Cybersecurity Pathway

Grade 9	Grade 10	Grade 11	Grade 12
Introduction to Computer Science	IT Fundamentals	Cybersecurity I - CompTiA A+	Cybersecurity Practicum

Extras: employability, work-based learning, standards acknowledgement

Introduction to Computer Science (Computer Science Discoveries)

Course Description	**Introduction to Computer Science** is a course intended to provide students with exposure to various information technology occupations and pathways such as Cybersecurity, Data Science, and Software Development. Upon completion of this course, proficient Students will be able to describe various information technology (IT) occupations and professional organizations. Moreover, they will be able to demonstrate logical thought processes and discuss the social, legal, and ethical issues encountered in the IT profession.
Recommended Prerequisites	N/A
Pathway Sequence	This is the first course in the FRNYC Cybersecurity, Data Science, and Software Development Pathway.
Aligned Non-Degree Credential	N/A
Course Standards	**Career Exploration** 1. Investigate various career opportunities within the computer science field, examining characteristics of specific roles, and present findings through various media. 2. Explore various professional societies related to information technology and compare and contrast the services and benefits provided by each. For example, investigate the Institute for Electrical and Electronics Engineers

	(IEEE), Computing Technology Industry Association (CompTIA), and the Association for Computing Machinery (ACM). **Problem Solving** 3. Students will learn how to interpret a variety of problems, learning a framework for developing steps and collaborating with others on strategies. **What is a computer?** 4. Understand components that come together to make a computer: input and outputs, processing, storing data, and more. **History and Emerging Technologies** 5. Research the history of the Internet, identifying important milestones and events, and use those events to explain the Internet's historical evolution from its inception to the present time. **Social, Legal, and Ethical Issues** 6. Research the various social, legal, and ethical issues encountered by IT professionals. Identify the roles and responsibilities one must consider while developing a prospective project or addressing an IT problem. 7. Evaluate the impact of computing technologies on equity, access, and influence in a global society and describe ways that complex computer systems can be designed for inclusivity and to mitigate unintended consequences. **Fundamental Concepts in Cybersecurity, Software, Data Science** 8. Analyze, articulate, and justify the need for ethical security practices, including but not limited to the issues of data security, confidentiality, authentication, nonrepudiation, physical security, etc. 9. Be introduced to the different factors driving software development: user needs, design, prototyping, and testing. 10. List off some key computer programming languages: Python, HTML, PHP, C++, Visual Basic, Java, JavaScript, and C #. 11. Explore different methods of representing information and creating a data set. Explore ASCII and Binary Representation. Learn how a computer represents images, numbers, and texts. 12. Identify how to problem solve with data, posing questions, collecting data, and structuring data into formats easy for computers to work with.

IT Fundamentals	
Course Description	**IT Fundamentals** is a course intended to teach students the basic concepts of cybersecurity. The course places an emphasis on security integration, application of cybersecurity practices and devices, ethics, and best practices management. The fundamental skills in this course cover both in house and external threats to network security and design, how to enforce network level security policies, and how to safeguard an organization's information. Upon completion of this course, proficient Students will demonstrate an understanding of cybersecurity concepts, identify fundamental principles of networking systems, understand network infrastructure and network security, and be able to demonstrate how to implement various aspects of security within a networking system.
Recommended Prerequisites	Introduction to Computer Science
Pathway Sequence	This is the second course in the FRNYC Cybersecurity Pathway
Aligned Non-Degree Credential	CompTIA IT Fundamentals CISCO IT Essentials (stepping stone)

Standards	• Students will learn the troubleshooting methodology and understand how it can be used to troubleshoot problems.
	• Students will be introduced to the basic IT concepts, notations, and basics of programming, and how data is stored.
	• Set up and install common peripheral devices to a laptop/PC or secure a basic wireless network.
	  ○ Optical drives
	  ○ Combo drives and burners
	  ○ Connection types
	  ○ Hard drives
	  ○ Solid state / flash drives
	  ○ RAID types
	  ○ Floppy
	  ○ Tape drive
	  ○ Media capacity
	• Students will learn about basic hardware devices for most computing systems.
	• Students will learn the basics of networking and wireless networking. Define and describe key elements of computer networking. For example, explain the types of networks and what a client-server environment is.
	• Students will learn about software and the different types of software.

