## **CYBR 495A: Cybersecurity Design Project A (1 credit)**

This course is a project-based course that allows students to apply their knowledge and skills in cybersecurity to a practical project. The course focuses on developing a cybersecurity solution to a real-world problem, and students work in teams to design and implement a comprehensive cybersecurity solution. *(Prerequisite: Senior Level (90 Credits), and GPA greater than or equal 2.0)*

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Define a clear problem statement, objectives, and scope for the cybersecurity design project.

A2. Conduct a comprehensive literature review and a solid technical background relevant to the cybersecurity design project.

B1. Analyze cybersecurity problems using appropriate computing principles, theories and concepts.

B2. Develop a proof of concept/prototype for the proposed cybersecurity design project.

B3. Communicate effectively the cybersecurity design project both in written and oral forms to diverse stakeholders.

C1. Develop a detailed project plan outlining task, timelines, resource requirements, and milestones.

C2. Assess the ethical implications of the cybersecurity design project, considering social, environmental, and professional responsibilities.

C3. Collaborate effectively with team members from diverse backgrounds to address complex cybersecurity challenges and meet project objectives.

**Course Learning Materials:**

* There are no specific textbooks required for Cybersecurity Design Project A, as the focus is on practical application of cybersecurity concepts and theories. However, students may be required to read and study relevant cybersecurity materials related to their project.

**Course Content:**

The specific topics covered in Cybersecurity Design Project A will vary depending on the nature of the project chosen by the students. However, typical topics may include:

1. Identification and analysis of cybersecurity risks and threats
2. Development of a comprehensive cybersecurity solution
3. Network and system design and implementation
4. Cryptography and data protection
5. Incident response and recovery planning
6. Compliance and regulatory requirements
7. Communication and documentation of the project.