upon developing effective threat hunting enterprise searches, the analyst must also assist in creating content detection / prevention rules. The analyst is part of a Tier 3 SOC function and must be able to create searches with high fidelity and minimize/negate potential false-positives. This position will also work in conjunction with several SOAR administrators to streamline and automate tasks as they pertain to Threat Intelligence & Incident Response.

## Cybersecurity Engineer Levels 1-7 (Privileged Access Strategist)



Metropolitan Transportation Authority  
New York, NY

DEPT/DIV: MTA IT/ Office of IT Cyber Security Services  
SUPERVISOR: Director, Identity and Access Management  
LOCATION: 2 Broadway, New York, NY 10004  
HOURS OF WORK: 9:00am – 8:30am (7.5hrs)

This position is eligible for telework. New Hires are eligible to apply 30 days after their effective date of hire.

<https://tinyurl.com/mr246tcw>

The purpose of this position is to provide critical technical expertise in managing and analyzing cybersecurity risks. The Privileged Access Strategist will play a crucial role in the organization, focusing on improving the overall user journey across all areas of Identity and Access Management (IAM), including Access Management (AM), Identity Governance and Administration (IGA), and Privileged Access Management (PAM). This role involves the deployment and management of robust PAM controls as a core component of IAM across various use cases, such as system administration access, machine-to-machine connectivity, automation, and cloud infrastructure. A key objective is to strike a balance between enhancing cybersecurity defense, achieving regulatory compliance, and enabling business processes. The role will require the strategist to tailor PAM deployment for each coverage area, introducing user segmentation, and adapting controls for different user groups, while also deciding on the capabilities and deployment model, and determining necessary integrations with adjacent security or service management tools. This position is instrumental in driving zero standing privileged access and promoting a safe, structured, and orderly environment.



## Information Security Analyst (Entry Level - College Grads)



Millennium Soft Inc  
Franklin Lakes, NJ

<https://tinyurl.com/2489ts63>

### Job description

Position: Information Security Analyst [Entry Level – College Grads]

Location: Franklin Lakes, NJ [Office and remote locations]

Description To improve the security of products and solutions by design, in use and through partnership. This role will focus on Integrated Supply Chain and Manufacturing Operational Technology (OT). This entry level person should have a technical understanding of enterprise IT and OT environments. They should have experience investigating complex technical security incidents. You will leverage a broad array of investigative information, including log data, to identify and investigate potential security incidents.

## Cyber Security Analyst (CyberArk)



PSEG

Newark, NJ

<https://tinyurl.com/bdd7f98k>

**Job Summary** This position is an experienced, senior level, hands-on technical lead, performing privileged access management (PAM) security functions and PAM maintaining systems, while providing technical guidance to the team. Manages PAM technologies, as well as PAM security policies and procedures, and incident response as needed. Provides technical expertise and support IT management and staff in cybersecurity threat risk assessments, development, testing and the implementation and operation of appropriate information security plans, procedures, and control techniques designed to prevent, minimize, or quickly recover from cyber-attacks or other serious events.

# Appendix C: Draft Articulation Agreements

**THE CITY UNIVERSITY OF NEW YORK  
ARTICULATION AGREEMENT (Draft)  
between  
NYC COLLEGE OF TECHNOLOGY  
and  
QUEENSBOROUGH COMMUNITY COLLEGE**

## A. SENDING AND RECEIVING INSTITUTIONS

Sending College: Queensborough Community College (QCC)

Department: Engineering Technology

Program: Cybersecurity

Degree: Associate in Applied Science (AAS)

Receiving College: New York City College of Technology (NYCCT)

Department: Computer Systems Technology

Program: Cybersecurity

Degree: Bachelor of Science (BS)

## B. ADMISSION REQUIREMENTS FOR SENIOR COLLEGE PROGRAM

- The AAS degree and a minimum GPA of 2.50
- Grade of C or higher in credit-bearing major courses
- Grade of C or higher in freshman composition, its equivalent, or a higher-level English course

Students who earn an AAS in Cybersecurity program at QCC will be accepted into the BS in Cybersecurity under the requirements in effect at the time of admission. To earn a baccalaureate degree, admitted students must earn a minimum of 60 credits of which 34 credits must be taken in residence and 17 in the major.

Students who wish to transfer but do not meet all the above requirements or are unable to enroll within two years after graduation will receive admission consideration under our standard transfer credit policies.

