STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR 450 - CYBERSECURITY BODY OF KNOWLEDGE

Created by: Minhua Wang
Updated by: Minhua Wang

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
CENTER FOR CRIMINAL JUSTICE, INTELLIGENCE AND CYBERSECURITY
SPRING 2020

A. **TITLE**: CYBERSECURITY BODY OF KNOWLEDGE

B. **COURSE NUMBER:** CYBR 450

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

 # Credit Hours: 3
 # Lecture Hours: 3 **per week**
 # Lab Hours: **per week**
  Other: **per week**

Course Length: 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Fall or Spring

G. **COURSE DESCRIPTION:** This course provides a comprehensive, trustworthy framework of practices for assuring cybersecurity. It helps future security professionals understand how the various roles and functions within cybersecurity practice can be combined and leveraged to secure an organization. The course content is derived from the Department of Homeland Security's Essential Body of Knowledge (EBK) for IT Security and the International Information System Security Certification Consortium's Common Body of Knowledge (CBK).

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CITA 250 Information Security
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

Course Student Learning Outcome [SLO]	_PSLO_	_ISLO_
a. Specify fundamental concepts and components of Cybersecurity from both managerial and professional end user perspective	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
b. Summarize and compare Cybersecurity requirements for various types of decision making and planning strategies	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5

c. Evaluate the impact of Cybersecurity on society	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA] 4[ER] 5
d. Dissect foundations of Cybersecurity to the demands of electronic commerce, connectivity, and networked economy	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA, PS] 5
e. Recommend Cybersecurity solutions to specific electronic system implementations	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[O,W] 2[PS] 5
f. Identify examples of most current developments in Cybersecurity	6. Adapt to new situations and demands by applying and/or updating his/her knowledge and skills	5

KEY	Institutional Student Learning Outcomes [ISLO 1 – 5]
ISLO #	ISLO & Subsets
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA], Inquiry & Analysis [IA], Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit,/Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL], Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J.   APPLIED LEARNING COMPONENT: Yes__X___   No_____
- Classroom/Lab

K.   TEXTS: None

L.   REFERENCES: Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database

M.   EQUIPMENT: Computer lab classroom with virtual machine software installed

N. <u>**GRADING METHOD:**</u> A-F

O. <u>**SUGGESTED MEASUREMENT CRITERIA/METHODS:**</u>
- Exams
- Quizzes
- Participation

P. <u>**DETAILED COURSE OUTLINE:**</u>

I. INTRDUCTION TO ESSENTIAL BODIES OF KNOWLEDGE AND COMMON BODY KNOWLEDGE
        A. Essential Bodies of Knowledge
        B. Common Body of Knowledge

II. ESSENTIAL BODIES OF KNOWLEDGE ROLES AND REQUIRED CAPABILITIES
        A. The Executive role.
        B. The Functional role.
        C. The Corollary role.

III. ESSENTIAL BODIES OF KNOWLEDGE ROLES AND REQUIRED CAPABILITIES
        A. Data Security.
        B. Digital Forensics.
        C. Enterprise Continuity.
        D. Incident Management.
        E. IT Security Training and Awareness.
        F. IT Systems Operations and Maintenance.
        G. Network and Telecommunications Security.
        H. Personnel Security.
        I. Physical and Environmental Security.
        J. Procurement.
        K. Regulatory and Standards Compliance.
        L. Security Risk Management.
        M. Strategic Security Management.
        N. System and Application Security.

IV. COMMON BODY KNOWLEDGE DOMAINS
        A. Security and Risk Management.
        B. Asset Security.
        C. Security Engineering.
        D. Communication and Network Security.
        E. Identity and Access Management.
        F. Security Assessment and Testing.
        G. Security Operations.
        H. Software Development Security.

VIII. Other Topics: As Defined by the Instructor (The topics on most recent advanced Cybersecurity developments are strongly recommended.)

Q. <u>**LABORATORY OUTLINE:**</u> N/A