COURSE SYLLABUS

Tunxis Community College

Education That Works For a Lifetime

Course Title:	Network Security Fundamentals	**Date submitted:**	May 2019 (AAC: 19-25)
Department:	Business and Technology		
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*270
Course Type:	X

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

Elective Type:	G

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:	F/S

Prerequisites:

Network Essentials I (CST*130) and Windows Server Administration (CST*163)

Corequisites:

None

Other Requirements:

None

Catalog Course Description:

Introduces students to the subject of network security. Topics include security models, authentication, attacks, infrastructure devices, intrusion detection, and the basics of cryptography along with physical security and disaster recovery. This course emphasizes preparing the student for the CompTIA Security+ certification.

Topical Outline: List course content in outline format.

1. Introduction to security concepts
2. Authentication
3. Denial of Service attacks, Spoofing, Worms, Backdoors, Logic Bombs
4. Remote Access Security (L2TP, IPSec)
5. Email Security, Spam
6. Web Security
7. Wireless 802.11 Standards and Instant Messaging
8. Security devices (firewalls, routers, switches)
9. Intrusion Detection
10. Network Security Topologies

11. Cryptography
12. Physical Security
13. Disaster Recovery

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:

COURSE:

1. Demonstrate an understanding of network security and the goals of network security.
2. Create strong passwords and store them securely.
3. Explain the major types of malicious software and identify a counter measure for each one.
4. Demonstrate how to safeguard against email vulnerabilities.
5. Identify vulnerabilities associated with certain web applications such as instant messaging.
6. Conduct a security site survey.
7. Explain the role of routers, switches, firewalls and other networking hardware in security.
8. Identify the place and role of the demilitarized zone in the network.
9. Detail the differences between host-based and network-based intrusion detection.
10. Explain the concept of cryptography and how it relates to network security.
11. Implement the disaster recovery process for a given scenario.

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

Computer Information Systems Associate Degree

NETWORKING

11. Analyze and evaluate a networking scenario and recommend appropriate solutions.

GENERAL EDUCATION: *(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 inferences 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 (embedded) -** 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.

   Does Not Demonstrate: Does not sufficiently identify or reflect 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. Hands-on assignments and case studies will demonstrate an understanding of theories
2. Written examinations will demonstrate an understanding of major facts, procedures and theories.
3. A comprehensive project will demonstrate the ability to apply theories and knowledge to a specific situation.

The comprehensive project will be designated as an electronic portfolio piece for uploading to ePortfolio.org.

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: Computer Lab Desired: None
Textbook(s)	Refer to current academic year printout.