Foundations of Secure Information Systems

Course Description:

This course provides an exploratory foundation in secure information systems, networking, and cybersecurity. Students will engage in hands-on activities, projects, and discussions to develop knowledge and skills related to computer hardware, networks, cybersecurity principles, and ethical technology use. The course integrates employability skills with technology standards, preparing students for advanced pathways in Information Support, Networking, and Cybersecurity.

Classroom Expectations:

- Be on time and ready to learn.
- Respect is a two-way street; employ it with everyone and it will be reciprocated; be kind to one and other.
- Educational discourse is key, and you must actively listen; listen while others are talking.
- The classroom is always your place of business necessitating professionalism, no horseplay.

Classroom Procedures:

Entering the Classroom:

- Line up against the wall outside the classroom. (***No food, drinks, or phones in hand this is an energy/power and electronics classroom; safety is always #1)***.
- Enter the classroom quietly take out your composition notebook and record the days Learning Target, Essential Question, and Agenda. ***(No food, drinks, or phones)***.
- Gather necessary materials for the days lesson and hang all bags on the back of the chair that you are occupying. ***(Specific materials will be highlighted on the Energy Systems White Board)***.
- Begin work on opening exercise quietly.

Exiting the Classroom:

- Secure all classroom equipment and place in assigned area.
- Ensure that your area is clean and clear before leaving. ***(This includes computer workstations that you were utilizing or other assigned spaces)***.
- Turn-in classroom assignments to appropriate physical or digital drop box.
- Return to your assigned seat until the bell rings and you are dismissed by the instructor.

Disciplinary Actions: *The order and type of consequences depend on the nature and severity of the infraction.*

- Verbal Warning
- Lunch Detention and phone call home. *(Minor Infractions)*.
- Counselor Referral.
- Discipline Referral. (*Major and Chronic Disciplinary Infractions)*.

Course Standards and Objectives:

MS-CS-FSIS Standards:

1. **Employability Skills**
    - Demonstrate employability skills required by business and industry, such as communication, accountability, and teamwork.
2. **Computer Hardware and Networks**
    - Investigate and identify computer hardware components and their functions.
    - Differentiate between various types of networks (LAN, WAN, Wi-Fi).
3. **Computational Thinking**
    - Apply computational thinking principles to solve real-world IT problems.
    - Demonstrate logical reasoning and troubleshooting techniques.
4. **Networking Fundamentals**
    - Understand network structures and types, including wired and wireless.
    - Explore the OSI model and its impact on data flow.
5. **Cybersecurity Basics**
    - Examine cybersecurity fundamentals, including the CIA triad (Confidentiality, Integrity, Availability).
    - Identify and implement strong password strategies and access control mechanisms.
6. **Advanced Cybersecurity Mechanisms**
    - Explain principles of encryption, hashing, and data protection techniques.
    - Demonstrate knowledge of firewalls, intrusion detection/prevention systems, and VPNs.
7. **Cybersecurity Ethics and Laws**
    - Discuss the importance of ethics in technology and cybersecurity.
    - Examine laws related to privacy, data protection, and digital rights.
8. **Problem Solving and Analysis**
    - Investigate ethical and legal issues using computational problem-solving approaches.
    - Analyze troubleshooting scenarios to develop resolutions.

IT Industry Standards (Integration with CTAE Standards)

1. **Hardware and Networking**
    - Recognize the significance of basic hardware assembly and maintenance.
    - Distinguish between various network topologies (e.g., star, mesh, hybrid).
2. **Cybersecurity in Practice**
    - Implement basic risk management strategies in cybersecurity.
    - Use tools and software to simulate real-world cybersecurity scenarios.
3. **Digital Citizenship**
    - Promote safe and responsible behavior in the digital world.
    - Identify methods to combat cyberbullying and protect online privacy.
4. **Regulatory and Legal Compliance**
    - Understand the U.S. framework for cybersecurity laws and regulations.
    - Explore how regulatory bodies enforce compliance and safety.

