Chino Valley Unified School District
High School Course Description

A. CONTACTS	
1. School/District Information:	School/District: Chino Valley Unified School District Street Address: 5130 Riverside Drive Phone: (909) 628-1201 Website: chino.k12.ca.us
2. Course Contact:	Teacher Contact: Office of Secondary Curriculum Position/Title: Director of Secondary Curriculum Site: District Office Phone: (909) 628-1201 X1630
B. COVER PAGE - COURSE ID	
1. Course Title:	Cybersecurity Honors
2. Transcript Title/Abbreviation:	Cybersec H
3. Transcript Course Code/Number:	5E85
4. Seeking Honors Distinction:	Yes
5. Subject Area/Category:	Meets UC/CSU "G" Elective: Mathematics - Computer Science
6. Grade Level(s):	10-12
7. Unit Value:	5 units per semester/10 credits
8. Course Previously Approved by UC:	No
9. Classified as a Career Technical Education Course:	No
10. Modeled after an UC-approved course:	Yes
11. Repeatable for Credit:	No
12. Date of Board Approval:	February 16, 2023

13. Brief Course Description:

This cybersecurity course offers an in-depth survey of the field of Computer Networking and Internet Security, preparing students for the CompTIA Network+, A+, and Security+ Certification exams and entry-level industry positions. The course also prepares students for the Cisco CCNA Unified Certification exam. Cybersecurity Honors is a year-long course in the Biomedical Science and Technology (BST) program at Chino High School.

14. Prerequisites:	None

15. Context for Course:

Aligned with the California K-12 Computer Science Standards, this course empowers students to delve into the fields of networking, computer components/configurations and cybersecurity to prepare students for entry-level industry positions.

In Network+ students will acquire knowledge, using online software, of basic computer hardware and operating systems, covering such skills as installation, upgrading, configuring, troubleshooting, optimizing, diagnosing and preventative maintenance. Students will also gain knowledge of additional elements such as networking and server issues, security, safety, environmental issues, communication, and professionalism.

In Security+ students will take in-depth and comprehensive view of security by examining the attacks that are launched against networks and computer systems, and the necessary defense mechanisms to counter attackers.

In A+ students seeking career-oriented, entry-level computer hardware, software, and networking skills will gain fundamental computer and mobile device hardware, software configuration and troubleshooting skills. Students will prepare for the CompTIA A+ certification exams.

16. History of Course Development:

As the world becomes more technologically advanced, current trends indicate an increased need for individuals who can maintain the interconnectivity of a computer network and ensure that the network is secure from intrusion. Aligned with the California K-12 Computer Science Standards, this course empowers students to delve into the fields

of networking, computer components/configurations and cybersecurity to prepare students for entry-level industry positions.	
17. Textbooks:	**Suggested Text** CompTIA Security+, Guide to Network Security Fundamentals, Mark Ciampa, Cengage, 7th Edition, 2022 Network+ Guide to Networks, Jill West, Jean Andrews, Tamara Dean, Cengage, 8th Edition, 2019
18. Supplemental Instructional Materials:	Supplemental online materials

C. COURSE CONTENT

1. Course Purpose:

This cybersecurity course offers an in-depth survey of the field of Computer Networking and Internet Security, preparing students for the CompTIA Network+, A+, and Security+ Certification exams and entry-level industry positions. This course also prepares students for the Cisco CCNA Unified Certification exam.

2. Course Outline:

Unit 1 - Introduction to Networking

This unit begins by exploring the question "What is a network?" Students will learn the fundamental types of networks and will be able to describe the devices and topologies that create a network. Students will also learn the OSI model and best practices for safety when working with networks, specifically focusing on the seven-step troubleshooting model. The unit next considers the question "How Computers Find Each Other on Networks" where students investigate standards used by devices on a network and explain how hostnames and domain names work. Students will also learn about ports and sockets at the Transport layer and IP addresses at the Network layer. This section of the unit concludes with an introduction to commands used in troubleshooting networks. Finally, in this unit, students will examine "How Data is Transported Over Networks" focusing on the functions of the core TCP/IP protocols, as well as common IPv4 and IPv6 routing protocols. Students will learn about multiple TCP/IP utilities used for network discovery and troubleshooting. Throughout this unit, students will be engaged in close reading and annotation of complex text, will collaborate with peers to assist with learning concepts and to cooperatively accomplish tasks, and will write both informally and formally as a means to demonstrate understanding and mastery of the concepts.

