I. TITLE OF COURSE: CS1903- Information Security

II. COURSE DESCRIPTION: 3 **credit hours**
3 **credit hours of lecture and** 0 **credit hours of lab per week.**

This course examines principles of information security. Security awareness, analysis, design, implementation and maintenance are explored.
Course will prepare students for the Security+ certification.

For each unit of credit, a minimum of three hours per week with one of the hours for class and two hours for studying/preparation outside of class is expected.

Pre-requisite: None

III. PROGRAM AND/OR DEPARTMENT MISSION STATEMENT:

The CIS Program will provide superior learning opportunities in the area of information technology, utilizing state-of-the-art technology, for both CIS majors and non-CIS majors to enable all students to achieve their career and/or educational goals.

IV. TEXTBOOK AND MATERIALS:

Textbook selected when course is offered.

V. SCCC OUTCOMES

Students who successfully complete this course will demonstrate the ability to do the following SCCC Outcomes.

1: Read with comprehension, be critical of what they read, and apply knowledge gained to real life

5: Demonstrate the ability to think critically by gathering facts, generating insights, analyzing data, and evaluating information
6: Exhibit skills in information and technological literacy

VI. COURSE OUTCOMES:

Upon completing of the Introduction to PC Systems Hardware course with 80% or higher mastery of course competencies, the student should be able to:
Introduction to security aspects of information in society
Establish understanding in information security
Describe legal, ethical and professional issues
Identify risk management and security planning
Security Technologies
How to implement security programs
How to evaluate and maintain security programs

VII. COURSE OUTLINE:

1. Explain characteristics of information
2. System Development Life Cycle
3. Security in business

4. Common threats and attacks
5. Information laws and policies
6. Ethical issues
7. Identify, assess and control risk
8. Contingency plan
9. Incident response plan
10. Disaster recovery plan
11. Business continuity plan
12. Firewall and Virtual Private Network
13. Intrusion detection
14. Cryptography
15. Physical and virtual security considerations
16. Security management practices
17. Monitor/evaluate security program

VIII. INSTRUCTIONAL METHODS:

Classroom lecture/discussion
Handouts, videos, on screen presentations
Demonstrations using projector
Hands-on computer lab projects both in teams and individually
Instructors will enforce the Academic Honor Code & Cheating Policy as set forth in the SCCC College Catalog. Students who fail to adhere to this policy will receive an F for the course final grade unless otherwise stated in the instructor's course policies.

IX. INSTRUCTIONAL AND RESOURCE MATERIALS:

Assorted periodical and newsletter articles as they apply to course
Miscellaneous personal computer hardware/software

X. METHODS OF ASSESSMENT:

Outcomes #1, #5, and #6 will be assessed by:
Hands-on lab assignments, quizzes and exams will assess student knowledge of the material covered.
Group assignments and projects will assess student ability to think critically by gathering and analyzing data and generating insight into problem solving methodology.

XI. ADA STATEMENT:
Under the Americans with Disabilities Act, Seward County Community College will make reasonable accommodations for students with documented disabilities. If you need support or assistance because of a disability, you may be eligible for academic accommodations. Students should identify themselves to the Dean of Students at 620-417-1106 or going to the Student Success Center in the Hobble Academic building, room 149 A.

Syllabus Reviewed: 03/25/2020 17:15:01