Cyber Security Certificates

The cyber security certificates are designed for the person who has a strong computer background and is already working in the cyber security field and wants to enhance their skills.

For each Certificate, 9 credits must be completed at Charter Oak and a
ll courses must be completed with a grade of 'C' or better.

Cyber Security Fundamental Certificate

ITE 145: Fundamentals of Information Systems Security	3cr
CSS 146: Legal Issues in Information Security	3cr
CSS 230: Managing Risk in Information Systems	3cr
CSS 245: Security Policies and Implementation Issues	3cr
CSS 345: Auditing IT infrastructure for Compliance	3cr
CSS 435: Fundamentals of Network Security	3cr
Total	**18cr**

Security Strategies Application Certificate

ITE 145: Fundamentals of Information Systems Security	3cr
CSS 230: Managing Risk in Information Systems	3cr
CSS 347: Security Strategies in Windows OS/Applications	3cr
CSS 348: Security Strategies in Linux OS/Applications	3cr
CSS 438: Security Strategies for Web Apps and Social Networking	3cr
Total	**15cr**

Cyber Security Investigation Certificate

ITE 145: Fundamentals of Information Systems Security	3cr
CSS 146: Legal Issues in Information Security	3cr
CSS 230: Managing Risk in Information Systems	3cr
CSS 436: Systems Forensics Investigation and Response	3cr
CSS 437: Hacker Techniques Tools and Incident Handling	3cr
Total	**15cr**

Technical Security Administration Certificate

ITE 145: Fundamentals of Information Systems Security	3cr
CSS 230: Managing Risk in Information Systems	3cr
CSS 346: Access Control, Authentication and PKI	3cr
CSS 347: Security Strategies in Windows OS/Applications	3cr
CSS 435: Fundamentals of Network Security	3cr
CSS 437: Hacker Techniques Tools and Incident Handling	3cr
Total	**18cr**

Student Learning Outcomes

Students who graduate with one of the Certificates listed above will be able to:

1. explain the landscape, key terms, and concepts related to the many layers of information systems security;

2. explore and explain the fields in digital forensics and cyber policy analysis;
3. create policies and standard operating procedures for organizations that are ethically, morally, and legally sound while recognizing ethical dilemmas and social responsibilities;
4. identify and critically assess issues and concepts related to the protection of information and information systems; and
5. use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions at risk in information systems.