Minor: CYBERSECURTIY MINOR

_____

Student's Last Name   First Name   Middle Initial

_____

Advisor   Date Major Declared

Course #	Title of Course	Hours Required	Semester Completed	Grade
Required Courses:				
CBR 110	Introduction to Cybersecurity	3		
CBR 220	Information Security	3		
CSA 250	IT Infrastructure	4		
CBR 360	Cyber Law and Ethics	3		
CBR 415	Information Security Policy	3		
CBR 470	Cybersecurity Capstone	1		
	3-hour elective course pre-approved by the CBR minor advisor selected from a discipline other than CBR and related to the field of cybersecurity and the capstone project.	3		
	TOTAL HOURS FOR MINOR	**20 hrs**		

If any substitutions or waivers of requirements are allowed, please list below and initial.

_____

_____

Advisor Signature: _____   Department Chair Signature: _____

Contact: Dr. Linda Webster, Chair   Assistant Professor: C. Cox
Email: linda.webster@wcmo.edu   Instructor: C. Webster
                                               Visiting Professor: R. Manfredi

A minor in Cybersecurity will enhance the skills of students in any discipline by preparing them to be knowledgeable consumers of digital resources and aware of the associated risks. The issue of Cybersecurity is not unique to any one type of organization. Businesses, nonprofit organizations, and governments all face security issues related to computing technology. Social organizations, clubs, and political groups face similar issues. Students who complete a minor in Cybersecurity will be prepared to identify cyber risks to an organization and work with information technology security specialists to protect the digital assets of that organization. All disciplines rely on digital communication, digital files, and other digital assets; thus, the Cybersecurity program will be relevant to a student in any discipline who is interested in protecting digital assets of an organization.

CBR MINOR LEARNING OBJECTIVES:

Students graduating with a minor in Cybersecurity will be able to:
- Identify cybersecurity risks facing different types of organizations.
- Explain security strengths and weaknesses of different infrastructure and policy components of an organization.
- Work with IT security staff to design, implement, and evaluate security policies.
    Demonstrate the integration of cybersecurity concepts within a specific discipline through capstone project