K12 CYBERSECURITY Learning Standards

K-12 Cybersecurity Learning Standards project supported by:

CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

This original version of the K-12 Cybersecurity Learning Standards was published on August 4, 2021. Future versions of this document will include revision numbers after the version.

Table of Contents

Foreword

As the United States faces an onslaught of increasingly sophisticated cyberattacks, the nation lacks the workforce needed to combat these threats. There is a shortfall of over 464,000 cybersecurity professionals nationwide, as the global cybersecurity workforce shortage is projected to reach 1.8 million unfilled positions by 2022. There is a real and urgent need to grow the cybersecurity workforce, and this begins with expanding K-12 cybersecurity education and improving student cybersecurity literacy nationwide. It is imperative that the next generation workforce has the skills and knowledge needed to enter into the cybersecurity workforce and that all students grow up to be good digital citizens that will live, work and play in cyberspace safely and ethically.

To help solve this problem, CYBER.ORG partnered with K-12 educators, higher education faculty, the cybersecurity industry and government to create the first-ever national K-12 Cybersecurity Learning Standards. The standards are designed to help teachers introduce students to the foundational concepts of cybersecurity, and provide them with the technical skills and knowledge needed to pursue cybersecurity careers in greater numbers. The standards establish the learning goals for what students should know and be able to do at each grade level.

As the first national effort to provide cybersecurity learning standards to all 50 states, this resource will give educators a comprehensive road map to teach cybersecurity concepts across grade levels. The standards provide curriculum developers and teachers on the ground with the resources they need to provide every student with a robust cyber education.

This CYBER.ORG-driven effort is a part of the organization's mission to address the growing cybersecurity workforce crisis by increasing foundational cybersecurity awareness and interest in the cybersecurity profession, ultimately building a larger and more diverse pipeline of individuals entering the cybersecurity field. CYBER.ORG's K-12 Cybersecurity Learning Standards initiative is critical to guaranteeing that the future cybersecurity workforce is equipped to handle the cybersecurity challenges of tomorrow.

Development Model

After contracting with McREL International to help develop the standards, CYBER.ORG began the search for both standards development and review committee members. After receiving overwhelming support from the organization's more than 22,000 teachers-in-network, CYBER.ORG selected thirty educators and higher education partners to assist with the development of the standards and twenty local, state, and federal partners to assist with the standards review process.

The standards development process was split into several sessions. The development team analyzed other published models and sample standards documents to help develop the format for the standards. The draft document was evaluated by the review committee, and two rounds of their comments were incorporated into drafts by the writing team.

At the close of the development process, the standards were also made available to the public for review. During the open comment period, nearly two dozen responses were received across all grade and content areas of the standards. Each comment was reviewed by the CYBER.ORG team and incorporated into the final standards.

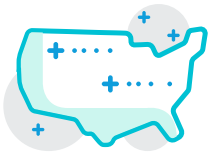
The K-12 cybersecurity learning standards center around three core themes – Computing Systems (CS), Digital Citizenship (DC), and Security (SEC) – all of which represent key fundamentals in cybersecurity education.

Computing Systems (CS)	Digital Citizenship (DC)	Security (SEC)
Communication and Networking	Online Safety	Information Security
Network Communication (COMM)	Cyberbullying (CYBL)	CIA Triad (CIA)
Network Components (COMP)	Digital Footprint (FOOT)	Access Control (ACC)
Cloud Computing (CC)	Public and Private Information (PPI)	Data Security (DATA)
Protocols (PROT)	Ethics	Threats and Vulnerabilities (INFO)
Data Loss (LOSS)	Threat Actors (THRT)	Cryptography (CRY)
Hardware	Ethical Integrity (ETH)	Network Security
Network Hardware Components (HARD)	Policy and Legal Issues	Authentication (AUTH)
Internet of Things (IOT)	Rules, Laws, and Regulations (LAW)	Securing Network Components (COMP)
Operating Systems (OS)	Intellectual Property (IP)	Threats and Vulnerabilities (NET)
Software	Usage and User Agreements (AUP)	Physical Security
Software Updates (SOFT)		Threats and Vulnerabilities (PHYS)
Programming and Scripting (PROG)		Security Controls (CTRL)
Applications (APPS)		

Vision for Implementation

The K-12 Cybersecurity Education Standards have been designed with usability in mind. CYBER.ORG has designed the standards to be comprehensive, easy to use, and easy to find. States, districts, and all educators will be able to use the standards. They are available for wholesale adoption and are available for districts and educators to incorporate into existing curricula opportunities or course standards. The table below showcases eight different ways the standards can be implemented.