Total transfer credits granted toward the Bachelor of Science: 60

Total additional credits required at NYCCT to complete Bachelor of Science: 60

Total credits required for the Bachelor of Science in Cybersecurity: 120

## C. REQUIREMENTS OF QCC AS IN CYBERSECURITY DEGREE TRANSFER CREDITS AWARDED

QCC graduates who complete the Associate in Applied Science degree (AAS) in Cybersecurity will receive -- credits toward the Bachelor of Science (BS) degree in Cybersecurity at NYCCT.

<b>QCC Associate in Applied Science in Cybersecurity Degree Requirements</b>	
<b>Required Common Core</b>	
English Composition	6
Mathematical & Quantitative Reasoning <sup>6</sup>	3
Life & Physical Sciences <sup>7</sup> (PH101)	4
Total Required Common Core	13
<b>Flexible Common Core</b>	
History Course or Social Science Course	3
Humanities Course	3
Total Flexible Core	6
Total Common Core	19
<b>Major Curriculum Requirements (Program Core – complete All courses)</b>	
ET 506 Linux Operating System	3
ET 574 Programming and Applications with Python	3
ET 581 Object Oriented Programming in Java	3
ET 704 Networking Fundamentals I	3
ET 705 Networking Fundamentals II	3
ET 725 Computer Network Security	3
ET 726 Advanced Network Security	3
ET 754 Security Policies and Procedures	3
ET 756 Database Administration	3
ET 760 Ethical Hacking and Penetration Testing	3
Total Curriculum Requirements Credits	30
<b>Major Curriculum Requirements (Electives – complete 8 credits)</b>	
<a href="https://qcc.catalog.cuny.edu/programs/CYB-AAS">https://qcc.catalog.cuny.edu/programs/CYB-AAS</a> (check list of courses)	
Total Elective Credits	8
<b>Major Curriculum Requirements (Additional Requirements - complete 1 course)</b>	
<a href="https://qcc.catalog.cuny.edu/programs/CYB-AAS">https://qcc.catalog.cuny.edu/programs/CYB-AAS</a> (check list of courses)	
Total Additional Requirements Credits	3
Total Program Credits	60

<sup>6</sup> MAT440 is advised to be taken to satisfy the area of Mathematical & Quantitative Reasoning.

<sup>7</sup> PH101 is advised to be taken to satisfy the area of Life & Physical Sciences.

City Tech Courses: BS in Cybersecurity	Queensborough Courses: AAS in Cybersecurity	Credits
MAT 440	MAT 1375	4
CST 1101	ET 574	3
CST 1201	ET 581	3
CST 2307	ET 704 & ET 705	3
CST 2410	ET 725 & ET 726	3
CST 2415	ET 506	3
CST 3507	ET 705	3
ENGL 101	ENG 1101	3
ENGL 102	ENG 1121	3
	Flexible Core (History or Social Sciences Course)	3
	Flexible Core (Humanities Course)	3
PHYS 1433	PH 101	4

#### D. SENIOR COLLEGE UPPER DIVISION COURSE REMAINING FOR BACCALAUREATE DEGREE

Courses students will be required to take at NYCCT after completing AAS in Cybersecurity to earn the BS in Cybersecurity

COLLEGE OPTION REQUIREMENTS		
Public Speaking	COM 1330 or higher. If public speaking already taken, then as advanced liberal arts course	3
Interdisciplinary Course	Any approved interdisciplinary (ID) course	3
Total Common Core & College Option Requirements		6

DISCIPLINE REQUIREMENTS		
Gray highlight denotes courses that will be transferred to City Tech		
ENG 1101	English Comp 1	3
ENG 1121	English Comp 2	3
MAT 1375	Quantitative Reasoning	4
PHYS 1433	Life and & Physical Science ‡	3
<b>Flexible Core:</b>		
	World Culture and Global Issues	3
	US Experience and Diversity	3
	Creative Expression	3
	Individual and Society	3

