CYBERSECURITY

The Cybersecurity program that will prepare students to design, develop, and maintain secure computer systems and provide security for the users they service. Students in this program will study cybersecurity as it relates to hardware, software, user, and data security. Tracks are available in Secure Coding, Network Defense, Cyber Forensics, Cyber Science.

Cybersecurity is a discipline that is needed in every aspect of our society. Organizations that do electronic business are required to keep the information that they handle secure from hackers and others. Many organizations are just identifying the need for Cybersecurity professionals. Data and networks have to be secured to do business in the world today. Businesses often hire consulting agencies or hire Cybersecurity specialists to secure networks.

The Cybersecurity program is set up to be completed in two years. There are no admission requirements for the program.

Certificate Descriptions:

The Cyber Network and Forensics Fundamentals certificate provides fundamental concepts related to defending computer resources, including networks, and understanding the relationships between cyber defense and forensics (responding to breaches).

The Network Defense - Advanced certificate will prepare students with knowledge of security and forensics using network and cloud technologies. Students in this program will study network security, authentication, and ethical hacking as it relates to network and cloud environments.

The Cyber Forensics - Advanced certificate presents a study of digital forensics principles and related laws, how to respond to security breaches, how to secure data, devices and networks for forensics investigations, and how to write the conclusions of a forensics investigation (reporting). Presents concepts on computer forensics, Mobile Device Forensics, network and cloud forensics and ethical hacking from a forensics view.

The Cyber Defense Fundamentals certificate presents fundamentals concepts for the field of cybersecurity. This certificate is specifically designed to meet the National Security Agency and the U.S. Department for Homeland (NSA/DHS) security criteria for schools who wish to apply to be a Center of Academic Excellence in Cyber Defense (CAE-CD) for two-year colleges.

The Cryptography Fundamentals certificate presents a study of cryptography. Presents concepts related to historical and contemporary encryption techniques and algorithms, mathematical concepts used with cryptography, and software development for cryptographic algorithms.

The Secure Coding – Fundamentals certificate introduces programming concepts with secure coding principles and practices by focusing on developing software that is free from security vulnerabilities. This certificate provides a comprehensive study of secure software development. Emphasis will be placed on skills required to design, develop, and analyze secure software. Presents concepts which meet national standards in secure software development.

The Secure Coding – Advanced certificate provides students with a more in-depth study of secure programming, data structures, modern programming languages, and secure web application development. Emphasis will be placed on skills required to determine security issues and vulnerabilities and mitigate such vulnerabilities. Presents concepts which meet national standards in secure software development.

The Secure Coding – CIT Bridge certificate provides CIT students with cybersecurity secure coding principles and practices. Presents concepts which meet national standards in secure software development focusing primarily on developing secure code and not “how to program” which is taught in CIT programming courses.

DEGREES

- Cybersecurity - AAS (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cybersecurity-aas/)
  - Cyber Forensics Track (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cybersecurity-aas/#cyberforensicstrack)
  - Cyber Science Track (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cybersecurity-aas/#cybersciencetrack)
  - Network Defense Track (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cybersecurity-aas/#networkdefensetrack)
  - Secure Coding Track (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cybersecurity-aas/#securecodingtrack)

CERTIFICATES

- Cryptography Fundamentals - Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cryptography-fundamentals/)
- Cyber Defense Fundamentals - Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cyber-defense-fundamentals/)
- Cyber Forensics- Advanced- Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cyber-forensics-advanced/)
- Cyber Network and Forensics Fundamentals - Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/cyber-network-and-forensics-fundamentals/)
- Network Defense- Advanced - Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/network-defense-advanced/)
- Secure Coding- Advanced- Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/secure-coding-advanced/)
- Secure Coding- CIT Bridge - Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/secure-coding-cit-bridge/)
- Secure Coding- Fundamentals- Certificate (https://catalog.kctcs.edu/programs-of-study/aas/cybersecurity/secure-coding-fundamentals/)

Course	Title	Credits
CYS 231	Internet of Things Security and Forensics	3
CYS 234	Computer Operating Systems Forensics	3
CYS 249	Ethical Hacking	3
CYS 250	Secure Software Development II	3
CYS 258	Survey of Programming Languages	3
CRJ 211	Liability & Legal Issues	3
Electives approved by CYS Coordinator [1]		

[1] CIT 120 may be accepted as an elective only for those bridging.