Computing Systems and Security

Design Brief for Standards Writers

SUGGESTED CITATION: Computer Science Teachers Association. (2026). *Computing systems and security: Design brief for standards writers*. https://csteachers.org/k12standards/research

This design brief focuses on the following learning outcomes for the Computing Systems and Security topic area described in the *Reimagining CS Pathways* report:

- **CS.1** Identify various types of hardware (including components) and software (including operating systems)
- **CS.2** List security practices (e.g., safe passwords, two-factor authentication)
- **CS.3** Explain what networks (including the Internet) are and how they work
- **CS.4** Explain how an operating system, other software, and hardware work together
- **CS.5** Describe why cybersecurity is important
- **CS.10** Describe vulnerabilities in networks

Design Recommendations

Based on our analysis of overlaps between the K–12 Cybersecurity Learning Standards and the Computer Science Teachers Association (CSTA) K–12 Computer Science Standards, as well as a comprehensive literature review, we have the following recommendations for the revised CSTA Computer Science standards in Computing Systems and Security.

Grade Band	Design Recommendations
Not Grade Specific	**Security** and **Networks:** Students need an understanding of networked communication in order to understand encryption mechanisms. For example, knowledge of HTTPS (Hypertext Transfer Protocol Secure) and the TLS (Transport Layer Security) protocol is useful in understanding data confidentiality and authentication online. When drafting Security standards, consider whether the standards require a particular understanding of networks and verify that knowledge is covered in the Networks standards. ***Consider whether to include the following topics***: Cyberbullying, Digital Footprint, Internet of Things, Cloud Computing, and Data Loss.
Elementary	**Hardware/Software:** Students should know the components or parts of computing devices. **Security:** Students should know what a good password is and understand the importance of strong passwords. They should also understand what personal information is and how to protect it. **Networks:** Students should know about different network access methods, including those they may not encounter in their daily lives. **Internet as a Network:** Students should know that the Internet is different from the devices used to access it and from the activities it facilitates. They should also be able to distinguish online activities from offline activities. **Data Flow:** Students should have a basic understanding of downloading and sending data.

Grade Band	Design Recommendations
Middle	**Security:** Students should be knowledgeable about ways to physically and digitally keep devices and information secure. Digital security knowledge should include methods of cryptography to securely transmit data. **Troubleshooting:** Students should (a) be able to form a comprehensive view of the computing systems they work with and (b) know how to navigate various representations of computing systems (e.g., the physical computing artifact, paper-based representations, code). **Networks:** Students should have knowledge about protocols used to transmit data across networks. Students should understand the concept of a modular network with various networking devices (e.g., routers, switches, base transceiver stations) that function as data crossroads. **Internet as a Network:** Students should understand that the Internet is a network of networks with specific servers and connections. **Data Flow:** Students should know about factors influencing connection speed of networks.
High	**Security:** Students should have knowledge of the roles of software and software developers in keeping devices and information secure. They should also be knowledgeable of different security measures (including encryption), understand the strengths and weaknesses of the measures, and understand potential security threats. **Troubleshooting:** Students should know how to identify and address bugs in syntax, logic, and physical components. **Networks:** Students should have knowledge about threats and vulnerabilities, including attacks that affect the security of sensitive data.

Recommended K–12 Cybersecurity Learning Standards to Add to the Revised CSTA CS Standards for Computing Systems and Security

	K–2	3–5	6–8	9–12
Cyberbullying	**K–2.DC.CYBL** Discuss examples of cyberbullying and model age-appropriate responses to cyberbullying.	**3–5.DC.CYBL** Discuss and demonstrate examples of cyberbullying and methods of age-appropriate intervention.	**6–8.DC.CYBL** Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying.	**9–12.DC.CYBL** Prepare a plan to raise awareness of the effects of cyberbullying.
Digital Footprint	**K–2.DC.FOOT** Differentiate between good and bad online behavior.	**3–5.DC.FOOT** Describe the concept of a digital footprint.	**6–8.DC.FOOT.1** Recognize the many sources of data that make up a digital footprint. **6–8.DC.FOOT.2** Recognize the permanence of a digital footprint.	**9–12.DC.FOOT** Examine the implications of both positive and negative digital footprints.
Internet of Things	**K–2.CS.IOT** Identify examples of devices that are part of the Internet of Things.	**3–5.CS.IOT** Define the Internet of Things.	**6–8.CS.IOT** Evaluate the risks and benefits of Internet of Things devices.	**9–12.CS.IOT** Analyze the vulnerabilities of Internet of Things devices.
Cloud Computing	**K–2.CS.CC** State the benefits of storing and sharing information using cloud computing.	**3–5.CS.CC.1** Demonstrate ways to store and share information using cloud computing. **3–5.CS.CC.2** Demonstrate safe cloud computing practices.	**6–8.CS.CC** Identify the advantages and disadvantages of various cloud computing models.	**9–12.CS.CC** Evaluate the risks and benefits of cloud computing.
Data Loss	**K–2.CS.LOSS** Define data loss and service outages.	**3–5.CS.LOSS** Explain the role and importance of backups (e.g., via auto-save features).	**6–8.CS.LOSS** Explain the role and importance of backups (e.g., via redundant systems).	**9–12.CS.LOSS** Develop a plan for risk mitigation that implements redundancy.