	Scientific World	3
	Additional 6 <sup>th</sup> course	3
<b>College Option:</b>		
	Speech / Oral Communication	3
	Interdisciplinary Course	3
	Additional Liberal Arts course I	3
	Additional Liberal Arts course II	3
<b>Program General Education Requirements :</b>		
MAT 1375	Precalculus	4
MAT 1475	Calculus I	4
MAT 1575	Calculus II	4
MAT 2440	Discrete Struct. and Algorithms I	3
MAT 2572	Probability and Mat. Statistics I	4
<b>BS major ore requirements: Computer Systems Fundamentals:</b>		
CST 1100	Introduction to Computer Systems	3
CST 1101	Problem Solving with Comp. Programming	3
CST 1201	Programming Fundamentals	3
CST 1215	OS Fundamentals	3
CST 2307	Networking Fundamentals	3
CST 2410	Intro. To Computer Security <sup>8</sup>	3
CST 2405	Sys. Admin. Windows	3
CST 2415	Sys. Admin. Linux	3
<b>Cybersecurity Core:</b>		
CST 3507	Adv. Single-LAN Concepts	3
CST 3520	Computer Forensic	3
CST 3523	Task Auto. in Sys. Administration	3
CST 3610	Networking Security Fundamentals	3
CST 3616	Cryptographic Technologies <sup>9</sup>	3
CST 4710	Advanced Security Technologies	3
CST 4716	Cloud Security	3
CST 4726	Mobile Device Security and Privacy	3
CST 4816	Advanced Topics in Cybersecurity	3
CST 4916	Capstone Cybersecurity Course	2

## Writing Intensive Requirement

Students at New York City College of Technology must complete two courses designated WI for the baccalaureate level, one from liberal arts and one from the major.

Total degree credits to be taken at NYCCT	60
Total Credits for Degree:	120

#### E. ARTICULATION AGREEMENT FOLLOW-UP PROCEDURE

To facilitate the efficient transition between our institutions, interested QCC students are invited to utilize the pre-transfer advisement services of City Tech. Such services may be performed at NYCCT, or, by pre-arrangement, on-site at QCC. Successful graduates are also assured of availability to all ancillary services at NYCCT.

1. Procedures for reviewing, updating, modifying, or terminating agreement:

When either of the degree programs involved in this agreement undergoes a change, the agreement will be reviewed and revised accordingly by faculty from each institution's respective departments or programs, selected by their chairpersons and program directors.

2. Procedures for evaluating agreement (i.e., tracking the number of students who transfer under the articulation agreement and their success):

Each year New York City College of Technology (City Tech) will provide Queensborough Community College (QCC) the following information: a) the number of QCC graduates who applied to the program; b) the number of QCC students who were accepted into the program and the number of QCC students who enrolled and the aggregate GPA of those enrolled students at City Tech.

3. Sending and receiving college procedures for publicizing the agreement: this agreement will be publicized and posted, transfer advisors will publicize, 4. Both parties will notify the other of any changes.

Effective: Fall 2024

# Appendix D: Colleges Offering Degrees in Cybersecurity

## Sample Certificate in Cybersecurity

- SUNY Empire State University
  - Graduate Certificate in Cybersecurity  
<https://www.sunyempire.edu/graduate-studies/advanced-certificates/certificate-cybersecurity/>
  - Advanced Certificate in Cybersecurity  
<https://catalog.esc.edu/graduate/programs/cyber-security-advanced-certificate/>
- SUNY Fredonia
  - Advanced Certificate in Cybersecurity  
<https://www.fredonia.edu/academics/colleges-schools/college-liberal-arts-sciences/program/cybersecurity>
- SUNY Westchester Community College
  - Undergraduate Certificate in Cybersecurity  
<https://www.sunywcc.edu/academics/programs/cybersecurity-certificate/>
  - AAS in Cybersecurity  
<https://www.sunywcc.edu/academics/programs/cybersecurity/>
- Massachusetts Institute of Technology (MIT)
  - Professional Certificate in Cybersecurity  
<https://executive-ed.xpro.mit.edu/professional-certificate-cybersecurity>
- Harvard University
  - Cybersecurity: Managing Risk in The Information Age  
<https://harvardx-onlinecourses.getsmarter.com/presentations/lp/harvard-cybersecurity-online-short-course>
- New York University (NYU)
  - Chief Information Security Officer (CISO) Program  
<https://em.online.engineering.nyu.edu/chief-information-security-officer-program>



