FITCHBURG STATE UNIVERSITY

These top fields will be completed by the SGOCE office.

Academic Year: * 2024-2025 SGOCE#: * 4

New Graduate Course Proposal

Form Procedure
To share the form with others prior to Submitting choose the **Save Progress** option at the bottom.
Create a PDF of the saved form go to Print and choose Save as PDF copy rather than print.
To access the saved form for editing or to finalize submission visit forms.fitchburgstate.edu to log in and view your Pending/Drafts under My Forms.

Course Title

Course Title: * Introduction to Cybersecurity

Proposed Banner Abbreviation: * Intro to Cybersecurity

Banner limit of 30 characters, including punctuation, spaces, and special characters.

Department/Committee Information

The main contact person for the Graduate Curriculum Committee should fill out this form.

Requestor Name: * Xuzhou Chen

Members of the Graduate Curriculum Committee: Brady Chen, Guy Karlebach, Natasha Kurtonina, Nadimpalli Mahadev, Hefei Qiu, Ricky Sethi

Department / Unit Developing: * Computer Science

Department Chair: * Dr. Nadimpalli Mahadev * nmahadev@fitchburgstate.edu

Academic Dean: Dr. Jannette McMenamy jmcmenamy@fitchburgstate.edu

Program Chair: The Program Chair for this request is among the people listed above.
* (•) Yes
( ) No

Graduate Program: * MS CS

The above program would be responsible for scheduling, staffing & assessing this course.

Course Information

Course Description

* This course will introduce students to basic cybersecurity concepts, including risk management, threats, vulnerabilities, and defense techniques. Topics include CIA, threats, attacks, defense, access control and password management, security policies, cyber resilience, physical security, end point security, cloud security, incident response and disaster recovery plan, risk assessment, and management.

Course Objectives

? Reasonable understanding of the fundamentals of the cyber-security domain and related issues
? Identify and define key knowledge areas of cybersecurity.
? Explain what to protect, why to protect, and create a plan to protect in the cyber world.
? Describe cybersecurity in the real world and apply their knowledge to scenarios to reflect technology's latest capabilities and trends.
? Explain concepts related to applied cryptography, including plain text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
? Explain the concepts of malicious code, including viruses, Trojan horses, and worms.
? Describe threats to networks, including sniffing and spoofing, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.

Rationale and expected outcomes of offering the Course

* The department is planning to create Cybersecurity concentration to address the growing demand for the cybersecurity professionals. As one of the required courses for the concentration, it provides students with introductory knowledge of basic cybersecurity concepts, including risk management, threats, vulnerabilities, and defense techniques.

What are the Learning Outcomes for the Course?

Upon successful completion of this course, students will
? have Reasonable understanding of the fundamentals of the cyber-security domain and related issues
? have demonstrated knowledge of identify and define key knowledge areas of cybersecurity.
? be able to explain what to protect, why to protect, and create a plan to protect in the cyber world.
? have the knowledge of and describe cybersecurity in the real world and apply their knowledge to scenarios to reflect technology's latest capabilities and trends.
?be able to explain concepts related to applied cryptography, including plain text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
? learn and explain the concepts of malicious code, including viruses, Trojan horses, and worms.
? be able to describe threats to networks, including sniffing and spoofing, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.

Number of Credits: * 3

Discipline Prefix or Prefixes: * CSC

Brief rationale if more than one prefix:

Level of Course: * (•) 7000 ( ) 8000 ( ) 9000

Brief rationale for level choice:: * Will serve as an introductory course for the Cybersecurity concentration

The course will be: [x] Requirement [x] Elective

Elective or Requirement Note/Special: Will be required for Cybersecurity concentration.

Is there a similar undergraduate course? * ( ) Yes (•) No

Does this course affect offerings in any other department or program? * ( ) Yes (•) No

Course Enollment

Expected Average Enrollment: * 20

This course is a replacement for: Course # / Name

Has the course been offered previously as a "Topics" course? * ( ) Yes (•) No

Is this an Extended Campus Course? * ( ) Yes (•) No

Which semester will this course be offered for the first time?: * Fall 2025

How often thereafter to be offered?: * Every year

Course Requirements

Prerequisite course(s) if any:

Additional Requirements

Laboratory Hours:

Fieldwork Hours:

Pre-Practicum Hours:

Practicum Hours:

Other Requirements (specify):

Syllabus Upload

New Course Syllabus Upload: Syllabus Cyber.docx

Signatures

*Click on the **Submit Form** button at the bottom of the page after you have signed the form.*
You should receive an email confirmation that your signature has been completed.