Core Integration Areas

1. **Science, Technology, Engineering, and Math (STEM)**
    - Apply STEM principles in problem-solving and technical design.
    - Develop flowcharts, diagrams, and digital presentations to explain technical processes.
2. **English Language Arts (ELA)**
    - Construct argumentative essays and reflective writings.
    - Present ideas clearly through verbal and written communication.
3. **Workplace Readiness**
    - Cultivate skills like teamwork, leadership, and professional ethics.
    - Prepare for IT-related careers through career exploration and pathway presentations.

Weekly Schedule and Outline:

Unit 1: Employability and Career Exploration (Weeks 1-2)

- **Topics:**
    - Communication and interpersonal skills in IT
    - Work readiness traits: integrity, accountability, respect
    - Career research and pathways in IT
- **Deliverables:**
    - Career pathway presentation
    - Peer discussions on IT trends

Unit 2: Computer Components and Networks (Weeks 3-5)

- **Topics:**
    - Disassembling and reassembling a computer

    - Basic hardware components and functions
    - Introduction to networking: LAN, WAN, and Wi-Fi
- **Deliverables:**
    - Hardware component diagram
    - Network topology lab

Unit 3: Computational Thinking and Problem-Solving (Weeks 6-7)

- **Topics:**
    - Decomposition, pattern recognition, and algorithmic thinking
    - Troubleshooting hardware and software issues
    - Ethical and legal problem-solving in technology
- **Deliverables:**
    - Logical flowchart for troubleshooting scenarios
    - Ethical dilemma case study

Unit 4: Networking Fundamentals (Weeks 8-9)

- **Topics:**
    - Network topologies: star, ring, bus, mesh, hybrid
    - Wired vs. wireless networks
    - Overview of OSI model layers
- **Deliverables:**
    - OSI model infographic
    - Comparative analysis of network types

Unit 5: Cybersecurity Basics (Weeks 10-12)

- **Topics:**
    - CIA triad: Confidentiality, Integrity, Availability
    - Access control principles and strong password strategies
    - Security risk management steps
- **Deliverables:**
    - Cybersecurity risk assessment report
    - Secure password development exercise

Unit 6: Advanced Cybersecurity Mechanisms (Weeks 13-14)

- **Topics:**
    - Cybersecurity principles: encryption, hashing, steganography
    - Anti-malware, firewalls, IDS/IPS, VPN concepts
    - Internet protocol and data packets
- **Deliverables:**
    - Encryption project: Create a secure message
    - Presentation on network security tools

Unit 7: Cybersecurity Ethics and Laws (Weeks 15-16)

- **Topics:**
  - Ethical vs. unethical hacking
  - Digital citizenship and cybersecurity ethics
  - Privacy laws and cyberbullying prevention
- **Deliverables:**
  - Argumentative essay on cybersecurity ethics
  - Cyberbullying prevention guidelines

Assessment Methods:

Major Grades= 40% Minor Grades= 60% Total= 100%

- Classwork/Homework = Minor
- Quizzes = Minor
- Exams = Major
- Papers/Presentations/Debates = Major
- Projects = Major

Late Assignments: Late work/assignments are defined as, "assignments that are submitted after the specific deadline".

- Late assignments may result in scores being reduced by 5% per school day for a 25% maximum reduction (five school days).
- Late work submitted after the fifth school day will **NOT** be accepted.
- Repeated incidents of late work may result in a teacher-student-parent conference to examine and correct the student's work habits through an academic contract.

Resources:

- Scientific journals and articles
- Online databases and tools
- Guest speakers from industry

Materials:

- 2 Composition Notebooks
- Pens or Pencils
- Wired Headphones with 3.5mm jack
- 2-3" Binder (Professional Portfolio)
- Loose Leaf Paper (College Rule OK)

This syllabus provides a structured framework for the course, ensuring a comprehensive understanding of energy and power generation, transmission, and distribution while aligning with academic standards and fostering essential employability skills.

_____
Student Printed Name

_____
Student Signature and Date

_____
Parent Printed Name

_____
Parent Signature and Date

Thomas M. Gonzales, MSCIA
Security+, Energy Industry Fundamentals
Energy & Power/Electronic Pathways
Richmond County Technical Career Magnet
gonzath@boe.richmond.k12.ga.us
706-823-5580 ext. 1543