Unit 2 - Networking, Cloud Computing and Risk Management

In this unit students begin by looking at Structured Cabling and Networking Elements which introduces best practices for managing network and cabling equipment, and explains issues related to managing power and the environment in which networking equipment operates. Students will also learn characteristics of NIC and Ethernet interfaces and explain how to create a network map that can be used in network troubleshooting.

The next section of the unit, Network Cabling has students exploring basic data transmission concepts, including signaling, data modulation, multiplexing, bandwidth, baseband, and broadband. Students will also be able to describe several Ethernet standards and compare the benefits and limitations of different networking media. Students will additionally explore connectors, converters, and couplers for each cabling type, and will conclude with an examination of common cable problems and the tools used for troubleshooting those problems.

The third section of this unit, Wireless Networking, examines how nodes exchange wireless signals and identifies potential obstacles to successful wireless transmission. It describes WLAN (wireless LAN) architecture and specifies the characteristics of popular WLAN transmission methods. In this section students will learn how to install and configure wireless access points and clients, manage wireless security concerns, and evaluate common problems experienced with wireless networks.

The section on Cloud Computing and Remote Access will introduce students to the growing fields of cloud computing and remote access, IT innovations that touch nearly every industry. Students will also investigate the protocols, standards, and techniques for securing data in transit and for authenticating those clients are who they say they are.

Finally, the section on Network Risk Management focuses on how networks have become more geographically distributed and heterogeneous, increasing the risk of their misuse. Students will consider the largest, most

heterogeneous network in existence: the Internet. Students will explore and discuss the millions of points of entry, millions of servers, and millions of miles of transmission paths, exacerbating the vulnerability to millions of break-ins. Students will research the threat of an outsider accessing an organization's network via the Internet, and then stealing or destroying data using case studies and current examples. In this section, students will learn how to assess a network's risks, how to manage those risks, and, perhaps most important, how to convey the importance of network security to the rest of the organization through an effective security policy.

Unit 3 - IT Essentials

Students develop a working knowledge of how computers operate, how to assemble computers, and how to troubleshoot hardware and software issues. Students will expand learning onto mobile device hardware and software configuration, plus diagnostics and common security threats and vulnerabilities. There will be an emphasis on the practical application of skills and procedures needed for hardware and software installations, upgrades, and troubleshooting. The Cisco Packet Tracer simulation-based learning activities promote the exploration of networking and network security concepts while allowing students to experiment with network behavior. Online assessments provide immediate feedback to support the evaluation of knowledge and acquired skills. This unit helps students develop the career skills needed to successfully communicate within an ICT business environment and interact with customers.

Unit 4 - Network Performance and Enterprise Networking

This unit begins with the topic of Unified Communications and Network Performance Management. In this section students will learn how to optimize networks for today's high-bandwidth needs, and to protect your network's performance from faults and failures.

Following this, students will learn about Network segmentation and Virtualization which takes the divide-and-conquer approach to network management. Students will learn that when done well it increases both performance and security on a network. Students will also learn about two ways to logically segment at network, subnets, and virtual LANs, which are both used when dividing a large LAN (broadcast domain) into multiple LANs. Fundamentally, a subnet is a group of IP addresses, and a VLAN is a group of ports on a switch. These two forms of network segmentation are used in conjunction with each other, but students will learn about them separately first. Additionally, students will learn about other virtual network components, such as switches, routers, and firewalls. This section also includes an explanation of the benefits of network segmentation and then discusses how subnet masks are used.

This unit addresses Wide Area Networks, describing them as a network that connects two or more geographically distinct LANs. One might assume that WANs are the same as LANs, only bigger. Students will learn that although a WAN is based on the same principles as a LAN, including reliance on the OSI model, its distance requirements affect its entire infrastructure. As a result, WANs differ from LANs in nearly every respect.

This unit discusses the technical differences between LANs and WANs and describes WAN transmission media and methods in detail. It also notes the potential pitfalls in establishing and maintaining WANs. In addition, it introduces various wireless WAN technologies, including WiMAX, HSPA+, LTE, and satellite communications.

Finally, students will investigate Industrial and Enterprise Networking. Students will learn about a special kind of network, an industrial network, which involves specialized equipment and needs. This chapter also covers the special needs of enterprise networks in large organizations. These organizations often require that network administrators follow a formal change management process when making changes to the network and its computers. Such a system often includes extra documentation and detailed approval and deployment processes. The unit also discusses some physical security controls that are most often found in larger, enterprise-scale networks, and concludes with information on disaster recovery and forensics.