	• Students will learn the fundamentals of databases and the types/structures of databases.
	
	• Students will learn about the CIA Triad and the basics of security for networks and systems.
	  ○ Physical security (e.g., lock doors, tailgating, biometrics, badges, key fobs, retinal, etc.)
	  ○ Digital security (e.g., antivirus, firewalls, antispyware, user authentication, etc.)
	  ○ User education
	  ○ Principles of least privilege

Cybersecurity I - CompTia A+ Concepts	
Course Description	**Cybersecurity I/CompTIA A+** is a course that challenges students to understand concepts and terminology of cybersecurity. This course builds on previous concepts introduced in IT Fundamentals while expanding the content to include malware threats, cryptography, wireless technologies and organizational security. Upon completion of this course, proficient students will demonstrate an understanding of cybersecurity ethical decisions, malware threats, how to detect vulnerabilities, principles of cryptology, security techniques, contingency plan techniques, security analysis, and broad risk management techniques.
Recommended Prerequisites	IT Fundamentals
Pathway Sequence	This is the third course in the FRNYC Cybersecurity Pathway
Aligned Non-Degree Credential	CompTIA A+
Standards	Hardware Identifying, using and connecting hardware components and devices, including the broad knowledge about different devices that is now necessary to support the remote workforce. Operating Systems Install and support Windows OS including command line and client support, system configuration imaging and troubleshooting for Mac OS, Chrome OS, Android and Linux OS.

	Software Troubleshooting Troubleshoot PC and mobile device issues including common OS, malware and security issues. Networking ● Demonstrating knowledge of key network protocols such as Transmission Control Protocol and Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP), directory services (e.g., Domain Name System (DNS)), and Simple Mail Transfer Protocol (SMTP). Troubleshooting Troubleshoot real-world device and network issues quickly and efficiently. Security Identify and protect against security vulnerabilities for devices and their network connections. Mobile Devices Install and configure laptops and other mobile devices and support applications to ensure connectivity for end users. Virtualization and Cloud Computing Compare and contrast cloud computing concepts and set up client-side virtualization. Operational Procedures Follow best practices for safety, environmental impacts, and communication and professionalism. Research and explain the features and requirements of common security procedures used to protect system resources on a network. Research the following storage devices and backup media. List examples of each device and detail their purpose, characteristics, proper maintenance, and methods used to back up and protect data from unauthorized use and access of data. a. Optical drives b. Combo drives and burners c. Connection types d. Hard drives e. Solid state / flash drives f. RAID types g. Floppy drive h. Tape drive

	i. Media capacity **Organizational Security Techniques** ● Define characteristics of environmental controls. For example, show how BIOS sets controls on a system. ● Develop simple policies that support the operations of security in an organization. ● Research and analyze security awareness in an organization. Provide examples of how to manage user habits and expectations related to: j. Security policy training and procedures k. Personally identifiable information l. Information classifications m. Data labeling, handling, and disposal n. Compliance with laws, best practices, and standards o. User habits p. Threat awareness q. Use of social networking

Cybersecurity Practicum	
Course Description	**Cybersecurity Practicum** is a capstone course intended to provide students with the opportunity to apply the skills and knowledge learned in previous Cybersecurity courses toward the completion of an in-depth project with fellow team members. Students who have progressed to this level in the Cybersecurity pathway take on more responsibilities for producing independent work and managing processes involved in the planning, designing, refinement, and production of cybersecurity applications. Upon completion of the practicum, proficient Students will be prepared for postsecondary study and career advancement in cybersecurity.
Recommended Prerequisites	Cybersecurity I / CompTIA Cert
Pathway Sequence	This is the fourth course in the FRNYC Cybersecurity Pathway
Aligned Non-Degree Credential	CompTIA Network+ + CompTIA Security + CISCO CCNA
Standards	**Define ethical hacking**

	• Identify current legislation that governs computer related crimes. Compare, contrast, and summarize common computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and trademark ethics pertaining to images, videos, and recorded
	• **Blue Team vs Red team**
	
