



Carroll ISD

Year-At-A-Glance

AP Cybersecurity

	1 st Grading Period	2 nd Grading Period	3 rd Grading Period	4 th Grading Period
Course Info	In AP Cybersecurity students will gain a deep understanding of the importance of ethical application of the knowledge and skills they have and will acquire. Students will gain the knowledge and skills required to recognize vulnerabilities, recognize the types of adversaries, recognize the types of attacks, how to recognize an attack has occurred, assess risk, manage risk, secure networks, secure devices, and secure data and applications.			
TEKS	Introduction to Security 1.1, 1.2, 1.3, 1.4, 1.5,	Unit 3 - Securing Networks	Unit 4 - Securing Devices	Unit 5 - Securing Applications and Data
Topic Focus	Unit 1 - Introduction to Security 1.1 Understanding Social Engineering 1.1.A Identify common indicators of social engineering tactics. 1.1.B Explain how social engineering tactics influence victims to perform a desired action. 1.1.C Describe possible impacts for victims of social engineering attacks. 1.2 Suspicious Wi-Fi Login	Unit 3 - Securing Networks 3.1 Network Vulnerabilities and Attacks 3.1.A Identify common network attacks. 3.1.B Explain how adversaries can exploit network vulnerabilities to steal, disrupt, or destroy network communication. 3.1.C Assess and document risks from	Unit 4 - Securing Devices 4.1 Detecting Network Attacks 4.1.A Identify types of computing devices. 4.1.B Identify the type of malware used in a cyberattack. 4.1.C Explain how adversaries can exploit common device vulnerabilities to cause loss, damage, disruption, or destruction. 4.1.D Assess and document risks from	Unit 5 - Securing Applications and Data 5.1 Application and Data Vulnerabilities and Attacks 5.1.A Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction. 5.1.B Explain how application attacks exploit vulnerabilities. 5.1.C Assess and document risks from application and data vulnerabilities. 5.2 Protecting Applications and Data: Managerial Controls and Access Controls 5.2.A Explain how the state or classification of data impacts the type and degree of security applied to that data.



Carroll ISD

Year-At-A-Glance

AP Cybersecurity

	○ 1.2.A Identify common signs of a password attack. ○ 1.2.B Explain how adversaries take advantage of weak authentication. ○ 1.2.C Explain how to make authentication stronger. ● 1.3 Dangers of Public Wi-Fi ○ 1.3.A Identify the type of adversary conducting a cyberattack. ○ 1.3.B Identify types of wireless cyberattacks. ○ 1.3.C Describe actions individuals can take to increase protection of sensitive data when using the internet and Wi-Fi ● 1.4 AI-Based Cybersecurity Attacks ○ 1.4.A Explain how adversaries use AI-powered tools to augment cyberattacks.	○ network vulnerabilities. ● 3.2 Protecting Networks: Managerial Controls and Wireless Security ○ 3.2.A Identify managerial controls related to network security. ○ 3.2.B Configure wireless network security features. ● 3.3 Protecting Networks: Segmentation ○ 3.3.A Identify techniques for segmenting a network. ○ 3.3.B Explain why network segmentation can increase network security. ● 3.4 Protecting Networks: Firewalls	○ device vulnerabilities. ● 4.2 Authentication ○ 4.2.A Explain why hashes (also called hash outputs, checksums, message digests, or digests) are used to store passwords. ○ 4.2.B Explain how password attacks exploit vulnerabilities. ○ 4.2.C Determine the type of authentication used to verify the identity of a user. ○ 4.2.D Configure login settings to make a device more secure. ● 4.3 Protecting Devices ○ 4.3.A Identify managerial controls related to device security.	○ 5.2.B Identify managerial controls related to application and data security. ○ 5.2.C Determine an appropriate access control model to protect applications and data. ○ 5.2.D Configure access control settings on a Linux-based system. ● 5.3 Protecting Stored Data with Cryptography ○ 5.3.A Explain how encryption can be used to protect files. ○ 5.3.B Apply symmetric encryption algorithms to encrypt and decrypt data. ● 5.4 Asymmetric Cryptography ○ 5.4.A Determine the appropriate asymmetric key to use when sending or receiving encrypted data. ○ 5.4.B Explain why the length of a key impacts the security of encrypted data. ○ 5.4.C Apply asymmetric encryption algorithms to encrypt and decrypt data. ● 5.5 Protecting Applications ○ 5.5.A Identify the application security principles of secure by design and security by default.
--	---	---	---	---