## Sample AAS in Cybersecurity Programs

- Queensborough Community College
  - AAS in Cybersecurity  
<https://www.qcc.cuny.edu/academics/degree-programs/aas-cybersecurity.html>
- Bronx Community College
  - AAS in Cybersecurity and Networking  
<https://www.bcc.cuny.edu/academics/academic-departments/engineering-physics-and-technology/degree-certificate-courses/cybersecurity-networking-aas/>
- SUNY Adirondack (hybrid with 50% of lectures online)
  - AAS in Information Technology: Cybersecurity  
<https://www.sunyacc.edu/degree-programs/information-technology-cybersecurity>
- SUNY Herkimer County Community College
  - AS in Cybersecurity and Digital Forensics  
<https://www.herkimer.edu/academics/programs-and-majors/program/19/cybersecurity-and-digital-forensics-a-s>
- SUNY Monroe Community College
  - AS in Homeland Security (two courses in computer security and cybersecurity)  
<https://www.monroecc.edu/depts/computerprogramming/programs/homeland-security-as-degree/>
- SUNY Finger Lakes Community College
  - AAS in Networking and Cybersecurity  
<https://www.flcc.edu/academics/networking-cybersecurity/>
- SUNY Westchester Community College
  - AAS in Cybersecurity  
<https://www.sunywcc.edu/academics/programs/cybersecurity/>
- Southern New Hampshire University

- Associate Degree in Cybersecurity  
<https://www.snhu.edu/online-degrees/associate/as-in-cyber-security>

### Samples BS in Cybersecurity Programs

- SUNY Canton
  - BS in Cybersecurity  
[https://www.canton.edu/sci\\_health/cyber/](https://www.canton.edu/sci_health/cyber/)
- John Jay College of Criminal Justice
  - BS in Computer Science and Information Security  
<https://www.jjay.cuny.edu/computer-science-and-information-security-major-advising-resources>
- Southern New Hampshire University
  - Bachelor's Degree in Cybersecurity  
<https://www.snhu.edu/online-degrees/bachelors/cyber-security>
- University of South Florida
  - BS in Cybersecurity  
<https://www.usf.edu/engineering/cse/undergraduate/bs-cybersecurity.aspx>
- University of Colorado Denver
  - Bachelor of Science in Cybersecurity  
<https://engineering.ucdenver.edu/undergraduate-programs-in-computer-science/cybersecurity>
- Rochester Institute of Technology (RIT)
  - Bachelor of Science Degree in Cybersecurity  
<https://www.rit.edu/study/cybersecurity-bs>
- Pennsylvania State University (Penn State)
  - BS in Cybersecurity Analytics and Operations  
<https://bulletins.psu.edu/undergraduate/colleges/information-sciences-technology/cybersecurity-analytics-operations-bs/>

## Sample MS in Cybersecurity Programs

- City College of New York
  - MS in Cybersecurity  
<https://cybersecurity.ccny.cuny.edu/>
- John Jay College of Criminal Justice
  - MS in Digital Forensics' and Cybersecurity  
<https://new.jjay.cuny.edu/academics/graduate-programs/masters-programs/graduate-programs-digital-forensics-cybersecurity>
- SUNY Polytechnic Institute
  - MS in Network and Computer Security  
<https://sunypoly.edu/academics/majors-and-programs/ms-network-computer-security.html>
- SUNY Empire State University
  - MS in Cybersecurity  
<https://catalog.esc.edu/graduate/programs/ms-cybersecurity/>
- Syracuse University
  - MS in Cybersecurity (online)  
<https://onlinegrad.syracuse.edu/engineering/cybersecurity/>
- Northeastern University
  - Master's in Cybersecurity  
<https://graduate.northeastern.edu/program/master-of-science-cybersecurity-boston-5249/>
- Fordham University
  - MS in Cybersecurity  
<https://www.fordham.edu/academics/departments/computer-and-information-science/academic-programs/graduate-programs/master-of-science-in-cybersecurity>

## Appendix E: CST Industry Advisory Board Meeting

Tentative list shown below:

