Information Technology Career Cluster
Foundations of Secure Information Systems (MS-CS-FSIS)
Course Number: 11.01100

Course Description: This course will provide an exploratory foundation in information systems, networking, and cybersecurity. It is designed to be taught in a 9-week rotation in 45-minute daily classes. Standards should be taught in the order presented with the exception of Standard 1 being an embedded standard with ongoing learning regarding employability and career opportunities. Through integrated instructional activities, students will have opportunities to apply employability skills and to research possible career options in the information technology area. They will also complete many hands-on activities to build a strong foundation in computer hardware and connectivity. Capstone projects should be incorporated at the completion of all standards as time allows. Students who successfully complete this course will be prepared for the following pathways upon entering high school: Information Support & Services, Networking, and Cybersecurity. This course may be taught in 6th, 7th, or 8th grade.

Requirements for teaching this and other computer science courses: This course should be taught in a lab setting with a 1:1 ratio of student to personal computer. Additional devices, such as tablets, robots, Raspberry pi computers, and drones will enhance the program and can be shared in groups of 2-3 students. All devices should be current technology with strong connectivity capabilities. To further enhance student learning, the lab should contain at least one personal computer that students can disassemble and reassemble to learn the working parts within the computer.

Course Standard 1

MS-CS-FSIS-1
Demonstrate employability skills required by business and industry to explore, research, and present careers in information technology.

1.1   Communicate effectively through writing, speaking, listening, reading, and interpersonal abilities.
1.2   Make collaborative observations and demonstrate potential technology and interpersonal interactions in the digital world.
1.3   Model work-readiness traits required for success in the workplace including integrity, honesty, ethics, accountability, punctuality, time management, and respect for diversity.
1.4   Exhibit critical thinking and problem-solving skills to locate, analyze, and apply information in career planning and employment situations.
1.5   Present a professional image through appearance, behavior and language.
1.6   Investigate educational requirements, job responsibilities, employment trends, and opportunities within information technology career pathways using credible sources.

Course Standard 2

MS-CS-FSIS-2

Investigate and identify the basic components of computers and networks.

2.1 Identify the basic components of the computer by disassembling and reassembling a demonstration model personal computer (can be done 'virtually' online if demo model is not available).

2.2 Demonstrate an understanding of key functional components (input devices, output devices, processor, operating system, software applications, memory, storage, Wi-Fi and/or Ethernet ports, and IP addresses).

2.3 Demonstrate an understanding of the terms and units used to describe major hardware components (RAM, ROM, GHz, MHz, GB, MB, CD, DVD, RW).

2.4 Explain the interrelation of the operating system software, application software, and utility software, citing specific examples of each.

2.5 Develop a basic vocabulary of networks including the Internet, wired, wireless, cellular, Wi-Fi, messages, packets, connections, bandwidth, broadband, firewall, hacking, cybersecurity, encryption, local area network (LAN), wide area network (WAN), and OSI model.

2.6 Demonstrate an understanding of the fundamental concepts for how computers process programming commands (hex, binary language, sequence of commands, conditional structures, and looping structures).

Course Standard 3

MS-CS-FSIS-3

Develop through application logical observations relative to computational thinking procedures to analyze and solve problems current to everyday life.

3.1 Identify characteristics of computational thinking (decomposition, pattern recognition, algorithmic thinking, and abstraction).

3.2 Explain issues and analyze routine hardware and software problems current to everyday life.

3.3 Apply troubleshooting concepts to issues regarding compatibility, data, and identity.

3.4 Describe ways to solve operational problems caused by hardware errors.

3.5 Explain how technology can create ethical and legal issues in the business world and a technology-based society and how it can be used to solve & manage those issues.

Course Standard 4

MS-CS-FSIS-4

Investigate ways to differentiate networks and how they are used in business and industry.

4.1 Create diagrams to illustrate types of network topologies to include star, ring, bus, mesh, and hybrid.

4.2 Differentiate networks based on coverage area including local area network (LAN), wide area network (WAN), and personal area network (PAN).

4.3 Differentiate between different network mediums including Wi-Fi, wired, satellite, and microwave.

Course Standard 5

MS-CS-FSIS-5
Evaluate and provide a rationale for the levels of the Open Systems Interconnection (OSI) model.
5.1   Summarize from multiple credible sources the physical and digital aspects of computing networks.
5.2   Trace the layers required to transmit data from one node to another (the OSI model).
5.3   Construct and explain the basic functions of the OSI model.

Course Standard 6

MS-CS-FSIS-6
Examine the basics of cybersecurity needs for business, government, and organizations.
6.1   List and define the elements of the confidentiality, integrity, and availability (CIA) triad.
6.2   Explain components of access control: Identification, Authentication, Authorization, Accountability, and Non-repudiation.
6.3   Identify the characteristics of strong vs. weak passwords in data and identity security.
6.4   List and describe the basic steps in security risk management.
6.5   Develop a logical argument for the importance of physical security.

Course Standard 7

MS-CS-FSIS-7
Cite evidence regarding the principles of cybersecurity and basic mechanisms used for protecting data and resources.
7.1   Define the cybersecurity first principles of least privilege, minimization, abstraction, domain separation, process isolation, information hiding, layering, simplicity, modularity, and resource encapsulation.
7.2   Apply concepts related to the principles behind encryption, including the purpose of cryptography, hashing, and steganography.
7.3   Draw conclusions illustrating a basic understanding of internet protocol (IP) packets, ports and network transmission.
7.4   Summarize from multiple credible sources a basic understanding of anti-malware, firewalls, intrusion detection system/intrusion prevention system (IDS/IPS), and virtual private network (VPN).

Course Standard 8

MS-CS-FSIS-8
Analyze and describe the characteristics of cybersecurity ethics, digital citizenship, and laws governing privacy.
8.1   Explain the differences between an ethical (white hat) hacker and an unethical (black hat) hacker.
8.2   Cite evidence regarding the practice of ethical digital decision-making, including plagiarism, copyright law, and software licensing types (freeware, public domain, shareware, etc.).

8.3   Summarize and provide examples regarding security and privacy laws and their impact on society, citing recent cases.

8.4   Collect and compare cyberbullying evidence, including legal and social consequences, and develop guidelines to prevent cyberbullying.

8.5   Develop an argument regarding network security, citing policy-driven and technology-driven examples.