CIS 226: INTRO TO INFO ASSURANCE

Class Schedule:	Tuesday, Thursday 11am to 12:50pm
Instructor:	Chad Johnson
Office:	SCI B231
Phone:	715-346-2021
Email:	Chad.Johnson@uwsp.edu
Office hours:	Mondays and Wednesdays, 11am to 1:50pm

COURSE DESCRIPTION

This course will provide an overview of the field of Information Assurance, which includes aspects such as IT governance, data security, risk management, and threat assessment. It will cover data security from both a penetration testing and endpoint security perspective, and will focus on understanding industry standards, terms, and tools to provide a comprehensive introduction to the world of Information Assurance.

COURSE OBJECTIVES

- Understand Information Assurance topics and parlance.

- Understand the role of IT policy from a governance perspective and understand the elements of data security policies.

- Identify key concerns with federal and state regulations concerning data security (FERPA, HIPAA, SOX, etc.)

TEXTBOOK

- We will be using open-source texts, posted to Canvas.

LECTURES

- Lecture notes will be posted on Canvas. I make every effort to make my notes available, but I may decline to include them at my discretion.

- Students are strongly encouraged to attend each class and actively participate in class discussions.

- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

GRADING

- 4 Exams: 60% (15% each)
- 8 Labs: 40% (5% each)

Final grades will be assigned according to the following scale:

A: score >= 90	A-: 87 <= score < 90	
B+: 83 <= score < 87	B: 80 <= score < 83	B-: 77 <= score < 80
C+: 73 <= score < 77	C: 70 <= score < 73	C-: 65 <= score < 70
D: 60 <= score < 65		
F: score < 60		

Scale may be adjusted, depending on the overall performance of the class.

ASSIGNMENTS AND DEADLINES

- Labs will be a variety of tasks. Some may require writing a short paper. Others might require completing multiple steps to achieve a goal (as in a CTF.) Each assignment will have those expectations detailed in the assignment instructions.
- Exams are open note/book, and you can use the Internet to search for answers. Please do not collaborate on them. They are not group assignments. You will have the week to complete the exam. Two attempts. Questions will be randomly chosen from a bank. Multiple-choice, multi-select, and true/false only. If you miss an exam, it cannot be made up.

OFFICE HOURS POLICY

- I prefer that you contact me via email.
- However, you are still welcome to my office to ask me any questions at any other times.
- I fear the phone.
- Virtual office hours will be posted to Canvas or you can just make an appointment with me through Bookings.

REGRADING

Grades will be posted in Canvas. After the scores are announced, you have 7 days to request regrading by contacting the instructor (office hours or email). Your grade will be final after 7 days.

CANVAS

The Canvas URL is https://canvas.uwsp.edu. Use your UWSP NetID and password to login. We use Canvas for everything from important announcements, instructions, assignment submissions, and grades.

ACADEMIC HONESTY:

The university cannot and will not tolerate any form of academic dishonesty by its students. This includes, but is not limited to cheating on examinations, plagiarism, or collusion. **Any form of academic dishonesty may lead to F grade for this course. I assure you I take this extremely seriously.**

STUDENTS IN NEED OF ACCOMODATIONS:

If you require accommodation based on disability, please let me know. I am willing to provide any reasonable accommodation you require. The sooner you inform me the better.

RECORDED LECTURES:

I may record lectures and post them online. I do this as a convenience for students, not as an obligation. Online postings aren't a substitute for regular attendance of class, and I make no guarantee that they will be complete or available.

TENTATIVE SCHEDULE

Week	Lecture Topics	Due
1	Introduction & Syllabus	
2	Information Assurance Fundamentals	Lab 1
3	The CIA Triad	Lab 2
4	Information Quality vs Value	Exam 1
5	Security Controls	
6	Malware Taxonomy and AV	Lab 3

7	Exploits and Mitigation	Lab 4
8	Passwords	Exam 2
9	Access Control Models	Lab 5
10	Security Frameworks	
11	Compliance	Lab 6
12	Encryption	Exam 3
13	Application Control	
14	Firewalls	Lab 7
15	Case Studies in Security	Lab 8
16	Finals Week	Exam 4