COURSE SYLLABUS

Tunxis Community College

Education That Works For a Lifetime

Course Title:	Cyber Crimes	**Date submitted:**	October 2021 (AAC: 21-26)
Department:	STEAM		
Curriculum:	Computer Information Systems		

Course Descriptors: Make certain that the course descriptors are consistent with college and Board of Trustees policies, and the current course numbering system.

Course Code: (eg. ACC 101)	**CST*135**
Course Type:	**L/D**

A: Clinical B: Lab D: Distance Learning
I: Individual/Independent L: Lecture N: Internship
M: Seminar P: Practicum U: Studio
X: Combined Lecture/Lab Y: Combined Lecture/Clinical/Lab Z: Combined Lecture/Studio

Elective Type:	**G**

AH: Art History E: English FA: Fine Arts FL: Foreign Language G: General HI: History HU: Humanities LAS: Liberal Arts & Sciences M: Math S: Science SS: Social Science

Credit Hours:	3
Developmental: (yes/no)	No
Contact Hours: Lecture:	3
Clinical:	0
Lab:	0
Studio	0
Other:	0
TOTAL:	3
Class Maximum:	24
Semesters Offered:	S

Prerequisites:

C-or better in Integrated Reading and Writing II (ENG*075) OR Introduction to College Reading & Writing (ENG*093) OR Introduction to College English (ENG*096) OR Reading & Writing VI (ESL*162), or placement into Composition (ENG*101) [including embedded: Composition Workshop ENG*101E]

Corequisites:

None

Other Requirements:

None

Catalog Course Description:

This course provides an overview of the different types of computer crimes including hacking, fraud, social engineering, ransomware; their impact on the laws and regulations at the state, federal, and international level, and the guidance provided by the National Institute of Standards and Technology (NIST) to protect against cybercrime. Topics include types of cybercrimes, cybercrime laws and regulations, protection against cybercrime, impact of cybercrime in the economy.

Topical Outline: List course content in outline format.

1. Types of computer crimes
2. Hacking, computer break-ins, fraud.

3. Social engineering, phishing, vishing, Business email compromise (BEC)
4. Impact of cybercrime in the economy and security of nations
5. Laws and Regulations against cybercrime: State and Federal
6. Laws and Regulations against cybercrime: International
7. Security vs. Privacy Regulations
8. Response to Cybercrime: National Institute of Standards and Technology (NIST) Guidance
9. Security Frameworks: NIST vs. ISO
10. Role of Computer Forensics

Outcomes:
Describe measurable skills or knowledge that students should be able to demonstrate as evidence that they have mastered the course content.

Upon successful completion of this course, the student will be able to do the following:

1. Demonstrate an understanding of all types of computer crimes.
2. Identify the impact of cybercrime to business, economy, and security of nations.
3. Gain exposure to the latest types of social engineering attacks including phishing, vishing, Business email compromise.
4. Identify the laws and regulations created to combat cybercrime at the USA state and federal levels.
5. Identify the laws and regulations created to combat cybercrime at the International level.
6. Explain the difference between Security vs. Privacy in the context of cybersecurity.
7. Understand the strategies and frameworks created by NIST and ISO to guide organizations in their battle against cybercrime.
8. Understand the role Computer Forensics plays in fighting cybercrime

PROGRAM: *(Numbering reflects Program Outcomes as they appear in the college catalog)*

Cybersecurity Associate of Science Degree

3. solve computer-related problems
7. synthesize computer information systems knowledge and skills in solving basic information processing systems problems
10. knowledge of industry standard networking and communication technology

GENERAL EDUCATION/TAP OUTCOMES: *(Numbering reflects General Education Outcomes as they appear in the college catalog)*

2. **Critical Analysis/ Logical Thinking -** Students will be able to organize, interpret, and evaluate evidence and ideas within and across disciplines; draw reasoned interferences and defensible conclusions; and solve problems and make decisions based on analytical processes.

   Demonstrates: Identifies the issue(s); formulates an argument; explains and analyzes relationships clearly; draws reasonable inferences and conclusions that are logical and defensible; provides support by evaluating credible sources of evidence necessary to justify conclusions.

   Does Not Demonstrate: Identifies few or no issues; formulates an argument without significant focus; provides an unclear explanation of analysis and relationships; drawing few reasonable inferences and conclusions that are illogical and indefensible; provides little to no support using credible sources of evidence necessary to justify conclusions.

	3. **Ethical Dimensions -** Students will identify ethical principles that guide individual and collective actions and apply those principles to the analysis of contemporary social and political problems. **Demonstrates**: Identifies and reflects critically on ethical issues presented in classroom instruction or in assigned co-curricular or civic activities and/or professional internships and practica.
Evaluation: List how the above outcomes will be assessed.	**Assessment will be based on the following criteria:** 1. Written examinations will demonstrate an understanding of major facts, procedures, and theories.
Instructional Resources: List library (e.g. books, journals, on-line resources), technological (e.g. Smartboard, software), and other resources (e.g. equipment, supplies, facilities) required and desired to teach this course.	**Required:** No special software is required as a pre-requisite. **Desired:** None
Textbook(s)	Refer to current academic year printout