Indiana Department of Education

Academic Standards Course Framework

Computer Science III: Cybersecurity

Computer Science III: Cybersecurity introduces the secure software development process including designing secure applications, writing secure code designed to withstand various types of attacks, and security testing and auditing. It focuses on the security issues a developer faces, common security vulnerabilities and flaws, and security threats. The course explains security principles, strategies, coding techniques, and tools that can help make software fault tolerant and resistant to attacks. Students will write and analyze code that demonstrates specific security development techniques. Students will also learn about cryptography as an indispensable resource for implementing security in real-world applications. Students will learn foundations of cryptography using simple mathematical probability. Information theory, computational complexity, number theory, and algebraic approaches will be covered.

- DOE Code: 5251
- Recommended Grade Level: 11, 12
- Required Prerequisite: Computer Science I and Computer Science II
- Credits: 2 semester course, 2 semesters required, 1-3 credits per semester, 6 credits maximum
- Counts as a Directed Elective or Elective for all diplomas

Dual Credit

This course provides the opportunity for dual credit for students who meet postsecondary requirements for earning dual credit and successfully complete the dual credit requirements of this course. The Dual Credit crosswalk can be accessed here.

Application of Content and Multiple Hour Offerings

Intensive laboratory applications are a component of this course and may be either school based or work based or a combination of the two. Work-based learning experiences should be in a closely related industry setting. Instructors shall have a standards-based training plan for students participating in work-based learning experiences. When a course is offered for multiple hours per semester, the amount of laboratory application or work-based learning needs to be increased proportionally.

Career and Technical Student Organizations (CTSOs)

Career and Technical Student Organizations are considered a powerful instructional tool when integrated into Career and Technical Education programs. They enhance the knowledge and skills students learn in a course by allowing a student to participate in a unique program of career and leadership development. Students should be encouraged to participate in Business Professional of America, DECA, or Future Business Leaders of America, the CTSOs for this area.

Content Standards

Domain –Secure Coding Concepts

Core Standard 1 - Students gain an understanding of the theories of secure coding and security

- CS3S-1.1 Describe and discuss key concepts in security, including confidentiality, integrity and availability, authentication, and access control.
- CS3S-1.2 Describe and discuss key concepts in cybersecurity, including cryptology, cryptography, cryptanalysis, cipher, cryptographic algorithm, private and public key encryption, public key infrastructure, and trust/trustworthiness.
- CS3S-1.3 Discuss the basic concepts of probability, random variables and probability distributions as they apply to information theory and cryptography.

Domain –Secure Programming

Core Standard 2 - Students demonstrate their knowledge of secure programming techniques

- CS3S-2.1 Demonstrate the techniques to transform plaintext into ciphertext, the use of hash functions for authentication and data integrity, and the use of private and public key encryption.
- CS3S-2.2 Investigate security vulnerabilities in various data structures, such as out-of-bounds arrays and buffer overflows.

Domain – Cyberattack Defense

Core Standard 3 - Students understand how cyberattacks occur, how to prevent, and how to defend cyberattacks.

- CS3S-3.1 Discuss various types of cyberattacks on software and software systems along with possible countermeasures and security controls that minimize risk and exposure
- CS3S-3.2 Discuss current industry standards, tools, and security practices in software development, including use of multiple layers of defenses, wireless security, and risks in 3rd party applications and libraries.

Domain – Data Integrity

Core Standard 4 - Students understand how to accept and maintain information

- CS3S-4.1 Explain the tradeoffs of developing a program in a typesafe language
  Implement secure coding and testing techniques including input validation, data sanitization, and exception handling.
- CS3S-4.2 Describe when and how to properly use open source vs. closed source software.
- CS3S-4.3 Examine the need to update software to fix security vulnerabilities.

Domain – Secure Programming

Core Standard 5 - Students demonstrate concepts in a final project

- CS3S-5.1 Discuss the role of software security in a company-wide security policy.
- CS3S-5.2 Develop Secure Software Development Lifecycle.
- CS3S-5.3 Perform software security audit on a peer-reviewed project.