Course Name: Cybersecurity	
Department: STEM	Grade Level(s): 11,12
Duration/Credits: 1 year/1.0 credit Weighted 0.75	Prerequisites: Computer Science Principles
BOE Approval Date:	Course Code: HSTEM14

Course Description:

The PLTW Cybersecurity course exposes the high school student to the ever growing and far reaching field of cybersecurity. The student will accomplish this through problem-based learning, where the student will role-play as cybersecurity experts and train as cybersecurity experts do. The student will have a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. The student will use algorithmic thinking, computational thinking, and especially, "outside-the-box" thinking. The student will explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security.

Course Rationale:

There is an ever-pressing need to identify cybersecurity threats and protect against them. Informed citizens need to be able to detect intrusions and respond to attacks and examine one's digital footprint and protect personal data. This course provides the student the opportunity to explore a career in the emerging field of cybersecurity or learn how to defend their own personal data or a company's data.

Course Objectives:

1. The student will learn personal and digital security, verbally describe why they are important, and learn to be safe consumers of digital information in a variety of contexts. (A+ Speaking and Listening)
2. The student will learn the basic types of malware, security features of browsers, and how not to be a victim.
3. The student will role play to determine how cyber attacks occur, improve security features, and solve problems.
4. The student will read about information architecture, explain how networks evolve, and explore the security of a networks of various sizes. (A+ Reading)
5. The student will learn the security vulnerabilities of web services and how to secure an Ecommerce site.
6. The student will research various kinds of malware including propagation and symptoms and develop a plan to protect against such threats at various scales. (A+ Research)

7. The student will write explanations and arguments how to safely and securely exchange information on a public network. (A+ Writing)
8. The student will engage in multiple problem-solving scenarios, determine solutions, and communicate results.
9. The student will recognize patterns to identify security vulnerabilities and protect against malicious exploits.
10. The student will practice data hiding techniques including encryption, cryptography, and steganography.
11. The student will explore cybersecurity in an applied field.
12. The student will explore a crime scene and provide digital evidence to solve a mystery and determine possible consequences of the crime.