COWLEY COLLEGE
& Area Vocational Technical School

COURSE PROCEDURE FOR

Cyber Security Analyst, CySA+
CIS1758 3 Credit Hours

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

Catalog Description:

CIS1758 – Cyber Security Analyst, CySA+ (3 hrs)
This course will prepare students to take the exam for the CompTIA CySA+ certification. The topics will include various concepts and tools involved in the four domains of the CySA+ certification exam: Threat Management, Vulnerability Management, Cyber Incident Response, and Security Architecture / Tool Sets.

Prerequisites:
None.

Co-requisites:
None

Controlling Purpose:
This course is designed to prepare students to plan for prevention, recognize an incident, analyze the current incident, respond to the incident, and plan for prevention based on the results. This process involves using various cybersecurity tools.

Learner Outcomes:
Upon completion of the course, the student will be able to perform a reconnaissance, plan a response, plan a counter response, vulnerability identification, appropriate cyber incident response, and modification of network architecture in response to incidences.

Units Outcomes and Clock Hours of Instruction for Core Curriculum:
The following outline defines the minimum core content not including the final examination period. Instructors may add other material 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: Defending Against Cybersecurity Threats

Outcomes: Demonstrate knowledge of the appropriate response to a network-based threat along with techniques to secure a corporate environment.

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a network-based threat, implement or recommend the appropriate response and countermeasure.
						Explain the purpose of practices used to secure a corporate environment.

UNIT 2: Reconnaissance and Intelligence Gathering

Outcomes: Demonstrate the knowledge necessary to perform reconnaissance and intelligence gathering using various software tools and techniques

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
						Given a scenario, analyze the results of a network reconnaissance

UNIT 3: Designing a Vulnerability Management Program

Outcomes: Explain the process to analyze an entity for any vulnerabilities that may exist in the system and the appropriate response to the vulnerabilities.

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, implement an information security vulnerability management process.

UNIT 4: Analyzing Vulnerability Scans

Outcomes: Explain the process to analyze the scans of vulnerabilities along with common vulnerabilities that exist in an entity

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, analyze the output resulting from a vulnerability scan.
						Compare and contrast common vulnerabilities found in common targets within an organization.

UNIT 5: Building an Incident Response Program

Outcomes: Describe the development of an incident response program including impact analysis and communication during an incident

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
						Explain the importance of communication during the incident response process.

UNIT 6: Analyzing Symptoms for Incident Response

Outcomes: Explain the process of symptoms to identify that an incident has occurred and how this guides the appropriate response

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, analyze common symptoms to select the best course of action to support incident response

UNIT 7: Performing Forensic Analysis

Outcomes: Describe and build a toolkit for forensics analysis. In addition, use the toolkit on a simulated incident

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.

UNIT 8: Recovery and Post-Incident Response

Outcomes: Explain the process of summarizing the incident and planning an appropriate response given the severity of the incident.

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Summarize the incident recovery and post-incident response process.

UNIT 9: Policy and Compliance

Outcomes: Explain the how framework, common policies, controls, and procedures need to work together to help prevent and handle incidents

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Explain the relationship between frameworks, common policies, controls, and procedures.

UNIT 10: Defense-in-Depth Security Architectures

Outcomes: Explain how an incident should impact the security architecture of the entity including changes to prevent future incidents.

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, review security architecture and make recommendations to implement compensating controls.

UNIT 11: Identity and Access Management Security

Outcomes: Explain the possible remediation of identify and access management issues including the initial analysis of the original incident

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, use data to recommend remediation of security issues related to identity and access management.

UNIT 12: Software Development Security

Outcomes: Explain the various types of best practices for application security based on apply the Software Development Life Cycle

A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).

UNIT 13: Cybersecurity Toolkit Outcomes: Explain the purpose and usage of the popular cybersecurity tools and techniques						
A	B	C	D	F	N	Specific Competencies Demonstrate the ability to:
						Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.

Projects Required:
Varies, refer to syllabus.

Textbook:
Contact Bookstore for current textbook.

Materials/Equipment Required:
None

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 and which requires accommodations, contact the Disability Services Coordinator.