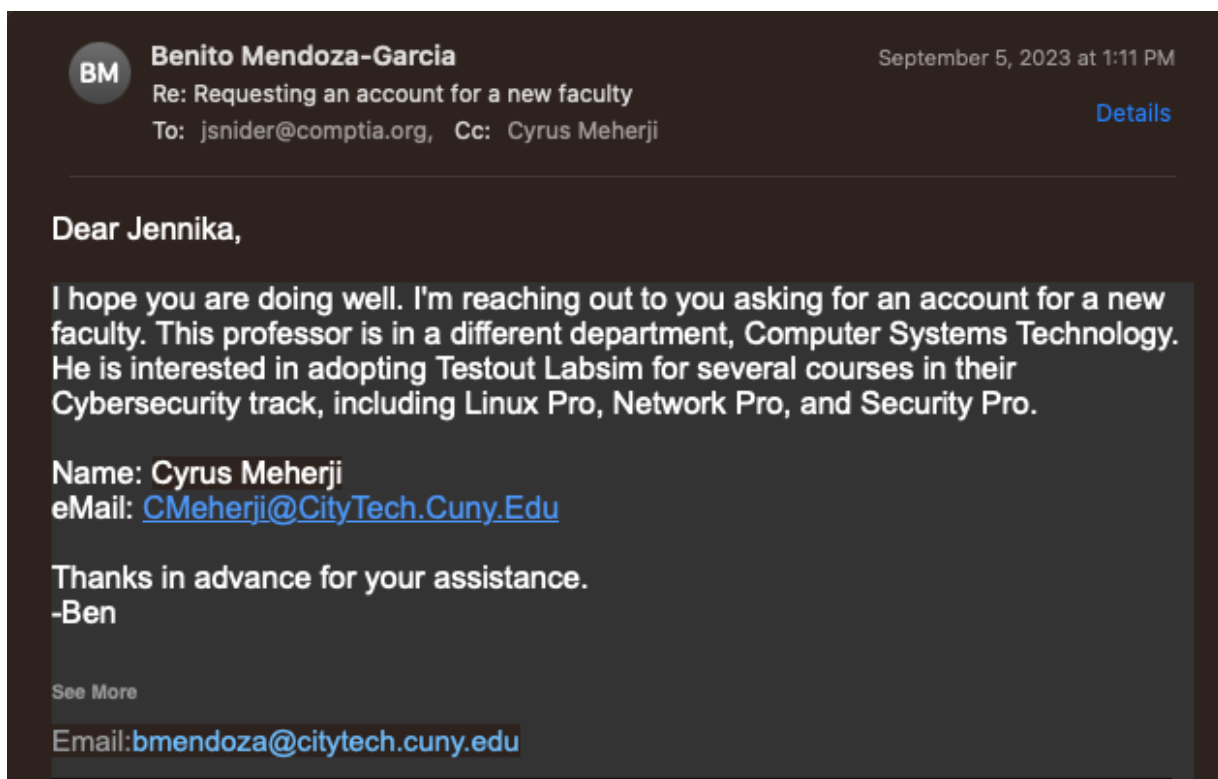
- Robert Magliaro, Education Lead, Google
- Mr. Joel Caminer, NYU-Tandon School of Engineering, Cybersecurity Program
- Mr. Felix Pretto, Enterprise CTO, Atlantic Tomorrows Office (MSP)
- Mr. Robert Ferrara, CISSP, Director of Enterprise Solutions, VC3 (MSP)
- Mr. Harry Srolovitz, Information Security, Atlantic Tomorrows Office (MSP)
- Mr. Stu Sjouwerman, CEO and Founder, KnowBe4 Security Training
- Mr. Roger Grimes, Data Driven Defense Evangelist, KnowBe4 Security Training

## Appendix F: Evidence of Consultation with Other Departments

**Contact:** Prof. Benito Mendoza,  
Associate Professor, CET Department  
Dept of Computer Engineering Tech  
New York City College of Technology

**Subject of consultation:** Discussion on network and security certifications

**Snippet of email communication:**



**Contact:** Prof. Ping Ji,  
Professor, Executive Officer & Director - CUNY Graduate Center Computer  
Science & Data Science Programs

**Subject of consultation:** Collaboration on CUNY Cybersecurity Education

**Snippet of email communication:**

**From:** Ping Ji <P.Ji@gc.cuny.edu>  
**Date:** Thursday, August 10, 2023 at 8:48 PM  
**To:** Rob Magliaro <rmagliaro@google.com>, Rosario osario <rosario@ccny.cuny.edu>, Shweta jain <sjain@jjay.cuny.edu>, Ashwin Satyanarayana <ASatyanarayana@CityTech.Cuny.Edu>, Joel Caminer <jc5429@nyu.edu>, Curtis Dann-Messier <CMessier@guttman.cuny.edu>, Cyrus Meherji <CMeherji@CityTech.Cuny.Edu>  
**Cc:** Lina Garcia <L.Garcia1@gc.cuny.edu>  
**Subject:** Reminder - 8/14 @GC Meeting on Collaborating for CUNY Cybersecurity Education

Hi everyone,

Just hope to send out a friendly reminder for our Monday meeting, at the same time welcome two more attendees to the meeting: Senior Director Joel Caminer from NYU and Dean Curtis Dann-Messier from Guttman Community College.

