FITCHBURG STATE UNIVERSITY

These top fields will be completed by the SGOCE office.

Academic Year: * 2024-2025 SOGCE #: * 7

New Graduate Program 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.

Program Request Information

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

Title of New Program: * Cybersecurity Concentration for Master of Computer Science Program

Department / Unit Developing: * Computer Science

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

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

Requestor Name: * Xuzhou Chen

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

Program Chair

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

Program Details

New Program and/or New Concentration:

- [ ] New Program
- [x] New Concentration

Type of Program: *(check all that apply)*

- [ ] Certificate
- [ ] Teacher Licensure
- [x] Degree

Catalog Description
Briefly describe new program/concentration as it will appear in university catalog:

* The Cybersecurity concentration offers students the opportunity to develop the necessary skills and knowledge to pursue careers in the field of cybersecurity such as network security, ethical hacking, digital forensics, and other related areas. It will provide the students with the necessary skills and knowledge in keeping computer systems and electronic data safe.

The concentration will be built on the core requirements for MS CS by directing the section of CSC 7000+ free electives towards cybersecurity. Students who choose the cybersecurity concentration will be required to take the following 4 courses besides the existing 6 required core courses:
CSC 7XXX Introduction to Cybersecurity
CSC 8025 Computer & Network Security
CSC 8026 Ethical Hacking
CSC 8027 Digital Forensics

Learning Outcomes
List the Student Learning Outcomes for the program.

Enrollment & Implementation

A Cohort Model will be used: * ○ Yes ◉ No

Additional faculty will be needed (day/adjunct) * ◉ Yes ○ No

The Program is expected to begin: * Fall * 2025

Semester Year

Population Description
Anticipated enrollment/staffing plan *(i.e., Who/how many will program serve?)*

*The concentration will serve the
1. Students who are interested in pursuing MS CS with a career goal in cybersecurity area, e.g. Information Security Analyst, Security Engineer, Cybersecurity Administrator, or Information security Specialist.
2. Students who are currently working in computer and/or IT industry and would like to pursue career in cybersecurity area or increase the competitiveness in their workplaces.

Rationale
Rationale and expected outcomes for new program:

*Data are everywhere. As more companies, organizations, government agencies, and individuals rely on these data for their routine business, there is growing demand for cybersecurity professionals and specialists. Students will have the ability of the following:
- Understand the fundamentals of the cyber-security domain and related issues
- Identify and define key knowledge areas of cybersecurity.
- Identify cyber threats, assess risks, design and implement security solutions
- 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.
- Describe some classical encryption/decryption techniques.
- Understand the basic principles and distinct uses of public-key cryptosystems.
- Implement some modern encryption/decryption algorithms such as DES, AES, RSA, and etc.
- 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.
- Analyze data to detect attacks, communicate security concerns effectively
- Understand cybercrimes and the tools used to recover and/or repair stolen or damaged data files.
- Understand the concept of Windows, Linux, Macintosh File Systems, forensics tools, the identification, preservation, collection, examination, analysis, and presentation of evidence.
- Learn to explore the vulnerabilities in various systems and operate the industry-leading tools and framework to perform penetration testing on different target systems.
- Stay updated on emerging cyber threats, all while applying critical thinking and problem-solving skills to protect sensitive information and systems within an organization

Resources
Library and other resources needed:

*No additional library resources needed. We may need to hire more adjunct faculty to help cover additional courses

Admissions
Describe program's admissions requirements:

*No additional admissions requirements are needed.

Implementation Plan
Describe how the new program will begin; will it be phased in; suggested execution:

*We plan to offer the concentration in Fall 2025. Here is the detailed schedule for course offerings:
Fall 2025:
CSC 7XXX Introduction to Cybersecurity (Robin Chataut)
CSC 8027 Digital Forensics (Md Masud Rana)
Spring 2026:
CSC 8026 Ethical Hacking (Mohamed Meky)
CSC 8025 Computer & Network Security (Md Masud Rana or Brady Chen)

Supporting Documentation

A plan of study must be included.
If new courses are proposed or major changes are made to existing courses, submit a Graduate Council New Course Approval form.
Attach any letter(s) of support from professional agencies or others within or outside the university.

Attach an approved Plan of Study: *Sample Template.pdf Supporting Documentation:

CIP Code

List the CIP code you would like associated with the program.
For a list of possible CIP codes to choose from visit nces.ed.gov/ipeds/cipcode.
NOTE - all CIP codes will be reviewed and approved by the Office of Institutional Research for final confirmation.

Proposed CIP Code: * 43.0303, 29.

* (•) Yes Institutional Research is this the ideal code?
( ) No

Signatures

...3630363938
Xuzhou Chen — 11/25/2024
Requester Signature: Date

...3136393937
Jannette McMenamy — 11/26/2024
Academic Dean Signature: Date

...3937383838
Nadimpalli Mahadev — 11/26/2024
Department Chair Approval: Date

...3231363031
Becky Cooper Glenz — 11/26/2024
SGOCE Dean Signature: 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

Institutional Research has checked the CIP Code.

Institutional Research Signature — Date

Notifications

Approval of the President — Date

SGOCE Dean Initials — Date

Reviewed by the Registrar: — Date

Cybersecurity Concentration for Master of Computer Science Program

Old Plan of Study			**New Plan of Study**		
Required Courses **Course number: Title of Course**	Pre-practicum Hours	Credits	**Required Courses** **Course number: Title of Course**	Pre-practicum Hours	Credits
CSC 7050 - Theory of Computation		3	CSC 7050 - Theory of Computation		3
CSC 7400 - Object Oriented Analysis and Design		3	CSC 7400 - Object Oriented Analysis and Design		3
CSC 8050 - Design and Analysis of Algorithms		3	CSC 8050 - Design and Analysis of Algorithms		3
CSC 7013 - Advanced Mathematics for Computer Scientists		3	CSC 7013 - Advanced Mathematics for Computer Scientists		3
CSC 7014 - The Practice of Computer Programming		3	CSC 7014 - The Practice of Computer Programming		3
CSC 7132 - Operating Systems and Networking		3	CSC 7132 - Operating Systems and Networking		3
Students select minimum of 15 credit hours of graduate level courses with advisor approval		15	• CSC 7XXX Introduction to Cybersecurity (3 cr.) • CSC 8027 Digital Forensics (3 cr.) • CSC 8026 Ethical Hacking (3 cr.) • CSC 8025 Computer & Network Security (3 cr.) • One 3 credit hour course approved by advisor		15
TOTAL CREDITS FOR PROGRAM		33	**TOTAL CREDITS FOR PROGRAM**		33