**James Logan High School**
**CyberSecurity**
**Course Syllabus**

**Instructor**: Ms. Banther

Welcome! You will now begin your training in Cybersecurity. The design of the course exposes high school students to the ever growing and far reaching field of cybersecurity. Students accomplish this through problem-based learning, where students role-play as cybersecurity experts and train as cybersecurity experts do.

Texts: All materials are on the PLTW site.

**Homework:** Homework may be assigned daily. You may be given 5-10 pages of reading per day and/or problems to solve on paper. You are encouraged to work with others on your homework in order to check your accuracy. Working together should be a mutual effort. Avoid situations where you will be just recording the answers, as this will hurt you later. Find a partner who can accept your help and give you help without doing the work for you. All homework assignments are due at the beginning of the period, although not all of them will be checked.

**Grading: We will utilize the Formative/ Summative grading policy.** The Formative part (HW, Projects and Quizzes) will make up 30% of your grade and Summative (Tests, Summative Projects and Final) will be the remaining 70%. There will not be separate categories just **Formative and Summative.** The grading scale is the standard 90%-100% A, 80%-89% B... percent table.

**Make-Up and Late work**: It is your responsibility to make up your work when you are absent. Tests and homework must be made up within a reasonable amount of time upon your return from an excused absence. Some quizzes may not be made up and therefore will not count against you if your absence is excused. Late homework is accepted for full credit 1 week after the due date and for up to half credit up to the end of the semester.

**Groups**: For the first semester, most of you will work in groups of two or three in class. Choose your partner carefully.

*Academic Dishonesty will result in zero for all parties involved. Group work is acceptable copying is not.*

**PLTW Cybersecurity** is a full-year course implemented in 10th grade or above. The design of the course exposes high school students to the ever growing and far reaching field of cybersecurity. Students accomplish this through problem-based learning, where students role-play as cybersecurity experts and train as cybersecurity experts do.

PLTW Cybersecurity strongly connects to the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF). Created by the National Institute of Standards and Technology (NIST), this framework identifies standards developed by numerous academic, industry, and government organizations. The framework objectives address topics that span K-12 education and guide learning progressions. The objectives also incorporate many of the big ideas and learning objectives outlined by the College Board and addressed in AP CSP and AP CSA. In addition, the course integrates Computer Science Teachers Association (CSTA) standards.

PLTW Cybersecurity gives students a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. It inspires algorithmic thinking, computational thinking, and especially, "outside-the-box" thinking. Students explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security. The course contains the following units of study.

    Unit 1 Personal Security (19%)
    Unit 2 System Security (24%)
    Unit 3 Network Security (32%)
    Unit 4 Applied Cybersecurity (25%)

**Unit 1: Personal Security**
Students learn the basic concepts of cybersecurity by leveraging their familiarity with technology they use every day, such as mobile devices and apps, as well as exploring the risks associated with how they use their email, personal files, and social networking habits.

**Lesson 1.1 Introduction to Cybersecurity**
Students learn personal and digital security, describe why they are important, and learn to be safe consumers of digital information in a variety of contexts.

    Activity 1.1.1 Cybersecurity and Code of Conduct (2 days)
    Activity 1.1.2 Password Protection and Authentication (3 days)
    Activity 1.1.3 Email and Social Media Security Risks (3 days)
    Project 1.1.4 Save the Day (2 days)

**Lesson 1.2 Security and the Internet**
Students learn that the internet is a loosely controlled collection of computers networked together and secured by firewalls. They learn the basic types of malware, security features of their browser, and how not to be a victim. They learn about files and processes, how to manage them, and how to identify suspicious data (potential malware). At the end of the lesson, students role play as victims of a malware attack. They determine how the attack occurred, improve the security of the firewall, and secure their browser.

    Activity 1.2.1 Firewalls and Malware (3 days)
    Activity 1.2.2 Managing Your Data (3 days)
    Activity 1.2.3 Securing Your Browser (3 days)
    Project 1.2.4 It's a Trap! (3 days)

**Lesson 1.3 Protect Your Data**
Students use their knowledge about files, directories, processes, browsers, suspicious emails, and malware to solve the unit problem.

Problem 1.3.1 A Dangerous Situation (5 days)

## Unit 2: System Security
Students broaden their cybersecurity knowledge from a personal system to a networked system. They learn how to assess the value of information security and delve deeper into types of malware. They learn the security vulnerabilities of web services and how to secure an Ecommerce site.

