



## **COMPUTER ENGINEERING V: Cybersecurity and Hacker Defense**

*Fairfield Ludlowe High School - Fairfield Warde High School*

---

**Full Year**

### **COURSE DESCRIPTION**

---

This course is the continuation of Computer Engineering 4. Students will learn how to construct, manage, use and defend a server in this culminating level course. This course will dive into computer and cyber security. Students will further develop, analyze, and apply skills related to Security + certification. Focus in this course will be on advanced networking, network security and hardware as well as encryption, security and managing a Windows server. Students will learn to protect a system from viruses and thwart hackers. The content of this course is aligned with CompTIA Security+ standards.

### **COURSE OBJECTIVES**

---

Students will be able to:

- Evaluate their own and others' digital footprint.
- React to cyberbullying scenarios.
- Given a scenario, distinguish the type of hacker or the ethics of that hacker.
- Identify and demonstrate appropriate use of artificial intelligence.
- Explain risk as it relates to Communication systems and business.
- Define risk management concepts and framework.
- Explain how risk is assessed.
- Define Cryptography
- Explain and create a symmetric Cryptography
- Explain and create asymmetric Cryptography
- Explain difference between Hashing Algorithms
- Explain cryptographic attack strategies
- Determine attackable data
- Understand attack scenarios
- Explain the meaning of the 3 A's (Authentication, Authorisation, Accounting)
- Describe how Access is managed on networked systems.
- Explain how Accounts are managed on networked systems.
- Explain Point-to-point Authentication
- Utilize operating system utilities
- Scan a network
- Monitor a network using applicable tools.
- Identify ways AI can be used to improve security and efficiency on a network.
- Identify vulnerabilities given relative system information.
- Identify the proper protocol for security breaches.
- Identify ways AI can be used to improve security and efficiency on an individual device.
- Set up a LAN network and its necessary hardware.

- 
- Establish a security system for a LAN network.
  - Set up a wireless network
  - Establish correct secure protocols for a network.
  - Given a scenario, defend a wireless network from an attack.
  - Select and implement the correct secure protocol for a given situation.
  - Set up a secure web application.
  - Defend a web application from an attack
  - Distinguish between pieces of hardware.
  - Identify security risks of a given hardware piece or application.
  - Calculate the risk based on a given scenario and set of parameters.
  - Employ digital forensic techniques to a given scenario.
  - Provide security advice based on an example of businesses security needs.
  - Manipulate databases with SQL and PHP commands.

## UNITS OF STUDY

---

- Unit 1: Ethics, Digital Citizenship and Computer Insecurity (3 weeks)
- Unit 2: Risk Management (3 weeks)
- Unit 3: Cryptography (3 weeks)
- Unit 4: Identity and Access Management (3 weeks) Unit 5: Network System Structure (3 weeks)
- Unit 6: Securing Devices and Individual systems (3 weeks)
- Unit 7: LAN Setup and Security (3 weeks)
- Unit 8: Securing Wireless Networks (3 weeks)
- Unit 9: Secure protocols (3 weeks)
- Unit 10: Network Security Testing (3 weeks)
- Unit 11: Responding To Network Security Incidents (3 weeks)
- Unit 12: Coding for Networks (SQL and PHP) (3 weeks)

## COURSE POLICIES AND REQUIREMENTS

---

**GRADING:** See district policy ([Policy 6146.1AR](#))

### Grading Communication

- Specific grading expectations and practices will be communicated to all students and families at the start of the school year via a consistent format.
- If students or parents have questions about grading practices, they should follow the district's established chain of command structure (see district website) with the first contact being to the teacher and then to the school administration.
- Buildings will send out reminders of the importance of checking students' grades in the Grading Portal with directions.
- Teachers will notify guardians when students fall into the F range after October 1st.

### Grade Reporting

- For a processed piece or "chunked" assignments that are part of a larger task, feedback and the grade shall be shared before the next step in the process, so long as students have submitted their work at those checkpoints, on time.
- Grades for summative assessments shall be entered within 10 school days from the date of submission or the date it was due, whichever is later. Grades for formative assessments shall be entered within 5 school

---

days from the date of submission or the date it was due, whichever is later, and prior to any subsequent assessment.

#### Guidelines for Late Work :

- Teachers will accept late work for both summative and formative tasks beyond the due date.
- Teachers will not accept late work beyond the deadline for late work. The deadline is defined as the next class period from the due date of the assignment or the alternative date that the teacher and student may agree upon depending on individual circumstances.
- Teachers may reduce the total points students can achieve as a penalty for late work up to the deadline. Students will earn a zero (0) if the assignment is not submitted or is submitted after the deadline.
- Late work only consists of assignments with an expected due date. Assessments, such as tests, quizzes and in class assignments, must be taken on the scheduled date except in cases of make-up assessments due to an excused absence.

#### REASSESSMENT GUIDELINES:

Eligibility of assessments	Teachers of the same course will determine which summative assessments are eligible. Students can select any part of a project to reassess. Reassessments may not be allowed one week before the end of a term.
Process	Students have two class periods in which to indicate they would like to take a reassessment. Teachers will make clear to students their preferred method for students to request reassessment ( <i>e.g.</i> email or filling out a simple form/spreadsheet).
Frequency	Students will have the opportunity to reassess on two summatives per year but not more than one per term (quarter).
Assessment Format	Based on discussion between the student and teacher, students will revise portions of the original assessment in which they did not show proficiency.
Gradebook impact	Original and reassessment scores will be averaged in the gradebook.

#### MATERIALS:

- As provided by the course.

#### EXPECTATIONS OF STUDENTS:

- Be Tech and Learning Ready: Come prepared with all necessary materials, including your charged device and any required software.
- Prioritize Safety: Follow all safety guidelines and procedures, especially when working with tools, equipment, or hazardous materials.
- Participate Actively: Engage in class discussions, ask questions, and contribute to group projects. Actively participate in lab activities by following instructions, working collaboratively, and cleaning up your workspace.
- Respect the Digital Realm: Treat all digital resources and equipment with care. Avoid actions that could harm or disrupt the learning environment.
- Embrace Digital Citizenship: Use technology ethically and responsibly. Be mindful of copyright laws and online etiquette.

#### EXTRA HELP:

- Students should seek out extra help when needed. The teacher is available for extra help before and after school as well as during prep periods.