Carroll ISD

Year-At-A-Glance

AP Cybersecurity

	○ 1.4.B Explain how to protect against some AI-augmented cyberattacks. ● 1.5 Leveraging AI in Cyber Defense ○ 1.5.A Explain how cyber defenders can leverage AI-powered tools to protect networks, applications, and data. ○ 1.5.B Explain how AI-powered tools are enabling faster and more accurate threat detection and response.	○ 3.4.A Identify types of network-based firewalls. ○ 3.4.B Explain how a firewall uses an access control list to allow or deny traffic entering or leaving a network. ○ 3.4.C Determine the effective placement of firewalls in a network. ○ 3.4.D Configure a firewall to manage the flow of network traffic.	○ 4.3.B Explain how anti-malware software can make a device more secure. ○ 4.3.C Explain why keeping a device's operating system and software updated makes it more secure. ○ 4.3.D Configure a host-based firewall. ● 4.4 Detecting Attacks on Devices ○ 4.4.A Explain how to detect attacks against devices. ○ 4.4.B Determine controls for detecting attacks against a device. ○ 4.4.C Evaluate the impact of a device detection method. ○ 4.4.D Apply detection	○ 5.5.B Explain how user input sanitization protects applications. ● 5.6 Detecting Attacks on Applications and Data ○ 5.6.A Explain how to detect attacks on data. ○ 5.6.B Determine controls for detecting attacks against applications or data. ○ 5.6.C Evaluate the impact of a method for detecting attacks against an application or data. ○ 5.6.D Identify whether a file has been altered by verifying its hash. ○ 5.6.E Apply detection techniques to identify and report indicators of application attacks by analyzing log files.
Unit 2	● 2.1 Cyber Foundations ○ 2.1.A Identify social engineering attacks. ○ 2.1.B Identify types of adversaries. ○ 2.1.C Describe the phases of a cyberattack. ○ 2.1.D Describe the risk	● 3.5 Detecting Network Attacks ○ 3.5.A Identify types of automated security tools used to detect		



Carroll ISD

Year-At-A-Glance

AP Cybersecurity

	assessment process. ○ 2.1.E Identify strategies for managing risk. ○ 2.1.F Identify types of security controls. ○ 2.1.G Explain why a defense-in-depth security strategy is necessary to optimally protect an organization. ● 2.2 Physical Vulnerabilities and Attacks ○ 2.2.A Identify common physical attacks. ○ 2.2.B Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets. ○ 2.2.C Assess and document risks from physical vulnerabilities. ● 2.3 Protecting Physical Spaces ○ 2.3.A Identify managerial	network attacks. ○ 3.5.B Explain how organizations can leverage artificial intelligence (AI) to enhance threat detection and response. ○ 3.5.C Determine a network detection method. ○ 3.5.D Evaluate the impact of a network detection method. ○ 3.5.E Apply detection techniques to identify indicators of network attacks by analyzing log files.	techniques to identify indicators of password attacks by analyzing log files.	
--	---	--	--	--



Carroll ISD

Year-At-A-Glance

AP Cybersecurity

	- controls related to physical security. ○ 2.3.B Determine mitigation strategies for risks from physical vulnerabilities. ● 2.4 Detecting Physical Attacks ○ 2.4.A Identify ways security controls can detect physical attacks. ○ 2.4.B Determine effective placement of security controls for detecting physical attacks. ○ 2.4.C Apply detection techniques to identify physical attacks.			
Additional Resources	Unit 1 Unit 2	Unit 3	Unit 4	Unit 5



tes Power Standards

Carroll ISD Year-At-A-Glance AP Cybersecurity

DRAFT Date