Unit 5 - Introduction to Security

Introduction to Security introduces students to the network security fundamentals that form the basis of the Security+ certification. It begins by examining the current challenges in computer security and why security is so difficult to

achieve. The unit then defines information security in detail and explores why it is important. Finally, the unit looks at the fundamental attacks, including who is responsible for them, and defenses.
Malware and Social Engineering Attacks are also studied in this unit. This section examines attacks that use different types of malwares, such as viruses, worms, Trojans, and botnets. It also looks at the different type of social engineering attacks.
Application and Networking-Based Attacks continues the discussion of threats and vulnerabilities from the previous unit's coverage of malware and social engineering. First this section looks at attacks that target server-side and client-side web applications; then it explores some of the common attacks that are launched against networks today. Finally, in Host, Application, and Data Security students will look at security for host systems achieved through both physical means and technology. They will also examine devices beyond common general-purpose computers, followed by an exploration of application security. Finally, students will look at how securing the data itself can provide necessary protections.

Unit 6 - Cryptography and Network Security
Basic Cryptography explores how encryption can be used to protect data. This unit covers what cryptography is and how it can be used for protection, and then examines how to protect data using three common types of encryption algorithms: hashing, symmetric encryption, and asymmetric encryption. It also covers how to use cryptography on files and disks to keep data secure.
Advanced Cryptography examines digital certificates and how they can be used. Students will look at public key infrastructure and key management. This section covers different transport cryptographic algorithms to see how cryptography is used on data that is being transported.
Network Security Fundamentals explores how to secure a network through standard network devices, through network technologies and by network design elements.
And finally, administering a Secure Network looks at the techniques for administering a network. This includes understanding common network protocols and employing network design principles. It also looks at securing three popular types of network applications: IP telephony, virtualization, and cloud computing.

Unit 7 - Mobile Security, Access Control, and Identity Management
This unit begins by looking at Wireless Network Security by having students investigate the attacks on wireless devices that are common today and explores different wireless security mechanisms that have proven to be vulnerable. It also covers several secure wireless protections.
The unit then moves into Mobile Device Security where students look at the different types of mobile devices and the risks associated with these devices. It also explores how to secure these devices and the applications running on them. Finally, it examines how users can bring their own personal mobile devices to work and connect them to the secure corporate network without compromising that network.
The next section of this unit explores Access Control Fundamentals which introduces the principles and practices of access control by examining access control terminology, the standard control models, and their best practices. Students learn about authentication services, which are used to verify approved users.
Finally, the section on Authentication and Account Management looks at authentication and the secure management of user accounts that enforces authentication. It covers the different types of authentication credentials that can be used to verify a user's identity and how a single sign-on might be used. It also examines the techniques and technology used to manage user accounts in a secure fashion.

Unit 8 - Compliance and Operational Security
The last unit of the course begins by looking at Business Continuity which covers the importance of keeping business processes and communications operating normally in the face of threats and disruptions. It explores disaster recovery, environmental controls, incident response procedures, and forensics.

An important part of this unit focuses on Risk Mitigation where students investigate how organizations can establish and maintain security in the face of risk. This section defines risk and the steps to control it. This section also covers security policies and the different types of policies that are used to reduce risk. Finally, students will explore how training and awareness can help provide the user with the tools to maintain a secure environment within the organization.
Vulnerability Assessment examines what vulnerability assessment is and examines the tools and techniques associated with it. Students will explore the differences between vulnerability scanning and penetration testing, as well as the risks associated with third-party integration into a system that they are examining as well as controls to mitigate and deter attacks.

3. Key Assignments:

Unit 1 - Introduction to Networking

Given a sample business scenario, students will create a “Map of Network Topology” that displays connected network devices in various rooms and buildings of the company. Working in teams, students will research and determine which IP address schemes will allow computer-to-computer communication based on provided information. Student teams will create a written report detailing how “subnet classes” can affect or improve network communications. Two teams will be assigned the same scenario so that they can present their plans to each other for comparison and feedback. As a final task for this unit, students will individually submit a written narrative of what a "Map of Network Topology" is, provide a sample map, and discuss how this type of analysis and plan would benefit a company.

Unit 2 - Networking, Cloud Computing and Risk Management

Students will develop and present a written business proposal to upgrade an existing computer system specific to meeting clients expanding needs based on scope, task, purpose, and security. The plan will specifically address wireless networking and will include techniques for securing data in transit and for authenticating users. In order to complete this assignment students will need to conduct research, collaborate with team members, synthesize relevant information, and create a concise and cohesive written proposal.

