Pamela Paquette
papaquette@madisoncity.k12.al.us
Planning period: 4th
Cybersecurity I

Cybersecurity I

Course Description

Cybersecurity I is designed to provide an entry into the quickly growing field of cybersecurity. It focuses on building key concepts and exploring the range and scope of the cybersecurity field. The course also looks at best practices, the importance of maintaining a high level of ethical behavior, the provisions and rationale for government regulations and laws, and the consequences of failure to abide by these rules. The course builds on students' basic knowledge of computers and networks to create a deeper understanding of how computer systems, devices, and other networks are interconnected through secure data networks. This course will continue to help prepare students for industry-level exams.

Career and Technical Student Organizations are integral, co-curricular components of each career and technical education course. These organizations enhance classroom instruction while helping students develop leadership abilities, expand workplace-readiness skills, and access opportunities for personal and professional growth. Students in the Information Technology cluster affiliate with SkillsUSA and/or TSA.

Foundational standards, shown in the table below, are an important part of every course. Through these standards, students learn and apply safety concepts, explore career opportunities and requirements, practice the skills needed to succeed in the workplace, develop leadership qualities and take advantage of the opportunities afforded by Career and Technical Student Organizations (CTSOs), and learn and practice

essential digital literacy skills. The foundational standards are to be incorporated throughout the course.

Pre-requisites

Information Technology Fundamentals or Programming Foundations

Instructional Delivery Plan *Students will:*

1. Learn and use standard safety practices.
2. Participate in a virtual design challenge
3. Study/take an industry Cybersecurity Certification Test

Course Goals

Foundational Standards

1. Incorporate safety procedures in handling, operating, and maintaining tools and machinery; handling materials; utilizing personal protective equipment; maintaining a safe work area; and handling hazardous materials and forces.
2. Demonstrate effective workplace and employability skills, including communication, awareness of diversity, positive work ethic, problem-solving, time management, and teamwork.
3. Explore the range of careers available in the field and investigate their educational requirements, and demonstrate job-seeking skills including resume-writing and interviewing.
4. Advocate and practice safe, legal, responsible, and ethical use of information and technology tools specific to the industry pathway.
5. Participate in a Career and Technical Student Organization (CTSO) to increase knowledge and skills and to enhance leadership and teamwork.
6. Use technology to collaborate with peers and/or experts to create digital artifacts that can be published online for a target audience.
7. Formulate new ideas, solve problems, or create products through the design and engineering process by utilizing testing, prototypes, and user feedback.

Technology Laws, Ethics, and Digital Safety

1. Identify and discuss ethical considerations and consequences resulting from technological advances.
   Examples: deepfake, facial recognition, big data, privacy concerns
2. Research and discuss federal laws, regulations, and agencies that govern online activities and individual and corporate network use.
   Examples: Computer Security Act, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, Payment Card Industry Data Security Standard (PCI DSS); COPPA, HIPAA, FERPA, and CMMC regulations
3. Gather and share information regarding ethical standards which apply to cybersecurity professionals.
4. Describe national and international standards and frameworks related to security operations.
   Examples: Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) RMF/CSF, International Organization for Standardization (ISO)
5. Identify security policies related to the employees of organizations or businesses and discuss the importance of establishing such policies.
   Examples: personnel policies, acceptable use, non-disclosure agreements, credential policies

Access Controls

6. Explain and differentiate among identification, authentication, authorization, and accounting for controlling access.
    a. Identify and describe authentication types and attributes.
    b. Compare and contrast authorization access control models.
    Examples: mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), lattice
7. Explain the principle of least privilege as it relates to account policy.
8. Perform the specific duties associated with using an administrator/root account in a given computer system.
9. Select and implement user account management controls for a given scenario.
10. Implement secure password and account policies in an operating system.
11. Perform basic system audits and analyze log files in a given scenario.
12. Use the command/terminal line to configure security settings.
13. Perform basic system administration tasks in more than one operating system.

