Empire College
Business – Law – Technology – Medical

CLASS NUMBER AND NAME:	**CSN323— Cybersecurity Fundamentals 2**
TOTAL HOURS/ UNITS:	72 HOURS/5.0 UNITS
PREREQUISITES:	CSN313— Cybersecurity Fundamentals
TEXTS AND MATERIALS:	*CompTIA Cybersecurity Analyst (CSA+) Cert Guide* , Troy McMillan, Pearson education, 2017 (ISBN 9780789756954)
CLASS DESCRIPTION:	A combination of lecture, lab exercises, and hands-on training designed to provide the student with the knowledge and skills required to identify incidents in a network, create an incident response plan, lock down applications and create policies for secure network environment.
CLASS OBJECTIVES:	To provide the student with an in-depth knowledge of incident identification, response and recovery. Students will create policies for security , access management and incident response while creating a secure network architecture. Students will prepare for the CompTIA Cybersecurity Analyst exam (CSA+)
CLASS FORMAT OVERVIEW:	The class is conducted in lecture and instructor demonstrations, opportunity will be given for questions-and-answer discussion as well as tactile learning experiences. Time spent in preparation for or reflection on course lecture will approximate two hours outside of class for each lecture credit hour utilized by the instructor in delivery of the material and ¼ hour outside of class for each hour of structured lab time.
METHOD OF INSTRUCTION:	Each topic will be discussed thoroughly and will be supplemented with written materials. Class work and homework will give the student experiential opportunities.
ATTENDANCE:	It is expected that each student will be in class <u>when class begins.</u> Should the student arrive more than <u>five minutes late</u> they should notify the instructor of their presence, it will be up to the instructor to decide if the student has arrived in time to be counted as present- the instructor's decision is final. A minimum of 80 % attendance is required to complete this class. (Note:If a student misses more than this, he or she will not get a passing grade in this class!)It will be the student's responsibility to learn of any assignments given in class when absent. .

TESTING: Weekly tests will be given each week, with a module final exam on the last week of the module.

LATE TESTING: A late test will result in a 10% penalty (Tests start with a B). All retakes and late tests must be scheduled with the instructor in a timely manner.

GRADING POLICIES: The grading system for this module consists of the following:

Attendance, participation, professional attitude	10%
Homework	25%
Weekly exams	40%
End-of-module final	25%

ANTICIPATED LEARNING OUTCOMES: Upon completing this course, the student will be able to:

1. Create an incident response plan
2. Recover data systems after and attack.
3. Use frameworks to create policies, controls and procedures
4. Remediate security issues
5. Provide identity and access management
6. Crate a secure network architecture
7. Implement secure application practices
8. Use a wide spectrum of cybersecurity tools.

Week 6
Chapters 14
Homework due, review
Test

6 Week Tentative Schedule

CSN323

Week 1
Chapters 8
Homework due, review
Test

Week 2
Chapter 9
Homework due, review
Test

Week 3
Chapters 10
Homework due, review
Test

Week 4
Chapters 11 and 12
Homework due, review
Test

Week 5
Chapters 13
Homework due, review
Test