Unit 3 - IT Essentials

Given a sample troubleshooting scenario, students will perform a troubleshooting diagnostic on a personal computer and select the appropriate computer components to build, repair, or upgrade the computer. Students will write a detailed report on the issues found and develop an action plan and estimate to resolve the problem.

Unit 4 - Network Performance and Enterprise Networking

Students will be placed into teams of three to develop a computer network that includes segmentation with virtual local area networks (VLANs) in order to create a collection of isolated subsystems within the data center. Each network must be a separate broadcast domain. Students will create a power point presentation that identifies how they have configured their network specifically highlighting how the VLAN segmentation severely hinders access to system attacks, how it reduces packet-sniffing capabilities, and how it increases threat agent effort. Each group will present their findings to the rest of the class who will use a rubric to evaluate effectiveness.

Unit 5 - Introduction to Security

Students will be placed into a group of four. Each student will analyze a recent cyber security incident including the financial risk, response and business control of social media, and relational impacts. Each student will also synthesize multiple sources of information to reveal incident response times and identify the response plan defined in their specific case. Students will share their analysis with their group of four, and as a group will identify sound security practices and appropriate responses. Each group will then be given a new business scenario in which they must develop a written security/response plan based on what they have learned. The final phase of the assignment is for each group to present to the class their list of sound practices and responses and their specific business plan.

Unit 6 - Cryptography and Network Security
Students will complete this assignment in pairs after learning about Caesar ciphers. Students will use Python to write programs to decode a Caesar cipher by brute force (testing all combinations) and then using frequency analysis of the letters to narrow in on the cipher key more quickly. Modern encryption strategies are more complicated than a Caesar key, but by completing this assignment, students will explore a concrete problem that can be tested with scripts that they write independently. By exploring how difficult (or not) it is to crack Caesar cipher encryption with a computer program, students get a hands-on look at an important area of cybersecurity as well as practice writing their own code. After completing the exploration phase of the assignment students will write a short summary of what encryption is, why it is a crucial component of system security, and measures that companies can take to ensure that their encryption methods are adequate to protect their company or agency against intrusion.

Unit 7 - Mobile Security, Access Control, and Identity Management
Students will work in teams of two to create a "mobile device security plan" and infographic for a simulated company. This plan must include steps to follow in order to create a secure practice using the company's mobile devices (minimum of 5 steps) as well as the reason why to follow each step. The final plan will be graphically illustrated on a visually pleasing infographic that could be distributed to employees and displayed throughout the company.

Unit 8 - Compliance and Operational Security
Students will practice the formal procedure of system/network security analysis and planning, to examine the vulnerability and security need of a university campus network, and to devise strategies to overcome system vulnerability.

To complete this assignment, the target network that students will examine is a simple Internet deployed on the campus of a small university. Students will be given written descriptions of the sub-networks involved as well as a system topology of the overall network. The Internet is divided into four sub-networks, each of which has its own internet address range.

This assignment contains the following three consecutive parts:

1. Vulnerability Assessment — In this part, students are asked to identify potential weakness (vulnerability) of this campus Internet, and of its individual sub-networks.
2. Security Service Selection — In this part, students are asked to propose prioritized set of services to amend the vulnerability of individual sub-networks and hence the overall campus Internet. Note that the proposed services must be prioritized so that they can be implemented in proper order under existing financial constraints.
3. Network Architecture Recommendation — In the process of vulnerability analysis and security service selection, students may discover weak points in the current network architecture. They may also discover the need to implement selected security services at some crucial sites in the network. Students will work in teams to create a written report of their finding of network architecture weakness and security deployment sites.

This assignment was developed by John K. Zao and can be found in its entirety at:

https://people.cs.nctu.edu.tw/~jkzao/Lecture/InetSec%2094S/Assign%201%20-%20Security%20Analysis%20+%20Planning%20(Zao%200510).pdf

4. Instructional Methods and/or Strategies:
To assist with learning and demonstrating mastery of content, students will, throughout this course, be engaging in close reading and annotation of complex text, collaborating with peers to complete research and tasks, and completing

informal and formal writing assignments. Speaking and writing scaffolds and templates will be used to support English Language Learners and students with disabilities.

5. Assessment Including Methods and/or Tools:

The evaluation of student progress and evaluation will be based on the following criteria outlined in Board Policy:

- Assessments: 60-75% of the final grade
- Assignments and class discussions: 25-40% of the final grade