**Course SLOs (Student Learning Outcomes) are below**

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

1. Identify and analyze common security threats across software systems.
2. Apply secure coding practices in software development.
3. Perform risk assessments using standard cybersecurity frameworks.
4. Use industry tools to detect and mitigate vulnerabilities.
5. Communicate technical security issues clearly in written and verbal formats.
6. Work collaboratively on technical projects in a team environment.
7. Demonstrate ethical decision-making in cybersecurity scenarios.

**Technical Requirements are**

Students must have:

* A working laptop with admin rights
* Access to Canvas and Zoom
* Installed Python, Git, and a code editor (e.g., VS Code)
* Basic Linux terminal knowledge is helpful but not required

**Assignments & Delivery -** Students will complete a variety of assignments designed to reinforce course content and develop practical skills:

* **Weekly Quizzes** (10 total): Delivered through Canvas. Timed and auto-graded.
* **Hands-on Lab Reports**: Submitted as PDFs after each lab session via Canvas.
* **Midterm Project**: Team-based assignment focused on secure software development, submitted through GitHub.
* **Final Presentation**: Delivered live via Zoom and accompanied by a visual slide deck.
* **Participation**: Includes in-class discussions, peer reviews, and real-time engagement in labs.

All submissions are due by **Sunday at 11:59 PM**, unless otherwise stated.