Use by Teachers	Use by School Districts	Use by State Departments of Education	Use by Informal Education Partners
Teachers can use the standards to guide and shape the instruction that will take place inside the classroom	Standards can be used to shape cyber-based pathways for students at any grade level and Career and Technical Education opportunities specifally at the high school level	States can use the standards to establish state-wide pathways in cyber education.	Community partners can embed standards into afterschool, weekend, or summer cam opportunities for students
Teachers can scaffold the learning to ensure students graduate from high school as cyber-literate students	Districts can support all educators (science, math, English, and social studies) to integrate cybersecurity into the classroom	Standards can be adopted for use within existing Computer Science and core subject standards	Standards can support connections of extra curricular opportunities to workplace expectations

CYBER.ORG is a cybersecurity workforce development organization that targets K-12 students with cyber career awareness, curricular resources, and teacher professional development. The United States Department of Homeland Security (DHS) supports CYBER.ORG through a grant from the Cybersecurity Infrastructure and Security Agency (CISA) to develop and distribute cybersecurity education content to educators across the country at no cost.

For more information, visit
www.CYBER.ORG/standards

Acknowledgments

Writers

Shendolyn Anderson
Dallas Independent School District
Duncanville, TX

Bobbie Bastian
Future Forward at Bollman
Thornton, CO

Kathleen Bellew
MOREnet
Columbia, MO

Tom Bonzon
Los Alamos Middle School
Rio Rancho, NM

Terry Braught
Center for Advanced Learning
Damascus, OR

Dr. Patrick Carter
Mater Academy East
Henderson, NV

Dr. Bernard Chen
University of Central Arkansas
Conway, AR

Carrie Day
Matanuska-Susitna Borough School District
Palmer, AK

Charlotte Dungan
North Carolina School of Science and Mathematics
Durham, NC

Keith George
Auburn University – Montgomery
Owens Cross Roads, AL

Robert Gibson
Sussex Central High School
Lewes, DE

Janet Hartkopf
Chandler Unified School District
Chandler, AZ

Willie Henderson
Caddo Parish Schools
Shreveport, LA

Nikki Hendricks
Texas Advanced Computing Center (TACC)
Austin, TX

Kitty Herbel
Enid Public Schools
Enid, OK

LaNessa Hof
St. Mary Catholic School
Dell Rapids, SD

Carolyn Hughes
Robert McQueen High School
Reno, NV

Dr. Doug Jacobson
Iowa State University
Ames, IA

Sarah Lee
Ladera Vista Junior High School of the Arts
La Mirada , CA

Marie Lewis
Manvel High School
Friendswood, TX

Andy Lindsay
Parallax
Rocklin, CA

Diana Mackiewicz
Eagle Hill School
Wales, MA

Dr. Deborah Marshall
Norfolk Public Schools
Newport News, VA

Monika Moorman
Broward County Public Schools
Plantation, FL

Billy Neill
Bossier Parish Schools
Bossier City, LA

Liz Owens
Episcopal Day School
North Augusta, GA

Lisa Oyler
Summit Technology Academy
Lee's Summit, MO

Duane Seward
Granby High School
Portsmouth, VA

Tabitha Teel
State of North Dakota Information Technology Department
Bismarck, ND

Dr. Thomas Trevethan
Palo Alto Networks
Norfolk, VA

Dr. John Underwood
East Baton Rouge Parish Schools
Baton Rouge, LA

Affiliations are for identification purposes and do not imply institutional or company endorsement. The views, thoughts, and opinions expressed in the text of this document belong solely to the individual author(s), serving in each author(s) respective individual capacity, and do not necessarily reflect the official policy or position of the author's employer, agency, company organization, committee, or other group or individual.

