CYBERSECURITY 2 OUTLINE

1. Key Standards or Course Competencies

First Quarter Key Standards or Course Competencies:

CSTA Standards - https://www.csteachers.org/page/standards
CTE State Plan for Cyber 2: http://coloradostateplan.com/wp-content/uploads/2020/05/Level-3-Cybersecurity-II.pdf
CDE State Standards: https://www.cde.state.co.us/apps/standards/12,15,0
National Cyber Standards:
https://drive.google.com/file/d/1EiX6U8J6kaLisJaWmDB3h-V_fcPm9BQb/view?usp=sharing

Topics for Quarter 1

Topic	CDE CS Standard	National Cyber Standards	CSTA Standards
Linux	2-4-4:Systems thinking is a way of holistically examining the various components and use cases that go into a given design.	5.3.2: Students will identify the processes of developing secure software. 6.1.3: Students will identify and explain how different system components impact the cybersecurity of a system design 8.1.2: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security.	1A-CS-01: Select and operate appropriate software to perform a variety of tasks, and recognize that users have different needs and preferences for the technology they use.
Python	3-7-1: The creation of a computer program requires a design process.	5.3.2	1A-CS-01
Legal/Ethical	2-4-1:Communication between computers (and over the internet) can be configured in many different ways and consist of several hardware and software components. 3-8-5: Computing solutions can have impacts (personal, ethical, social, economic and cultural) based on their use.	1.1.1: Students will analyze online and offline behaviors in societies, i.e., themselves, peers, families, communities, and countries, and deduce the values that govern these behaviors. 1.1.2: Students will understand how the role of values and ethics affects	3A-IC-24: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices. 3B-IC-28: Debate laws and regulations that impact the development and use of software.

	3-8-6: Security and software licensing can present constraints and restrictions in computational design and development.	political structures, laws, and policy decisions as it relates to cybersecurity. 1.3.2: Students will discuss how ethical obligations to society always coexist with ethical obligations to one's family, friends, employer, local community, and even oneself. 1.3.3: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical. 4.2.1: Students will compare and contrast data protection legislation, policies, and procedures that have been or are being introduced all over the world to protect personal Data. 8.1.1: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.	
Networking	1-3-6:Data can be represented in different ways for storage and exchange. 2-4-1 3-8-6	3.1.1: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers. 3.1.2: Students will explain how network standards and protocols allow different types of devices to communicate 3.2.2: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the	3A-NI-04: Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.

		transport layer, and the application layer.	
CIA Triad	2-4-4 2-6-7: Robust computing systems require data protection. 3-8-5	1.1.1 1.3.1: Students will explore the tensions that exist between transparency, autonomy, resilience and security. 2.1.1: Students will evaluate methods of keeping information secret from those whom the information should be kept secret. 2.1.2: Students will demonstrate that integrity involves trust and credibility. 2.2.1: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure. 2.3.4: Students will define the principle of least privilege 2.3.6: Students will know that the principle of data hiding 7.1.2: Students will be able to identify and prioritize the protection of information assets.	3A-NI-07: Compare various security measures, considering tradeoffs between the usability and security of a computing system. 3A-NI-08: Explain tradeoffs when selecting and implementing cybersecurity recommendations.

Second Quarter Key Standards or Course Competencies:

Topics for Quarter 2

Topic	CDE CS Standard	National Cyber Standards	CSTA Standards
Footprinting	1-3-8:Data from a computer program can be visually presented to better understand and articulate	3.2.2 5.3.1: Students will describe common security-related	3B-NI-04:Compare ways software developers protect devices and information from

	solutions to a problem. 2-4-4	software vulnerabilities. 7.1.4: Students will be able to conduct standard security testing and assessments.	unauthorized access.
Scanning Networks	1-2-4: Large, complex problems can be broken down into smaller, more manageable components. 1-3-6 2-4-1 2-4-4 2-6-7	1.3.1 3.1.2 5.3.1 6.2.2: Students will explain how intentional attacks can adapt to defenses and cause a system to fail. 7.1.4	3A-NI-04 3A-NI-05: Give examples to illustrate how sensitive data can be affected by malware and other attacks.
Enumeration	1-3-6 2-4-1 2-4-4 3-8-6	2.1.2 2.3.4 2.3.6	
System Hacking	1-2-4 1-3-8 2-4-1 2-4-4 2-6-7 3-8-5	2.1.3: Students will evaluate methods of protecting information and information systems from disruption and Destruction. 6.2.3: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking 7.1.4	3A-NI-04
Sniffing	1-2-4 1-3-8	1.3.1 3.2.1: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. 7.1.4	

Third Quarter Key Standards or Course Competencies:

