PRINCIPLES OF INFORMATION SECURITY (CYBERSECURITY I)

Teacher Name: Bill McIlwain   Teacher E-mail: wemcilwain@madisoncity.k12.al.us

Course Description:

This PLTW course introduces students to computer network systems that are most commonly the focus of attack. Students will build and configure the common elements found on the Internet to include database servers, web servers, and web application servers. Students will also be introduced to remote access terminal shells, which will be vital toward penetration testing and attack vectors. **Prerequisite:** Foundations of Informational Security

Course Objectives:

Students will learn the technical aspects of a highly networked world and the risks to information we all share. They will learn operating system and networking concepts, security frameworks, and packet analysis. They will be exposed to the different types of malware that can attack systems on a network and how to secure and protect a system against them. Students will also understand the history of encryption and ciphers and use frequency predictors to try to break the codes. They will practice data hiding techniques while learning cryptography. In addition, the course will help prepare the student to pursue the Security + certification exam.

Classroom Expectations:

You are expected to conduct yourself in a respectful and productive manner. In addition to all the rules and expectations listed in the student handbook, I expect you to have a positive attitude, treat others with respect, practice self-discipline, and demonstrate responsibility. If these conditions are not met, you can expect one-on-one meetings with me, parent/instructor conferencing, and administrative action, if necessary.

Concerning the use of cell phones and other electronic devices:
Devices should be on silent and kept in your purse, backpack, or pocket during class unless otherwise instructed. You may not place it on your desk. Parents, guardians, and other family members should call the front office in case of emergency.
If you violate this rule, you can expect the following consequences:
● *First offense* – The phone or device will be placed in a phone chart at the front of the room. You may pick it up at the end of class.
● *Second offense* – The phone or device will again be placed in a phone chart at the front of the room until the end of class and a parent/guardian will be notified.
● *Third offense* – This is defiance and I will notify an administrator.

Grading Policy:

Major assessments will count 70 percent of your grade. Homework and classwork will account for 30 percent of your grade. Grades will be updated weekly in PowerSchools. Each grading period will consist of nine weeks.

PRINCIPLES OF INFORMATION SECURITY (CYBERSECURITY I)

Teacher Name: Bill McIlwain   Teacher E-mail: wemcilwain@madisoncity.k12.al.us

Make-up Work Policy:	Make-up tests will **only** be given to a student who has an **excused absence**. **The student must make arrangements with the teacher to take a make-up test. Tests may be taken during Patriot Path with prior arrangement from each teacher.** A student only has two chances (the next two Patriot Paths after the absence) to make up a test. All make-up tests will be administered in the designated classroom on the Patriot Path session roster.
	Homework/Classwork: Students who are absent for **excused reasons** will be permitted to make up missed work. **It is the student's responsibility to get their work assignments the day upon return to school and complete the assignments according to a time frame determined by the teacher within two weeks of the date of the last absence**. Grades of zero will be assigned for assignments missed because of unexcused absences.
Text and Other Required Reading:	TestOut.com online training; Security Pro
Materials and Supplies Needed:	Laptop Note taking is strongly encouraged! *Other materials for Cybersecurity curriculum will be added on an as needed basis.
Laptops	Concerning laptop utilization: 1.Student laptops should not be hard-wired to the network or have print capabilities. 2. Use of discs, flash drives, jump drives, or other USB devices will not be allowed on Madison City computers. 3. Neither the teacher, nor the school is responsible for broken, stolen, or lost laptops. 4. Laptops and other electronic devices will be used at the individual discretion of the teacher.
Turnitin Notice	The majority of writing assignments in this course will be submitted to Turnitin via the Schoology learning platform. Turnitin generates a report on the originality of student writing by comparing it with a database of periodicals, books, online content, student papers, and other published work. This program will help students discern when they are using sources fairly, citing properly, and paraphrasing effectively - skills essential to all academic work.
	Students will have the opportunity to review their Turnitin originality report and will have the opportunity to make revisions before submitting their work for grading. Once their work is submitted, teachers have the opportunity to view the student/s originality report and grade accordingly.

PRINCIPLES OF INFORMATION SECURITY (CYBERSECURITY I)

Teacher Name: Bill McIlwain   Teacher E-mail: wemcilwain@madisoncity.k12.al.us

Accommodations   Requests for accommodations for this course or any school event are welcomed from students and parents.

18 – TENTATIVE WEEK PLAN*	
Week 1	**Unit 1: Network Security** Cyber I review, Cybersecurity Jobs, NICE Workforce Framework
Week 2	Network Devices, Attacks from the Net, Analyzing the Net
Week 3	Exploring Network Security, Exploring Security Frameworks
Week 4	Switch Attacks, Switch Security, Network Applications
Week 5	Packet Analysis, Attack Analysis, Finding the Exploits
Week 6	**Unit 2: Advanced Cryptography** Ciphers and Early Cryptography, Uses of Encryption, Decrypt the Encrypted
Week 7	Public Key Infrastructure, Asymmetric and Symmetric Encryption
Week 8	Commanding the OS, Processes, Finding the Secrets
Week 9	Cryptographic Attacks, Data Transmission Security
Week 10	**Unit 3: Digital Forensics** Ethical Hacking, Tools of the Trade, Tracing Identity
Week 11	Recon & Denial of Service, Spoofing & Poisoning
Week 12	Security Appliances, Device Hardening
Week 13	**Unit 4: Applied Cybersecurity** Detect and analyze the occurrence of a cybersecurity event.

PRINCIPLES OF INFORMATION SECURITY (CYBERSECURITY 1)

Teacher Name: Bill McIlwain   Teacher E-mail: wemcilwain@madisoncity.k12.al.us

Week 14	Acquire and maintain data in compliance with the digital forensics process.
Week 15	Positive and negative outcomes of different solutions related to data confidentiality, integrity, and availability.
Week 16	Defending the Network, Red Team-Blue Team
Week 17	The future of Cybersecurity & Study for Security + Exam
Week 18	**Review and Finals**

*This is a tentative plan and may change at the discretion of the teacher.

Please sign below to acknowledge that you have received, read, and understood the syllabus.

Student name: _____

Student signature: _____

Parent/guardian name: _____

Parent/guardian signature: _____

Parent/guardian, please provide two ways for me to contact you (email address, phone numbers):

Parent/guardian Email:

_____

Parent/Guardian Phone number:

_____