Indiana Department of Education
Indiana Academic Standards Course Framework

Networking II: Cybersecurity

Networking II: Cybersecurity is a capstone experience of the Network Support Pathway. It builds upon a base knowledge of Information Technology as gained through lower level courses such as IT support and Networking I. This particular capstone course concentrates on the Security field within networking, also called the cybersecurity field. Laboratory and classroom components are used to cover key elements such as Information Security, Systems Security, Network Security, Mobile Security and, Defense and Mitigation Techniques. The core concepts of confidentiality, integrity and availability are covered.

- DOE Code: 5245
- Recommended Grade Level: Grade 11-12
- Required Prerequisites: Information Technology Support
- Recommended Prerequisites: Networking I
- Credits: 1-3 credits per semester, maximum of 6 credits
- 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 Professionals of America, Future Business Leaders of America, or the Technology Student Association, the CTSOs for this area.

Content Standards

Domain 1 – Information Security

Core Standard 1: Students describe the importance and players in the cybersecurity field.

Standards

N2S-1.1 Describe the role of the cybersecurity professionals.

N2S-1.2 Describe characteristics of cybersecurity criminals.

N2S-1.3. Describe the various attack schemes in use.

Domain 2 – Systems Security

Core Standard 2: Students monitor, maintain, and configure network clients' backup to sustain network operations and security.

N2S-2.1 Install updates to client operating systems.

N2S-2.2 Manage Disk Volume, File system and RAID.

N2S-2.3 Configure client performance settings.

N2S-2.4 Implement security policies including anti-virus software and firewall.

N2S-2.5 Develop and implement Password security procedures.

N2S-2.6 Investigate and configure backup options.

N2S-2.7 Evaluate and configure system recovery options.

Domain 3 – Network Security

Core Standard 3: Students will secure access on network equipment and use Access Control Lists to secure access.

N2S-3.1 Secure administrative access on routing and switching equipment.

N2S-3.2 Secure access on remote connections.

N2S-3.3 Using Security tools to implement policy for equipment access.

N2S-3.4 Develop and implement ACLs to control information access.

N2S-3.5 Monitor and control ACLs to develop increased policy and procedure control.

Domain 4 – Mobile Security

Core Standard 4: Students will explain and describe endpoint vulnerability's, protection methods, and procedures used to tighten security on mobile devices.

N2S-4.1 Assess vulnerabilities in mobile devices and research solutions.

N2S-4.2 Explore tools to help alleviate Mobility security issues.

Domain 5 – Defense and Mitigation Techniques

Core Standard 5: Develop methods for implementing data confidentiality and integrity.

N2S-5.1 Implement secure Virtual Private Network.

N2S-5.2 Implement Firewall configuration using local connections.

N2S-5.3 Implement Firewall configuration using VPNs remotely.

N2S-5.4 Test network security and create a technical security policy.

Domain 6 – Confidentially, Integrity, and Availability

Core Standard 6: Use the CIA (confidentially, Integrity and Availability) triad to help secure the network.

- N2S-6.1 Describe the terms Confidentiality, Integrity and Availability.
- N2S-6.2 Develop procedures for network and host equipment to implement CIA standard policies.
- N2S-6.3 Test network security and create a technical security policy.
- N2S-6.4 Discuss forensics and legal implications.