Topics for Quarter 3

Topic	CDE CS Standard	National Cyber Standards	CSTA Standards
Malware	2-4-1 2-4-4	2.2.2: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts. 2.3.4 5.3.1 5.3.2	3A-NI-05
Social Engineering	2-6-7 3-8-6	1.1.1 1.1.2 1.3.1 2.1.2 2.2.1 2.3.4 6.1.4: Students will understand how social behaviors and human factors impact the cybersecurity of a system design.	
Cryptology	1-3-6 2-4-1 2-6-7 3-8-6	2.1.1: Students will evaluate methods of keeping information secret from those whom the information should be kept secret. 2.1.2 4.3.1: Students will define cryptography and explain how it is used in data security. 4.3.3: Students will employ public key (asymmetric) encryption and explain how it works.	
Create Incident Reports	1-2-4: Large, complex problems can be broken down into smaller, more manageable components. 1-3-7:Many problems appropriate for solving	2.2.1 2.3.1: Students will give examples of the principle of domain separation, which allows for the	3A-CS-03: Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix

	with a computer are organized around patterns. 2-4-4 2-6-6: Robust computing systems require multiple methods of recovery. 3-8-5:	enforcement of rules governing the entry and use of domains by entities outside the domain. 4.1.1: Students will analyze existing data security concerns and assess methods to overcome those concerns. 4.2.3: Students will evaluate and recommend technical controls that can be used to secure data. 5.3.1 7.1.4 8.1.1	errors. 3A-NI-05 3A-NI-06: Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts. 3A-NI-07 3A-NI-08:

Fourth Quarter Key Standards or Course Competencies:

Topics for Quarter 4

Topic	CDE CS Standard	National Cyber Standards	CSTA Standards
Wireless	1-3-6 2-4-1 2-6-7 3-8-5: 3-8-6	2.1.2 2.3.3: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact 3.1.2	3A-NI-04 3A-NI-05
Attack - Defense	1-2-4: Large, complex problems can be broken down into smaller, more manageable components. 2-4-1 2-4-4 2-6-6 2-6-7 3-8-5 3-8-6	1.1.1 1.1.2 1.3.1 2.1.2 2.2.2 2.2.3: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or	3A-NI-04 3A-NI-07

		device. 3.2.2 5.2.2: Students will identify some common hardware-related vulnerabilities. 7.1.1: Students will be able to differentiate between threats, vulnerabilities, and attacks. 7.1.4	
Architecture Design	1-3-8 2-4-1 2-4-2:Computer hardware, the lowest level of a computer system, consists of many different parts, each providing a specialized function. 2-4-4 2-5-5: Client considerations drive system design. 2-6-6 2-6-7 3-7-4: Client-based design requirements and feedback are essential to a quality computational product or service. 3-8-6	1.1.2 1.3.1 2.3.4 2.4.1: Given a scenario, students will identify the assumptions made in the design of the system 3.1.1 3.1.2	3A-NI-04 3A-NI-07 3A-NI-08:

7. Description of Benchmark Assessments

First Quarter:

Formative will include daily work to show proficiency Groups will also be used as a determination of the Colorado Essential Skills Summative assessments will include traditional tests but the majority of weight will be placed on test images. Students will be given a virtual image that matches the content for each quarter but also includes items from previous sections. This hands-on approach is a far better way to assess knowledge for this type of course.
Topics Include: Linux, Python, Legal/Ethical, CIA Triad, and networking basics.

Second Quarter:

Formative will include daily work to show proficiency Groups will also be used as determination of the Colorado Essential Skills Summative assessments will include traditional tests but the majority of weight will be placed on test images. Students will be given a virtual image that matches the content for each quarter but also includes items from previous sections. This hands-on approach is a far better way to assess knowledge for this type of course.

Topics Include: Footprinting, scanning networks, enumeration, system hacking, and sniffing.

Third Quarter:

Formative will include daily work to show proficiency Groups will also be used as determination of the Colorado Essential Skills Summative assessments will include traditional tests but the majority of weight will be placed on test images. Students will be given a virtual image that matches the content for each quarter but also includes items from previous sections. This hands-on approach is a far better way to assess knowledge for this type of course.
Topics Include: Malware, social engineering, cryptology, and incident reports.

Fourth Quarter:

Formative will include daily work to show proficiency Groups will also be used as determination of the Colorado Essential Skills Summative assessments will include traditional tests but the majority of weight will be placed on test images. Students will be given a virtual image that matches the content for each quarter but also includes items from previous sections. This hands-on approach is a far better way to assess knowledge for this type of course.
Topics Include: Wireless. attack-defense(Adversarial mindset), and architecture and design.