For more information on these design recommendations, go to https://csteachers.org/k12standards/research. See the following sections of *Comparison of CSTA Standards to Other Standards and Frameworks*: K–12 Cybersecurity Learning Standards (pp. 16–21) and Computing Systems and Security (pp. 64–65).

Computing Systems and Security

Aligned Learning Progressions

Aligned Computing Systems and Security Learning Progressions for CSTA K–12 CS Standards and K–12 Cybersecurity Learning Standards

The learning progressions in the following pages are the most closely related topics for Computing Systems and Security.

	Summary of Related CSTA K–12 CS Standards	Summary of Related K–12 Cybersecurity Learning Standards
K–2	**1A-NI-04** Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.	**K–2.SEC.AUTH** Describe the concept of a good password and its importance.
	1A-CS-02 Use appropriate terminology in identifying and describing the function of common physical components of computing systems (hardware).	**K–2.CS.HARD** Identify the components or parts of computing devices.
3–5	**1B-NI-05** Discuss real-world cybersecurity problems and how personal information can be protected.	**3–5.DC.PPI** Define personally identifiable information (PII). **[6–8].DC.PPI.2** Examine techniques to detect, correct, and prevent disclosure of PII. **[9–12].DC.PPI.1** Explain the importance of social identity and the implications of online activity regarding private data, long-term career impacts, and the permanence of digital data.
6–8	**2-NI-05** Explain how physical and digital security measures protect electronic information.	**6–8.SEC.ACC** Explain the concept of access control and how to limit access to authorized users. **[K–2].SEC.CIA** Identify the concepts of Confidentiality, Integrity, and Availability as presented in the CIA Triad. **[3–5].SEC.CIA** Describe the concepts of the CIA Triad and how they work to protect information. **[3–5].SEC.ACC** Describe the concept of appropriate access to private information. **[9–12].SEC.DATA** Formulate a plan to apply security measures to protect data in all three states. **[9–12].SEC.INFO** Distinguish the different types of attacks that affect information security for individuals and organizations.

	Summary of Related CSTA K–12 CS Standards	Summary of Related K–12 Cybersecurity Learning Standards
6–8	**2-NI-06** Apply multiple methods of encryption to model the secure transmission of information.	**6–8.SEC.CRYP** Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.
	2-NI-04 Model the role of protocols in transmitting data across networks and the Internet.	**6–8.CS.PROT** Identify the protocol connection types used for different services available online. **[9–12].CS.PROT.1** Compare and contrast the ports and protocols used for different services available online.
9–10	**3A-NI-08** Explain tradeoffs when selecting and implementing cybersecurity recommendations.	**9–12.SEC.COMP** Evaluate Defense in Depth strategies that can protect simple networks. **9–12.SEC.CTRL** Justify the use of Defense in Depth and the need for physical access controls. **9–12.SEC.AUTH** Evaluate authentication and authorization methods and the risks associated with failure. **9–12.SEC.DATA** Formulate a plan to apply security measures to protect data in all three states.
	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.	**9–12.SEC.INFO** Distinguish the different types of attacks that affect information security for individuals and organizations. **[6–8].SEC.INFO** Analyze threats and vulnerabilities to information security for individuals and organizations.
11–12	**3B-NI-04** Compare ways software developers protect devices and information from unauthorized access.	**[6–8].CS.APPS** Discuss the role that software plays in the protection of a secure system.