A few meeting details are laid out below:

**Time:** Monday August 14<sup>th</sup>, 10:15am to 2pm  
**Location:** Room 4321, CUNY Graduate Center (365 5<sup>th</sup> Ave.)  
**Agenda (flexible):**

1. 10:15am – 10:30am: arrival and opening introduction
2. 10:30am – 10:55am: Rob Magliaro, introduction of Google Certificate in Cybersecurity
3. 10:55am – 11:20am: Rosario Gennaro, introduction of CCNY Cybersecurity programs
4. 11:20am – 11:45am: Shweta Jain, introduction of John Jay Cybersecurity programs
5. 11:45am – 12:05pm: Ashwin & Cyrus, introduction of City Tech's initiatives
6. **12:05pm – 12:20pm: break & lunch served**
7. 12:20pm – 12:35pm: Dean Curtis, introduction of Guttman College's programs and needs (??)
8. 12:35pm – 12:50pm: Joel Caminer, introduction of NYU programs
9. 12:50pm ~ up to 2pm: discussions on formats and ways of collaborations, utilizing our existing resources, addressing common needs and challenges together

As indicated, this agenda is flexible. The timeframe serves as a guideline. *The most important thing is for us to share our programs' information and look for ways to collaborate.*

For everyone's convenience, I'm listing the attendees of this meeting below as well:

1. Ping Ji (me): Professor of Computer Science, Executive Officer, Director of Computer Science and Data Science, Graduate Center and John Jay
2. Rob Magliaro: Education Lead, Google
3. Rosario Gennaro: Professor of Computer Science & Director Master's Program in Cybersecurity, CCNY
4. Shweta Jain: Professor & Chair, Dept. of Math and CS, John Jay College
5. Ashwin Satyanarayana: Associate Professor & Chair, Dept. of Computer Systems Technology, City Tech
6. Cyrus Meherji: Professor of Computer Systems Technology, City Tech
7. Curtis Dann-Messier: Dean of Academic Innovation and Career Success, Guttman Community College
8. Joel Caminer: Senior Director, Center for Cybersecurity (CCS), NYU Tandon

I'm truly honored to have the opportunity to meet with all of you, looking forward to Monday!

Best regards,  
-Ping


Ping Ji  
PhD, Professor, Executive Officer, Director  
Computer Science & Data Science  
the Graduate Center & John Jay College of Criminal Justice  
City University of New York  
Tel: 212-817-8189  
Email: [pji@gc.cuny.edu](mailto:pji@gc.cuny.edu)  
Website: [click here](#)


**Contact:** Prof. Yu Wang, Ph.D  
Associate Professor & CET Program Coordinator  
Dept of Computer Engineering Tech  
New York City College of Technology

**Subject of consultation:** Include CET courses as Major electives in our BS in Cybersecurity

**Snippet of email communication:**

Re: Follow up Re: CET 4925 and CET 4973 for CST students

 Yu Wang  
To: Xiaohai Li; Benito Mendoza-Garcia; Janusz Kusk  
Cc: Ashwin Satyanarayana; Sunghoon Jang; Yu Wang  
Thu 3/2/2023 9:47 PM

 If there are problems with how this message is displayed, click here to view it in a web browser.

Prof. Kusk,  
We consult each course coordinator for which level of students to take CET 4973 and CET 4925.

For CET4973, depending on the program of study.  
In particular, we can accept students from **Computer Systems - BTECH** who have completed the courses in the sixth semester. The following courses are fundamental:

CST 3606	Object-Oriented Systems Analysis and Design	3
MAT 2440	Discrete Structures and Algorithms I	
or		
MAT 1475	Calculus I	4

On the other hand, we can accept students from **Data Science - BS\*** who have completed the courses in the fifth semester.

CST 3513	Object-Oriented Programming in Java	3
CST 3502	Data Mining	3

\* These students complete calculus I and Prob and Statistics earlier. They are better prepared for CET4973.

For CET4925,  
CET4925 does require hardware knowledge, no CST courses automatically qualify. Any CST students who want to take CET4925 must go through our department's approval. The Coordinator will look at each student's transcript before providing a recommendation. It is better to recommend senior students take elective CET4925 with CET Dept permission.

Please let us know if you need more information.  
Regards,

---

Prof. Yu Wang, Ph.D  
Associate Professor & CET Program Coordinator  
Dept of Computer Engineering Tech  
New York City College of Technology  
<http://www.cittech.cuny.edu/computer-engineering/>