	Offensive Security Methods & Tools
	• Reconnaissance of a Target
	• Analyzing Network Traffic
	• Evaluating an Exploit
	
	Data Security
	• Steganography, Hide Data in Plain Site
	• Encryption
	• Hashing
	
	Security Architecture & Security Operations
	• Network Security Data Analysis
	• Hardening Various Operating Systems
	• Web Security, Simulated Attacks
	  ○ Brute Force
	  ○ SQL Injection
	  ○ Cross Site Scripting
	  ○ Upload Attack
	
	Threats and Vulnerabilities
	Summarize the characteristics, risks, and implications of various types of attacks on systems and networks. Different types of attacks can include but are not limited to:
	a. Virus
	b. Worms
	c. Trojans
	d. Unpatched software
	e. Password cracking
	f. Advanced persistent threat
	g. Reconnaissance/footprinting
	h. Infiltration
	i. Network breach
	j. Network exploitation
	k. Attack for effects (e.g., deceive, disrupt, degrade, and destroy)
	l. DoS/DDoS, session hijacking
	m. HTTP spoofing

	n. DNS attacks o. Switch attacks p. Man-in-the-middle (MITM) attacks q. Cross site scripting r. Drive-by-attacks s. Social Engineering attacks **Wireless Security Techniques** Analyze attack methods on wireless networks. For example: man in the middle, sniffing, and wireless Service Set Identifier (SSID) spoofing. Demonstrate the use of wireless security protocols. **Advanced Methods of Cybersecurity** ● Utilizing prior fundamentals, demonstrate proper secure network configuration and administration regarding ports and routing tables ● Utilizing prior fundamentals, demonstrate proper secure network configuration and administration of the following communication capabilities/protocols: ● Configuring a Virtual Private Network (VPN). ● Demonstrating the knowledge and use of network statistics (netstat), and network maps such as that generated by Zenmap and similar utilities. **Course Project** ● In groups, collaborate on a security or ethical hacking plan based on a mock situation, presenting on relevant reconnaissance and potential attacks or defenses. ● Upon completion of the practicum, develop a public presentation showcasing highlights, challenges, and lessons learned from the experience of the FRNYC pathway.

Extras: Employability, Recommended Work-based Learning, Standards Acknowledgment

Employability Skills

Ensure employability skills are supported through classroom instruction and curriculum design. Employability Skills Framework, United States Department of Education. (2014). http://cte.ed.gov/employabilityskills

1. Demonstrate creativity and innovation
2. Demonstrate critical thinking & problem solving
3. Communicate clearly and effectively, verbally and in writing
4. Collaborate and work productively as a team member
5. Demonstrate information literacy
6. Use technology effectively and appropriately
7. Demonstrate initiative and self-direction
8. Demonstrate professionalism and ethical behavior
9. Demonstrate interpersonal and social skills using cultural/global competence
10. Demonstrate adaptability and flexibility
11. Demonstrate productivity and accountability

Recommended Work-Based Learning Experiences

Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring in addition to specific knowledge and skills referenced in the standards. Potential activities to address career exploration:

- Visit a workplace aligned with careers in the FRNYC pathway
- Revisit career interest survey and revise plan for required postsecondary education related to the career of interest
- Interview an employer to learn more about their profession
- Have an employer visit the classroom to discuss content related to standards and how this applies to their every-day job OR have students shadow an employer for a day

Standards Sources

The standards in these courses are derived from and aligned to national and state standards in Information Technology.

Standards are aligned to NY State Standards in Math, Science, and Technology, NY StateLearning Standards for Career Development and Occupational Studies, NYC Computer Science and Digital Fluency Standards, the Information Technology standards from the Common Career and Technical Core. **Standards are derived** from the National Institute for Science and Technology, National Initiative for Cybersecurity Education (NICE) Framework, Tennessee State standards in Information Technology, Texas State Standards in Information Technology, Nebraska State standards in Information Technology, Washington DC Public Schools Information Technology Standards, and the Greater Washington Partnership Employer Signaling System for Information Technology.