CSEC - CYBERSECURITY

CSEC 110. Principles of Cybersecurity
3 Credits (3)
Course covers contemporary trends in cybersecurity including understanding characteristics of security vulnerabilities as they relate to hardware, software, data, procedures, and user actions. Restricted to Community Colleges campuses

Learning Outcomes
1. Explain the importance of cybersecurity in the global economy.
2. Explain why cybersecurity is a growing profession.
3. Explain how hackers use unsuspecting individuals to propagate risk
4. Explain why cybersecurity is critical to industry and public safety
5. Explain approach to cybersecurity.
6. Explain the characteristics of cyber warfare.
7. Explain trends in the cyber threat landscape.
8. Explain the framework of enterprise security solutions.

CSEC 127. Internet of Things Integration
3 Credits (3)
Continuation of concepts taught in CTEC 127. Course expands on the importance of the Internet of Things (IoT) in society, control systems, communications, sensors, actuators, cloud computing, security, and databases. May be repeated up to 6 credits.
Prerequisite: CTEC 127.

Learning Outcomes
1. Demonstrate a detailed understanding of IoT.
2. Understand the societal impact of IoT.
3. Recognize challenges the IoT presents to security.
4. Develop an understanding of embedded programming language syntax and attributes.
5. Demonstrate assembly of electronic circuitry using a single-board computer.

CSEC 180. Introduction to Data Analytics
3 Credits (3)
A broad introduction to the field of data analytics that prepares students to explore key areas of the analytical process of how data is created, stored, cleaned, visualized, and analyzed. May be repeated up to 6 credits.

Learning Outcomes
1. Demonstrate basic principles of data analysis using analytical tools.
2. Apply data analytics to contemporary workplace performance.
3. Describe how data is stored and accessed through relational database(s).
4. Use programming language(s) to analyze data.
5. Integrate application software to analyze and visualize simple dataset.

CSEC 275. Introductory to Cryptography
3 Credits (3)
Introduction to the foundation of cryptography, principles behind cryptographic design, and cryptographic applications. Topics include encryption techniques, common cryptographic protocols and security functions.
Prerequisite(s)/Corequisite(s): MATH 1215 or above. Restricted to Las Cruces campus only.

Learning Outcomes
1. Describe the operations and benefits of cryptography
2. Able to understand necessary cryptography encoding
3. Able to use standard tools for penetration testing and compliance
4. Describe the basic need for cryptography and why it is essential for security.

CSEC 280. Introduction to Cyber Defense
3 Credits (3)
Introduction to the foundation of cryptography, principles behind cryptographic design, and cryptographic applications. Topics include encryption techniques, common cryptographic protocols and security functions.
Prerequisite(s)/Corequisite(s): MATH 1215. Restricted to Las Cruces campus only.

CSEC 283. Ethical Hacking and Penetration Testing
3 Credits (3)
Introduces students to the tools and software used in ethical hacking and penetration testing as well as introducing them to some of the vulnerabilities and exploits that exist within the cybersecurity field.
Prerequisite: E T 153 and E T 156.
Prerequisite/Corequisite: E T 283.

Learning Outcomes
1. Identify and describe common threats and vulnerabilities.
2. Describe/demonstrate how to secure a network.
3. Identify and demonstrate common tools used in ethical hacking/ penetration testing.
4. Identify and describe legal/ethical issues pertaining to ethical hacking.

CSEC 285. Introduction to Managing Information Security
3 Credits (3)
Managerial aspects of information security and assurance including access control models, information security governance, accountability metrics, legal responsibilities, and information security program assessment.
Prerequisite(s)/Corequisite(s): CTEC 290 or OECS 269. Restricted to Las Cruces campus only.

CSEC 286. Information Security Certification Preparation
4 Credits (4)
Covers the examination objectives and detailed preparation to prepare students to take the CompTia Security+ exam.
Prerequisite: E T 153, E T 156, and E T 283.

Learning Outcomes
1. Identify and describe common threats and vulnerabilities.
2. Identify and demonstrate common security devices/programs.
3. Describe/demonstrate how to secure a network.

CSEC 295. Cybersecurity Capstone
3-4 Credits (3-4)
Experiential hands-on learning applying skills and knowledge gained in technology and cybersecurity-related courses supporting contemporary workforce performance. May be repeated up to 8 credits.

Learning Outcomes
1. Evaluate technical components, systems and integrated systems.
2. Demonstrate individualized project-based skills.
3. Develop integrated system solutions.
4. Integrate cyber technology to support workplace performance.