

# 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. (

Enter the classroom quietly take out your composition notebook and record the days Learning Target, Essential Question, and Agenda.

Gather necessary materials for the days lesson and hang all bags on the back of the chair that you are occupying.

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.

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

## IT Industry Standards (Integration with CTAE Standards)

### 1. Hardware and Networking

- o Recognize the significance of basic hardware assembly and maintenance.
- o Distinguish between various network topologies (e.g., star, mesh, hybrid).

### 2. Cybersecurity in Practice

- o Implement basic risk management strategies in cybersecurity.
- o Use tools and software to simulate real-world cybersecurity scenarios.

### 3. Digital Citizenship

- o Promote safe and responsible behavior in the digital world.
- o Identify methods to combat cyberbullying and protect online privacy.

### 4. Regulatory and Legal Compliance

- o Understand the U.S. framework for cybersecurity laws and regulations.
- o Explore how regulatory bodies enforce compliance and safety.

## Core Integration Areas

### 1. Science, Technology, Engineering, and Math (STEM)

- o Apply STEM principles in problem-solving and technical design.
- o Develop flowcharts, diagrams, and digital presentations to explain technical processes.

### 2. English Language Arts (ELA)

- o Construct argumentative essays and reflective writings.
- o Present ideas clearly through verbal and written communication.

### 3. Workplace Readiness

- o Cultivate skills like teamwork, leadership, and professional ethics.
- o 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:

- o ~~Employability Skills: Communication, Teamwork, Problem Solving, Critical Thinking, Creativity, Adaptability, Resilience, Time Management, Organization, Self-Motivation, Professionalism, Ethics, Diversity and Inclusion, Global Awareness, Digital Literacy, Financial Literacy, Health and Wellness, Career Development, and Entrepreneurship.~~

0

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

### Topics:

- o Ethical vs. unethical hacking
- o Digital citizenship and cybersecurity ethics
- o Privacy laws and cyberbullying prevention

### Deliverables:

- o Argumentative essay on cybersecurity ethics
- o 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](mailto:gonzath@boe.richmond.k12.ga.us)  
706-823-5580 ext. 1543