# Fundamentals of Cyber Security Certificate

The Fundamentals of Cyber Security certificate is designed for students who want to pursue a career in cybersecurity. This certificate will provide learners with the essential skills and knowledge to protect networks, systems, and data from cyber threats. Students will learn about the principles and practices of cybersecurity, such as threat analysis, risk mitigation, security operations, and incident response. Learners will also gain hands-on experience with various security tools and technologies, such as encryption, firewalls, penetration testing, and digital forensics. Upon completion of this certificate, students will be prepared to take the CompTIA Security+ certification exam, which is a globally recognized credential for cybersecurity professionals. Students will also be ready to apply for entry-level internships in the cybersecurity field, where you can further develop your skills and advance your career.

Students will be advised to have a functioning computer (not Chromebook) with access to reliable Wi-Fi. It is also recommended that students have fundamental computer literacy skills (office, computer navigation) prior to enrolling in the program.

All course requirements must be completed with a grade of 'C' or higher. This program requires 6 credits be taken at Charter Oak.

## Major Requirements

| | |
|---|---|
| CSS 101: Cybersecurity Fundamentals | 3cr |
| Operating Systems and Asset Security | 3cr |
| Incident Response | 3cr |
| ITE 220:  Networking and Data Communications | 3cr |

### Program Learning Outcomes

Students who graduate with a certificate in Fundamentals of Cyber Security will be able to:

- identify and explain the key concepts and principles of cybersecurity, such as confidentiality, integrity, availability, authentication, authorization, and encryption;
- apply appropriate security tools and techniques to protect networks, systems, and data from cyber threats, such as malware, phishing, denial-of-service, and unauthorized access;
- analyze and evaluate the security posture and vulnerabilities of a given network or system, using methods such as risk assessment, penetration testing, and security auditing;
- demonstrate the ability to communicate effectively and ethically with various stakeholders in the cybersecurity field, such as clients, managers, colleagues, and users, using oral, written, and graphical modes; and
- prepare for the CompTIA Security+ certification exam by reviewing the exam objectives, format, and sample questions.