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

MASTER SYLLABUS

CYBR 354 - CYBER INCIDENT RESPONSE AND DISASTER RECOVERY

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**: CYBER INCIDENT RESPONSE AND DISASTER RECOVERY

B. **COURSE NUMBER:** CYBR 354

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 presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. It covers market-leading content on contingency planning, effective techniques that minimize downtime in an emergency, and ways to curb losses after a breach in case of a network intrusion.

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 incident response and disaster recovery	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 various methodologies in incident response and disaster recovery	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] 5
c. Recommend incident response and disaster recovery 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	2[CA, PS] 5

d. Exhibit example of most current developments in incident response and disaster recovery	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. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Exams
- Quizzes
- Participation
- Interactive lecture/lab

P. DETAILED COURSE OUTLINE:

I. Introduction to Cyber Incident Response and Recovery
   A. Incident Response.
   B. Incident Recovery.

II. Contingency Planning
   A. Planning for Organizational Readiness
   B. Data Protection Strategies for IR/DR/BC.

C. Incident Response Planning.
D. Computer Incident Response Teams.

III. Cyber Incident Response and Recovery Implementation
A. Incident Detection and Plan Activation.
B. Incident Response.
C. Incident Response Recovery and Preventative Maintenance.
D. Incident Response Forensics and eDiscovery.
E. Incident Recovery: Preparation and Implementation.
F. Business Continuity Planning and Implementation.
G. Crisis Management and Human Factors.

IV. Other Topics: As Defined by the Instructor (The topics on most recent Incident Response and Disaster Recovery developments are strongly recommended.)

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