...3236343639
Xuzhou Chen — Requester Signature — 11/17/2024 — Date

...3733333831
Jannette McMenamy — Academic Dean Signature — 11/20/2024 — Date

...3632353831
Nadimpalli Mahadev — Department Chair Approval — 11/18/2024 — Date

...3939323433
Becky Cooper Gleng — SGOCE Dean Signature — 11/22/2024 — Date

Graduate Council

The Graduate Council Chair Signature indicates that the Council has discussed this proposal and has decided it should move forward.

Graduate Council Chair Signature _____ Date _____

Notifications

Approval of the President _____ Date _____

SGOCE Dean Initials _____ Date _____

Reviewed by the Registrar: _____ Date _____

Introduction to Cybersecurity

COURSE DESCRIPTION:
This course will introduce students to basic cybersecurity concepts, including risk management, threats, vulnerabilities, and defense techniques. Topics include CIA, threats, attacks, defense, access control and password management, security policies, cyber resilience, physical security, end point security, cloud security, incident response and disaster recovery plan, risk assessment, and management.

Required Textbook: None

Recommended resources:

CompTIA Security+ Get Certified Get Ahead: SY0-701 Study Guide, by Joe Shelley (Author), Darril Gibson, 979-8988984801

COURSE OBJECTIVES:

Upon successful completion of this course, you will have demonstrated knowledge of:

- Reasonable understanding of the fundamentals of the cyber-security domain and related issues
- Identify and define key knowledge areas of cybersecurity.
- Explain what to protect, why to protect, and create a plan to protect in the cyber world.
- Describe cybersecurity in the real world and apply their knowledge to scenarios to reflect technology's latest capabilities and trends.
- Explain concepts related to applied cryptography, including plain text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
- Explain the concepts of malicious code, including viruses, Trojan horses, and worms.
- Describe threats to networks, including sniffing and spoofing, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.

GRADING POLICY:

Grades will be posted on Blackboard throughout the semester to provide an ongoing assessment of student progress, though the final assessment will be measured using the weighted average above. Once a grade is posted on Blackboard, students have two (2) weeks to dispute the grade.

Your course grade will be a weighted average according to the following:

Lab Assignments	60%
Final Exam	15%
In-Class Activities/Quizzes/Discussion/Presentation	25%

Homework: Homework will be assigned based on material from the lectures. These assignments are meant for you to become familiar with the course material.

Lab Assignments: Labs are an integral part of this course and are intended to provide experience in the application of the design techniques discussed in the lectures. These labs are meant to be individual assignments, so you should work on these alone unless explicitly directed otherwise by your instructor.

In-Class Activities/Quizzes/Discussion: These grades will be based on in-class assignments or short quizzes or discussions, which may be given at any time during the class without any prior notice.

Note: No late assignments will be accepted, so please make sure that you complete and submit all assignments on time.

GRADING SCALE

Letter Grade	Numerical Range	Grade Pt. Value
A	93-100	4.00
A-	90-92	3.67
B+	87-89	3.33
B	83-86	3.00
B-	80-82	2.67
C+	77-79	2.33
C	73-76	2.00
C-	70-72	1.67
D	60-69	1.00
F	0-59	0.00

ACADEMIC INTEGRITY:

Academic integrity is central to the mission of educational excellence at Quinnipiac University. Each student is expected to turn in work completed independently, except when assignments specifically authorize collaborative effort. It is not acceptable to use the words or ideas of another person--be it a world-class philosopher or your lab partner--without proper acknowledgment of that source. This means that you must use footnotes and quotation marks to indicate the source of any phrases, sentences, paragraphs, or ideas found in published volumes, on the internet, or created by another student. Anything generated by AI tools like ChatGPT, Google Bard, Bing, etc. if used for class work, must be clearly mentioned. I have a zero-tolerance policy for cheating, and all violations will result in substantial penalties. Any form of academic dishonesty may be penalized with a failing grade ("F") in the class. Additionally, violations may be referred to the Office of Academic Innovation and Effectiveness for further disciplinary action. If you have any doubts or questions about what constitutes academic misconduct, please do not hesitate to contact me.

SYLLABUS REVISIONS

This syllabus may be modified as the course progresses should the instructor deem it necessary. Notice of changes to the syllabus shall be made through Blackboard and/or class announcements.