### Lesson 2.1 Information Architecture
Students delve into information confidentiality and how it relates to information integrity and assurance, as they compare the value and the risks of sharing information. Students learn how host names relate to digital addresses, demystify the "cloud", learn how networks evolve, and explore the security of a small network.
    Activity 2.1.1 Confidentiality, Integrity, and Availability (3 days)
    Activity 2.1.2 Passive Analysis (2 days)
    Project 2.1.3 Ecommerce Architecture (3 days)

### Lesson 2.2 Server Vulnerabilities
Students learn more about the types of malware that are threats to information and the types of delivery systems. Using website applications and the back-end services that support them, they learn how attacks can occur. They explore a vulnerable web server and improve its security measures.
    Activity 2.2.1 More on Malware (3 days)
    Activity 2.2.2 Server Vulnerabilities (2 days)
    Activity 2.2.3 Server Analysis (2 days)
    Project 2.2.4 Secure the Server (1 day)

### Lesson 2.3 Server Exploits
Students delve deeper into how malware propagates and research the symptoms of various exploits. They analyze and secure one of the most common vulnerable environments: a web server hosting client applications.
    Activity 2.3.1 Securing Ecommerce Data (2 days)
    Activity 2.3.2 Stopping the Spread of Malware (3 days)
    Activity 2.3.3 Server Attacks (4 days)
    Project 2.3.4 Find the Exploits (3 days)

### Lesson 2.4 The Ecommerce Site
Students learn how information can be safely and securely exchanged on a public network. In the end-of-unit problem, students discover a breach, identify the security vulnerabilities, and enhance the system to secure it.
    Problem 2.4.1 Ecommerce Enrichment (5 days)

## Unit 3: Network Security
Students learn the technical aspects of a highly networked world and the risks to information we all share. They learn operating system and networking concepts, security frameworks, and packet analysis. They learn the types of malware that can attack systems on a network and how to secure and protect a system against them.

**Lesson 3.1 Files and Processes**
They learn how an operating system organizes information using command line tools to manage and secure digital information. Students learn about user and system processes and how malware spreads around a network. Then, they identify suspicious software running on the system and determine the problems it may have caused.
    Activity 3.1.1 Commanding the OS (2 days)
    Activity 3.1.2 Access Control (2 days)
    Activity 3.1.3 Analyzing Processes (4 days)
    Project 3.1.4 Find the Secrets (3 days)

**Lesson 3.2 Attacks from the Net**
Students explore network topologies and go deeper down the abstraction path to learn more about network security. They analyze network traffic, find patterns that may represent exploits, and identify security vulnerabilities.
    Activity 3.2.1 Exploring Network Security (4 days)
    Activity 3.2.2 Exploring Security Frameworks (3 days)
    Activity 3.2.3 Where Can I Learn More About Cybersecurity? (3 days)
    Project 3.2.4 Eradicate the Vulnerabilities (4 days)

**Lesson 3.3 Analyzing the Net**
Students analyze network traffic to witness, and then protect against, a malware attack. Students analyze packets to find telltale signs and patterns of malicious exploits. They apply what they've learned to perform a penetration test and secure a network against further attacks.
    Activity 3.3.1 Analyzing Address Resolution (2 days)
    Activity 3.3.2 Analyzing Control Messages (2 days)
    Activity 3.3.3 Analyzing Packet Fragmentation (2 days)
    Activity 3.3.4 Analyzing Wireless Authentication (2 days)
    Project 3.3.5 Analyzing the Attack (5 days)

**Lesson 3.4 Secure the Net**
Students are given an attack scenario and must identify the exploit, secure the system, and make improvements to prohibit future attacks.
    Problem 3.4.1 Is the Network Under Water? (8 days)

**Unit 4: Applied Cybersecurity**
Students explore cybersecurity in an applied field. They learn methods of cryptography and practice basic tenets of digital forensics. They process a crime scene to solve the mystery and explore the possible consequences of the crime.

**Lesson 4.1 Cryptography**
Students learn the history of encryption and ciphers and use frequency predictors to try to break the codes. They practice data hiding techniques, such as cryptography and steganography. Finally, they attempt to decrypt each other's encrypted messages.
    Activity 4.1.1 Ciphers and Early Cryptography

Activity 4.1.2 Symmetric and Asymmetric Encryption
Activity 4.1.3 Storage Encryption Techniques
Activity 4.1.4 Steganography
Project 4.1.5 Decrypt the Encrypted

**Lesson 4.2 Digital Forensics**
Students learn the process of gathering digital evidence, analyzing it, tracing the criminal through their digital footprint, and preparing to prosecute the criminal.
Activity 4.2.1 Evidence Handling
Activity 4.2.2 Data Integrity
Activity 4.2.3 Imaging Files and Devices
Activity 4.2.4 Establishing Identity in Cyberspace
Project 4.2.5 Phishing at Work

**Lesson 4.3 Criminal Justice and Computer Science**
Students use their knowledge from the entire course to investigate a crime and provide digital evidence to solve it.
Problem 4.3.1 Solve the Crime!