AP Cybersecurity

2026-2027 Course Syllabus

Instructor: Justen Early

Weeki Wachee High School
Email: early_j@hcsb.k12.fl.us
Course: AP Cybersecurity
Length: Full Year
College Board Course: AP Cybersecurity (Career Kickstart Program)

Course Description

AP Cybersecurity is a college-level course designed to introduce students to the principles and practices of cybersecurity. Students will learn how organizations identify, assess, mitigate, and detect cyber risks through a defense-in-depth security strategy. The course explores threats, vulnerabilities, attacks, security controls, authentication, networking, encryption, digital forensics, and artificial intelligence applications in cybersecurity. Students will engage in hands-on labs, simulations, collaborative projects, and authentic cybersecurity scenarios modeled after industry practices.

Successful completion of the course prepares students for the AP Cybersecurity Exam and provides foundational skills aligned with the NICE Workforce Framework and cybersecurity career pathways.

Instructor Contact Information

Teacher: Justen Early
Email: early_j@hcsb.k12.fl.us

Students and parents are encouraged to contact the instructor regarding course questions, grades, assignments, or academic support.

Course Objectives

Students will:

- Analyze cybersecurity risks and vulnerabilities.
- Develop mitigation strategies using layered security controls.
- Detect attacks through log analysis and monitoring tools.
- Collaborate effectively using professional cybersecurity practices.
- Utilize AI responsibly as both a cybersecurity defense and collaboration tool.
- Apply cybersecurity concepts to authentic real-world scenarios.
- Prepare for and successfully complete the AP Cybersecurity Exam.

AP Cybersecurity Skills

Throughout the year students will develop proficiency in:

Skill 1: Analyze Risk

- Identify vulnerabilities and threats
- Evaluate likelihood and impact of attacks
- Document cybersecurity risks

Skill 2: Mitigate Risk

- Implement security controls
- Develop defense-in-depth strategies
- Configure protective measures

Skill 3: Detect Attacks

- Analyze logs and evidence
- Monitor systems
- Identify indicators of compromise

Skill 4: Collaborate

- Work effectively in teams
- Communicate cybersecurity findings
- Utilize AI tools ethically and responsibly

Course Units

Unit 1: Introduction to Security

Approx. 10 Class Periods

Topics:

- Social Engineering
- Password Attacks
- Public Network Security
- AI-Powered Cyber Attacks
- AI in Cyber Defense

Unit 2: Securing Spaces

Approx. 21 Class Periods

Topics:

- Cybersecurity Foundations
- Physical Vulnerabilities
- Physical Security Controls
- Detecting Physical Breaches

Unit 3: Securing Networks

Approx. 26 Class Periods

Topics:

- Network Vulnerabilities and Attacks
- Wireless Security
- Network Segmentation
- Firewalls
- Intrusion Detection Systems

Unit 4: Securing Devices

Approx. 23 Class Periods

Topics:

- Malware and Device Attacks
- Authentication
- Device Security Controls
- Endpoint Detection and Response

Unit 5: Securing Applications and Data

Approx. 30 Class Periods

Topics:

- Application Vulnerabilities
- Access Controls
- Cryptography
- Public Key Infrastructure
- Secure Software Design
- Data Protection and Monitoring

Grading Policy

Student grades will be calculated as follows:

Category	Weight
Class Participation / Professionalism	10%
Class & Lab Projects	50%
Nine Weeks Exam	10%
Classwork & Daily Assignments	30%

Participation / Professionalism Includes:

- Daily engagement
- Team collaboration
- Lab safety and cybersecurity ethics
- Preparedness
- Responsible use of technology
- Professional communication

Projects Include:

- Security assessments
- Firewall configurations
- Networking labs
- Cryptography activities
- Log analysis investigations
- Scenario-based cybersecurity challenges
- AP-style performance tasks

AP Exam Information

Students will take the AP Cybersecurity Exam in the spring.

Exam Format:

- 60 Multiple Choice Questions (70%)
- 1 Free Response Question (30%)
- Total Time: 2 Hours 10 Minutes

Students will complete regular AP-style practice activities throughout the course.

Classroom Expectations

Students are expected to:

- Demonstrate academic integrity.
- Follow all district technology policies.
- Participate actively in labs and discussions.
- Respect classmates and equipment.
- Use cybersecurity tools only for authorized educational activities.
- Work collaboratively and professionally.

Required Materials

- School-issued laptop
- Charger
- Notebook or digital notes system
- Access to Microsoft 365
- Access to AP Classroom
- Course lab resources and cybersecurity tools as assigned

Late Work Policy

- Assignments should be submitted by the posted due date.
- Late work may receive reduced credit according to school and district policy.
- Projects and labs may have separate deadlines due to course pacing.

Academic Integrity & Cyber Ethics

Cybersecurity professionals are trusted with sensitive systems and information. Students in AP Cybersecurity are expected to uphold ethical standards and use all tools, techniques, and resources responsibly. Unauthorized access, misuse of technology, plagiarism, cheating, or attempts to compromise systems are strictly prohibited and may result in disciplinary action.

Student Success Tips

To be successful in AP Cybersecurity:

- Attend class regularly.
- Complete all labs and projects.
- Practice analyzing cybersecurity scenarios.
- Review AP-style questions frequently.
- Ask questions and seek assistance when needed.
- Develop strong time-management and collaboration skills.

Parent/Student Acknowledgment

I have read and understand the expectations, grading policy, and requirements for AP Cybersecurity.

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____