COWLEY COLLEGE
& Area Vocational Technical School

COURSE PROCEDURE FOR

PRINCIPLES OF INFORMATION ASSURANCE
CIS1906 3 Credit Hours

Student Level:
This course is open to students on the college level in either the freshman or sophomore year.

Catalog Description:

CIS1906 – PRINCIPLES OF INFORMATION ASSURANCE (3 hrs)
An Introduction to the general concepts of security issues and implementation of security within an organization.

Prerequisites:
None

Controlling Purpose:
This course is designed to meet the needs of students in explaining the various issues in computer security including protection, identification and implementation of security procedures and software

Learner Outcomes:
Upon completion of the course, the student will gain an understanding of basic security, methods of implementing software and hardware based security. Various techniques involved in cyber attacks will be discussed including protection against these attacks

Units Outcomes and Criterion Based Evaluation Key for Core Content:
The following defines the minimum core content not including the final examination period. Instructors may add other content as time allows.

Evaluation Key:

A = All major and minor goals have been achieved and the achievement level is considerably above the minimum required for doing more advanced work in the same field.

B = All major goals have been achieved, but the student has failed to achieve some of the less important goals. However, the student has progressed to the point where the goals of work at the next level can be easily achieved.

C = All major goals have been achieved, but many of the minor goals have not been achieved. In this grade range, the minimum level of proficiency represents a person who has achieved the major goals to the minimum amount of preparation necessary for taking more advanced work in the same field, but without any major handicap of inadequacy in his background.

D = A few of the major goals have been achieved, but the student's achievement is so limited that he is not well prepared to work at a more advanced level in the same field.

F = Failing, will be computed in GPA and hours attempted.

N = No instruction or training in this area.

UNIT 1: INTRODUCTION TO INFORMATION SECURITY Outcomes: Understand the basic definitions of information security						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						List the history of information security
						Explain what is meant by security
						Explain the critical characteristics of information
						Explain the idea of the NSTISSC Security Model
						List the components of an information system
						Explain what is meant by securing components
						Explain balancing information security and access
						List the approaches to information Security Implementation
						Explain the Systems Development Life Cycle and the Security Systems Development Life Cycle

UNIT 2: THE NEED FOR SECURITY Outcomes: Understand the need for security including types of threats						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain business needs
						List and Explain the different threats
						List and Explain the various forms of computer attacks
						Explain the need for secure software development

UNIT 3: LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY Outcomes: Understand the various legal, ethical and professional topics involved in securing a computer system						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain how laws and ethics interact in information security
						List relevant U.S. laws
						List international laws and legal bodies
						Explain ethics and information security
						Explain codes of ethics and professional organizations

UNIT 4: RISK MANAGEMENT Outcomes: Understand the various topics in risk management including identification, assessment, and control						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain what is risk management
						Explain what is risk identification
						Explain what is risk assessment
						List and Explain risk control strategies
						Explain how to select a risk control strategy
						Explain quantitative versus qualitative risk control practices
						Explain risk management discussion points
						List recommended risk control practices

UNIT 5: PLANNING FOR SECURITY Outcomes: Understand how to design a plan for implementing security						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain information security policy, standards, and practices
						Explain the information Security Blueprint
						Explain security education, training and awareness program
						Explain continuity strategies

UNIT 6: SECURITY TECHNOLOGY: FIREWALLS AND VPNS Outcomes: Understand how to implement security using software and hardware						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the physical design
						Explain and install firewalls
						Explain how to protect remote connections

UNIT 7: SECURITY TECHNOLOGY: INTRUSION DETECTION, ACCESS CONTROL, AND OTHER SECURITY TOOLS Outcomes: Understand how to detect intrusion in your computer system.						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain what is intrusion detection and prevention systems (IDSs and IPSs)
						Explain what are honey pots, honey nets, and padded cell systems
						Explain and use scanning and analysis tools
						Explain access control devices

UNIT 8: CRYPTOGRAPHY Outcomes: Understand the needs for cryptography and how to implement it						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the foundations of Cryptology
						Explain and calculate various cipher methods
						Explain various cryptographic algorithms
						Explain and use various cryptographic tools
						List Protocols for Secure Communications
						List and Explain Attacks on Cryptosystems

UNIT 9: PHYSICAL SECURITY Outcomes: Understand the physical considerations in implementing security						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						List physical access controls
						Explain fire security and safety
						Explain failure of supporting utilities and structural collapse
						Explain Interception of Data
						List and Explain Mobile and Portable Systems

UNIT 10: IMPLEMENTING INFORMATION SECURITY Outcomes: Understand the issues that come up in actual implementation						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain information security project management
						Explain implementation topics
						Explain nontechnical aspects of implementation
						Explain systems security certification and accreditation

UNIT 11: SECURITY AND PERSONNEL Outcomes: Understand the need for policies in dealing with personnel						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain positioning and staffing the security function
						List and Explain credentials of information security professionals
						Explain employment policies and practices
						Explain security considerations for nonemployees
						List and Explain interval control strategies
						Explain privacy and the security of personnel data

UNIT 12: INFORMATION SECURITY MAINTENANCE Outcomes: Understand how to continually maintain your system you have implemented						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						List and Explain security management models
						Explain the Maintenance Model
						Explain the need for digital forensics
						Use various digital forensics tools

Projects Required:
None

Textbook:
Contact Bookstore for current textbook.

Materials/Equipment Required:
Student will need to have the ability to install various software packages.

Attendance Policy:
Students should adhere to the attendance policy outlined by the instructor in the course syllabus.

Grading Policy:
The grading policy will be outlined by the instructor in the course syllabus.

Maximum class size:
Based on classroom occupancy

Course Time Frame:
The U.S. Department of Education, Higher Learning Commission and the Kansas Board of Regents define credit hour and have specific regulations that the college must follow when developing, teaching and assessing the educational aspects of the college. A credit hour is an amount of work represented in intended learning outcomes and verified by evidence of student achievement that is an institutionally-established equivalency that reasonably approximates not less than one hour of classroom or direct faculty instruction and a minimum of two hours of out-of-class student work for approximately fifteen weeks for one semester hour of credit or an equivalent amount of work over a different amount of time, The number of semester hours of credit allowed for each distance education or blended hybrid courses shall be assigned by the college based on the amount of time needed to achieve the same course outcomes in a purely face-to-face format.

Refer to the following policies:

402.00 Academic Code of Conduct
263.00 Student Appeal of Course Grades
403.00 Student Code of Conduct

Disability Services Program:
Cowley College, in recognition of state and federal laws, will accommodate a student with a documented disability. If a student has a disability, which may impact work in this class which requires accommodations, contact the Disability Services Coordinator.