Network Foundations

14. Differentiate among types of networking cable mediums and standards to determine which type to use in a given situation.
    Examples: copper cabling, fiber optic
15. Compare and contrast notational systems, including binary, hexadecimal, decimal, and ASCII.
16. Identify and describe common TCP and UDP ports and services.
    Examples: DNS, HTTP, SSH, TELNET, TLS, FTP, SMTP, IMAP, POP, DHCP, LDAP, NTP, SNMP, RDP, SCP, RTP \
17. Classify IP addresses according to IPv4 and IPv6, private and public IP ranges, and special IPs.
18. Use subnetting to determine the number of hosts and/or subnets on a given network.
19. Differentiate between the OSI and TCP/IP models, layers, encapsulation, and decapsulation.
20. Use various network tools in computer operating systems environments.
    Examples: ipconfig, ifconfig Ping, nslookup, tracert, netstat, iptables; Windows, Linux, Apple
21. Perform an install of an operating system in a virtual environment.

Security Foundations

22. Apply the parts of the CIA triad (confidentiality, integrity, and availability) to a given security scenario.
23. Describe various types of physical security controls and explain their importance.
24. Analyze attributes of various types of malware and other attacks to determine the key characteristics of each type.
    Examples: virus, worm, brute force, backdoor, spyware, remote access tool (RAT)
25. Describe various types of social engineering.
26. Describe various types of application attacks and threats.
    Examples: cross-site scripting, SQL injection, buffer overflow
27. Analyze types of network attacks.
    Examples: man in the middle, layer 2 attacks, denial of service, DNS poisoning
    a. Identify and analyze wireless network threats.
    Examples: evil twin, bluesnarfing, jamming, disassociation

28. Describe different types of threat actors and threat vectors.
    Examples: APT's; black hat, white hat, and gray hat hackers; supply chain; social media
29. Predict security concerns and possible vulnerabilities associated with system hardening.
    Examples: weak configurations, open ports and services, third-party risks
30. Describe the techniques used in security assessments.
    Examples: threat hunting, vulnerability scans, security information and event management (SIEM)
31. Explain basic cryptographic concepts.
    Examples: historic ciphers, symmetric, asymmetric, hashing, quantum computing uses
32. Describe the purpose and scope of a cybersecurity disaster recovery plan for a given simulated or actual work environment.

Credentialing

Security+ Certification testing will be offered to those ready to take it after approximately 100-125 hours of seat time during this course or during a follow-up course afterwards.

Grading and Assessment

Not all assignments are graded. It is imperative that students are conscientious and complete ALL of the required work on time. Students are required to take notes (annotations), participate in lectures, watch tutorial videos, read selections, and respond with appropriate grammar. It is the student's responsibility to obtain the class notes from another student if absent. Assessment is given in all kinds of formats; written, verbal, performance products, skills demonstrated, knowledge gained and development of problem-solving.

- *Assessments 70%*
- *In-Class Work 30%*

Late Work

Any assignments that are turned in late without excuse will result in 10 points deducted from the final grade. More than 3 days late will result in earning up to half the original points.

Makeup Work

If you are absent, you will be expected to make up the work that was missed. All missed assignments and tests must be made up within three days of an EXCUSED absence. If it is not excused, you will not be allowed to make up the work (including exams).
On the day you return to class, please see me immediately for any content that you missed or to make an appointment for a make-up quiz or test. If you enter school after class or leave school before class, you are expected to see me to find out what you missed or will miss. You will be held accountable for work due that day or work assigned for homework that night.

TSA (Technology Student Association) CTSO Integration

TSA is a fundamental part of this course and is a national career and technical student organization of students engaged in science, technology, engineering, and mathematics (STEM). TSA's integrated into the program which includes competitions and leadership opportunities. TSA provides students with activities during their class time and after school with our local TSA Chapter.

Embedded Numeracy Anchor Assignment

Students will …

This assignment will account for 200 points.

Embedded Literacy Anchor Assignment

Students will read and comprehend complex informational texts used to explain security, networking, and policies independently and proficiently. Students will write analysis and interpretation of text based on projects that they are working on by keeping a Cybersecurity Notebook of their work.

