COURSE SYLLABUS

LAST REVIEW	Fall 2022
COURSE TITLE	Enterprise Security Management
COURSE NUMBER	CIST 0235
DIVISION	Career and Technical Education
DEPARTMENT	CIST
CIP CODE	24.0101
CREDIT HOURS	3
CONTACT HOURS/WEEK	Class: 3 Lab:
PREREQUISITES	CIST 0125

COURSE DESCRIPTION

Microcomputer Business Software explores the use of microcomputers in business. The four most common programs of spreadsheets, database management, presentation and word processing are used as models.

PROGRAM ALIGNMENT

This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit: https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Demonstrates the necessary skills to score at least a 70% in the Network 1 course.
2. Obtain the skills necessary to pass the Certification COMPTIA SEC+ certification.
3. Applies judicious and ethical offensive security techniques using knowledge gained through cyber security coursework.
4. Obtain the skills necessary to pass the NET+ certification.

TEXTBOOKS

http://kckccbookstore.com/

METHOD OF INSTRUCTION

A variety of instructional methods may be used depending on content area. These include but are not limited to lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE

I. Planning for Contingency
   A. Continuity and recovery
   B. Plan Development
   C. Operating Systems back up

II. Security Risk Analysis
   A. Risk analysis principles
   B. Risk analysis methods
   C. Risk analysis process
   D. Minimize risks technology
   E. Continuous risk assessment

III. Security Policy
   A. Security policies principles
   B. Design of Security policy
   C. Security policy contents

IV. Common Criteria
   A. Common criteria principles
   B. Common criteria levels
   C. Procedures governing common criteria
   D. Regulations governing common criteria

V. Certification and Accreditation
   A. Federal information systems certification
   B. Federal information systems accreditation
   C. Key participant's duties and responsibilities
   D. Applications to non-government organizations

VI. Biometrics
   A. Biometrics process
   B. Biometrics accuracy
   C. Biometrics applications
   D. Scanning of fingerprint, facial, iris, retinal, and vocal
   E. Advanced biometric technologies
   F. Compromising biometrics

VII. Authentication
   A. Strong authentication
   B. The needs for strong authentication
   C. Authentication tokens
   D. RSA SecurID
   E. Smart cards

COURSE LEARNING OUTCOMES AND COMPETENCIES
Upon completion of the course, the student will:

A. Plan for contingency.

1. Understand the continuity and recovery concepts.
2. Develop plans for continuity and recovery.
3. Backup operating systems.

B. Analyze security risks.

4. Analyze security risks.
5. Explain security risk analysis methods
6. Explain security risk analysis process.
7. Minimize security risks.
8. Understand continuous risk assessment.

C. Understand security policy.

9. Understand security policies principles.
10. Design security policies.
11. Explain security policy contents.

D. Explain common criteria.

12. Understand common criteria principles.
13. Understand common criteria levels.
14. Explain procedures and regulations governing common criteria.

E. Explain federal information systems certification and accreditation.

15. Explain federal information systems certification.
16. Explain federal information systems accreditation.
17. Explain key participant's duties and responsibilities.
18. Understand applications to non-government organizations.

F. Understand biometrics technology.

19. Understand biometrics process.
20. Explain biometrics accuracy.
21. Explain biometrics applications.
22. Understand the process of scanning of fingerprint, facial, iris, retinal, and vocal.
23. Understand advanced biometric technologies
24. Compromise biometrics.

G. Understand biometrics technology.

25. Understand strong authentication.
26. Explain the needs for strong authentication.
27. Explain authentication tokens.
28. Explain RSA SecurID.
29. Explain smart cards.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor's course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook
https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog
https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.