Course Syllabus

[Jump to Today](https://oit.instructure.com/courses/15104/assignments/syllabus)

**Syllabus**

**CYB201: Cybersecurity Fundamentals  
Spring 2022**

**Professor:**Amy McLaughlin  
**Delivery:** Asynchronous online through Canvas  
**Email:**[amy.mclaughlin@oit.edu](mailto:amy.mclaughlin@oit.edu) (or use mail inside canvas)  
**Office Hours:**Contact me via email to schedule zoom office hours

**Course Overview**

This course is provided 100% online and is offered in an asynchronous modality.  I will post recorded lectures, videos, and class information online in Canvas.  All discussions, assignments and tests will be conducted through the Canvas classroom.

This course aims to introduce fundamental concepts used in Cybersecurity. Topics include:

* Threats, attacks, and vulnerabilities
* Confidentiality, integrity and availability (CIA Triad)
* Common cybersecurity  technologies and tools
* Security architecture and design principles
* Identity and access management (IAM)
* Risk management, and
* Cryptography

**Prerequisites:**None

**Textbooks/Learning Resources**

Required Textbook:

Security in Computing, Fifth Edition  
Authors: Charles P Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies

Publisher: PEARSON

ISBN10: 0134085043

ISBN 13: 9780134085043

**Course Structure**

This course is offered 100% online and is taught in an asynchronous format, so there are no specific class dates.  Assignments must be submitted on time each week and students are expected to stay on track with completing the course activities.

**Grades**

Course grades will be calculated based on the scores in each of these categories:

* Discussions
* Assignments/Labs
* Quizzes & Final Exam

Letter grades will be based on the following scale:

* 90-100% = A
* 80-89% = B
* 70-79% = C
* 60-69% = D
* <60% = F

**Due Dates**

Assignments are due by 11:59pm on Saturday each week, except for the Final Exam which is due on Wednesday. It is ultimately the students’ responsibility to know what is due and when it is due. Class attendance is important for your success – please plan to log in at least 3 times per week and stay on track to complete your coursework

**Late assignments may be accepted with a points penalty for up to 3 days.**In the event that you have an illness or emergency that impedes your ability to participate in class, please reach out and contact me as early as possible so we can identify a strategy for you to successfully stay on track in class.

**Learning Outcomes**

* Students will be able to describe potential system attacks and the actors that might perform them
* Students will be able to describe cyber defense tools, methods, and components.
* Students will be able to identify bad actors in cyberspace and compare their resources, capabilities/techniques, motivations, aversion to risk.
* Students will be able to describe different types of attacks and their characteristics
* Students will be able to list the first principles of security
* Students will be able to describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
* Students will be able to analyze common security failures and identify specific design principles that have been violated
* Students will be able to describe how identification, authentication, authorization, and accounting can be used to provide system security
* Students will be able to identify the elements of a cryptographic system
* Students will be able to describe the difference between symmetric and asymmetric algorithms
* Students will be able to describe which cryptographic protocols, tools and techniques are appropriate in a given situation
* Students will be able to describe how cryptography can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.
* Students will be able to describe the common security models of database management systems
* Students will be able to identify and describe common concerns in database management systems
* Students will be able to describe the various concepts in network defense.
* Students will be able to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)
* Students will be able to describe each type of service/model of cloud computing
* Students will be able to list the applicable laws for compliance in a given situation
* Students will be able to describe the characteristics of malware
* Students will be able to identify malware
* Students will be able to apply tools and techniques for identifying vulnerabilities

**Couse Outline**

|  |  |  |
| --- | --- | --- |
| **Week** | **Topic** | **Reading** |
| 1 | Introduction to basic concepts and fundamentals of cybersecurity | Chapter 1 |
| 2 | Networks: Threats and vulnerabilities in wired and wireless networks and network protections | Chapter 6 |
| 3 | Operating systems and operating system vulnerabilities | Chapter 5 |
| 4 | Authentication capabilities and limitations Implementation of access control Employing encryptions | Chapter 2 |
| 5 | Programs and Programming: Malicious code, programming oversights and vulnerabilities, protecting code | Chapter 3 |
| 6 | Web Security: Attacks targeting end users | Chapter 4 |
| 7 | Databases: key database terms, security requirements, and database vulnerabilities | Chapter 7 |
| 8 | Cloud Computing: Risks, opportunities and security tools for cloud environments | Chapter 8 |
| 9 | Security planning and Risk Analysis | Chapter 10 |
| 10 | Cryptography - Symmetric and asymmetric encryption, algorithms, and more | Chapter 12 |
| 11 | Final exam |  |

**General Course Policy Statements**

**Academic Integrity**

Students are expected to demonstrate their knowledge with honesty and integrity. Oregon Tech considers academic dishonesty to be an unacceptable practice. The complete Oregon Tech Student Academic Integrity Policy is available on the Oregon Tech website.

**Dropping the Course**

Please note that it is your responsibility to drop the course via Web for Students.  If you decide you must drop the course, you will need to do so by the close of the fifth calendar day of term (Friday) in order to receive a full 100% refund.  Refunds decrease the longer you wait to drop the course.

**Incomplete Grades**

In order to be eligible for an "Incomplete" grade, Oregon Tech policy requires that students must have completed 80% of all coursework by the time grades are due at the end of finals week. An incomplete is not automatic and is arranged at the discretion of the instructor.  FI you have a personal matter preventing you from completing the course and have successfully completed most of the coursework, please contact me as soon as possible.

**OIT Disability Statement**

Students with a documented disability who require assistance or academic accommodations should contact the office of Disability Services immediately to discuss eligibility. Disability Services staff are located on both the Klamath Falls and Wilsonville campuses, however, arrangements can be made to meet with a student on any campus.  Meetings are by appointment only, so please contact the Disability Services office at the campus closest to you.  Klamath Falls 541.885.1790 and Portland Metro 503.821.1308.  This link leads to the department's website: <https://www.oit.edu/academics/cares/access-campus-equity-services>