This assignment will account for 200 points**.**

Culminating Project

Students will use their learned skills with the …

Supplies

1. Folder or section in a binder for handouts.
2. Notebook will be electronic
3. Calculator
4. Shared Folder on Google Drive

Procedures

1. Once the bell has rung, the student is expected to be seated in class and ready to work.
2. Tardies are strictly enforced. James Clemens High School's tardy policy will be followed.

3. No hall passes for the **first or last 10** minutes of class
4. The hall pass binder is near the door. Students will be required to sign each time they leave/return to class.
5. You have three days to do makeup work and tests. It is up to you to look up the to-do list on schoology about the work missed. You can also review the latest posts on Schoology.
6. During fire drills we will exit the building to the correct exit of the building, and you are to walk with **PURPOSE**. You are to always stay with me and form a single file line once we are safely outside and be ready to be counted.
7. When the intercom sounds, you must immediately sustain all talking.
8. Raise your hand and wait to be called upon.
9. Listen without interrupting.
10. I employ the ***Ask 3 Before Me Principle***. This room is full of others that you can learn from or you can assist in their learning.
11. If we finish before the bell, you must remain seated at your desk. Take advantage of this time to work on homework, other class assignments, etc.

Computer/Internet Appropriate Usage Policies

1. You are required to bring your Chromebook, charged every day.
2. Please bring your charger every day to class.
3. Work on only software/apps for the class (or other classes).
4. DO NOT install any software/proxies/emulators on Lab PC's.
5. DO NOT copy, move, delete other's work sessions, files etc.

CTE Dual Enrollment

Students at James Clemens High School can attend Calhoun Community College, Drake State Technical Community College or University of Alabama at Huntsville to take dual enrollment courses:

Consent to Video Recording

Class Recordings: Instruction in this class might be recorded or streamed live. Any recordings will be available to students enrolled in this class. This is intended to supplement the classroom experience. Students are expected to follow appropriate school system and campus-wide policies and maintain the security of passwords used to access classroom recordings. Live streaming and recordings may not be captured or reproduced, shared with those not in the class, or uploaded to other online environments. Doing so would be a breach of the Madison City's Public School System's Acceptable Use Policy. If I, or an administrator, plans to use any recordings, beyond the classroom environment, students identifiable in the recordings will either be de-identified or will be notified prior to obtaining proper consent prior to such use.

Career Pathway Program	Cybersecurity and Infrastructure Program (Must teach three courses from this program list within two years.) This pathway provides students with the skills necessary for protecting information technology infrastructure and networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity is an enormous and growing field as consumers and businesses share data through online shopping and social media applications.		
Course Number	**Career Pathway Program Courses**	**Career Readiness Indicator (CRI)**	**In Demand Occupations**
10997G1001	Career Pathway Project in Information Technology	• Certiport Information Technology Specialist (ITS) Cloud Computing • Certiport Information Technology Specialist (ITS) Cloud Computing • Certiport Information Technology Specialist (ITS) Cybersecurity • Certiport Information Technology Specialist (ITS) Networking • Cisco Certified Network Associate (CCNA) • CompTIA IT Fundamentals • CompTIA Linux+ • CompTIA Network+ • CompTIA Security+ • Microsoft 365 Fundamentals • Microsoft Azure Data Fundamentals • Microsoft Azure Fundamentals • Microsoft Dynamics 365 Fundamentals CRM • Microsoft Dynamics 365 Fundamentals ERP • Microsoft Power Platform Fundamentals • Microsoft Security, Compliance, and Identity Fundamentals • TestOut Network Pro • TestOut Security Pro	• Cloud Architect • Cloud Engineer • Cloud Infrastructure Engineer • Cloud System Administrator • Data Engineer • DevOps Cloud Engineer • UI Developer
10102G1014	Cloud and Virtualization		
10997G1002	CTE Lab in Information Technology		
10020G1011	Cybersecurity I		
10020G1012	Cybersecurity II		
10020G1013	Cybersecurity III		
10109G1001	Foundations of Operating Systems		
10001G1000	Information Technology Fundamentals		
10109G1000	Linux Fundamentals		
10112G1001	Network Fundamentals		
10112G1002	Network Systems Administration		
10152G1001	Programming Foundations		