Reviewers

Kara Four Bear
Eagle Butte School District

Dr. Jeff Gray
University of Alabama

Kyla Guru
Bits N' Bytes CySec Education

Jeff Holcomb
Caddo Parish Schools

LTC Robert Hyver
Army - JROTC

Leigh Ann Jervis DeLyser
CSforAll

Dr. Terrie Johnson
Centenary College

Cortez Lake
Tenable

Mark Loepker
National Cryptologic Museum Foundation

Diane Madden
Louisiana Tech University

Jennifer Cramer Marden
Loudon County School District

Latasha McCord
Cybersecurity and Infrastructure Security Agency

Matt Morales
Office of the Maricopa County School Superintendent

Ross Nodurft
Venable

Kristi Rice
Spotsylvania County Public Schools

Steve Snow
North Dakota Department of Public Instruction

Allen Stubblefield
Fullerton Joint Union High School District

Dr. Lindsey Keith Vincent
Louisiana Tech University

Dr. Daphne Williams
Grambling State University

Donna Woods
Canyon Springs High School

LTC Myron Young
Army JROTC

Project Managers

David Awalt
CYBER.ORG

Betsy Callaway
McREL International

Ben Cronkright
McREL International

Callie Dean
CYBER.ORG

Claire Floyd
CYBER.ORG

Dr. Chuck Gardner
CYBER.ORG

Tonia Gibson
McREL International

Tommy Gober
CYBER.ORG

Fayce Hammond
McREL International

Heather Howle
CYBER.ORG

Joseph MacAdam
CYBER.ORG

Kevin Nolten
CYBER.ORG

Laurie Salvail
CYBER.ORG

Affiliations are for identification purposes and do not imply institutional or company endorsement. The views, thoughts, and opinions expressed in the text of this document belong solely to the individual author(s), serving in each author(s) respective individual capacity, and do not necessarily reflect the official policy or position of the author's employer, agency, company organization, committee, or other group or individual.

Structure of the Standards

The CYBER.ORG K-12 Cybersecurity Standards are arranged into three Core Concepts: **Computing Systems (CS)**, **Digital Citizenship (DC),** and **Security (SEC) .**

The Core Concepts represent major concepts or "big ideas" fundamental in cybersecurity education. Each Core Concept is divided into multiple Sub Concepts that represent specific ideas within that Core Concept. Each Sub Concept is further subdivided into multiple Topics which represent specific content areas within that Sub Concept and Core Concept. The standards are then arranged by grade band: K-2, 3-5, 6-8, 9-12.

For example, Core Concept: Security (SEC), Sub Concept: Information Security, Topic: Access Control (ACC), Grade Band: 6th grade -8th grade, Standard: 6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users. Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of why access control is needed across user platforms and what constitutes an authorized user.

Security (SEC)
Information Security
Access Control (ACC)
Kindergarten-2nd Grade
• **K-2.SEC.ACC Define access to private information.** Clarification Statement
3rd Grade–5th Grade
• **3-5.SEC.ACC Describe the concept of appropriate access to private information.** Clarification Statement
6th Grade–8th Grade
• **6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users.** Clarification Statement
9th Grade–12th Grade
• **9-12.SEC.ACC Compare and contrast the concepts presented by access control principles, access control modules, and the principle of least privilege access.** Clarification Statement

Core Concept
Subconcept
Topic
Standards by Gradeband

Sample standard by concept, subconcept, topic, & standards gradeband

Computing Systems (CS)

Communication and Networking

Network Communication (COMM)

Kindergarten–2nd Grade

- **K-2.CS.COMM.1 Define the concept of online**.

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of being online and describing various benefits of being connected through devices. Students should understand the internet is a globally networked service we connect with; it is not housed within the computer itself.

- **K-2.CS.COMM.2 Describe the difference between online and local use of computing devices.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how not everything is online, not everything can connect, networks connect devices, and the internet connects millions of devices around the world.

3rd Grade–5th Grade

- **3-5.CS.COMM Describe network communications.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of network communications as the exchange of information between connected devices.

6th Grade–8th Grade

- **6-8.CS.COMM.1 Compare and contrast network topologies.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of LAN or WAN topologies.

- **6-8.CS.COMM.2 Differentiate between a network device's MAC and IP addresses.**

  Clarification statement: Identify IP addressing schemes such as public and private IP address blocks. Students should understand a device has a built-in MAC and an assigned IP address.

9th Grade–12th Grade

- **9-12.CS.COMM Explain layers within the OSI networking model.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the seven layers of the OSI model. In addition, students should be able to explain the roles of various network layers.

Network Components (COMP)

Kindergarten–2nd Grade

- **K-2.CS.COMP Recognize that equipment is needed to access a network.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples about how we need more than one device to connect to a network. Students should know that the internet doesn't live within just one device. Devices must connect to a variety of additional devices to be online.

3rd Grade–5th Grade

- **3-5.CS.COMP Identify specific network components.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various network components such as access points, hubs/switches, routers, and user devices.

6th Grade–8th Grade

- **6-8.CS.COMP Identify the role of connected network components.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the roles of various network components such as access points, hubs/switches, routers, and user devices.

9th Grade–12th Grade

- **9-12.CS.COMP Create a diagram of a network utilizing appropriate network components.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of diagrams that include various network components such as access points, hubs/switches, routers, and user devices.

Cloud Computing (CC)

Kindergarten–2nd Grade

- **K-2.CS.CC State the benefits of storing and sharing information using cloud computing.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of cloud computing, which is defined as network/internet-based storage.

3rd Grade–5th Grade

- **3-5.CS.CC.1 Demonstrate ways to store and share information using cloud computing.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of cloud computing, such as mapped drives and Google Docs.

- **3-5.CS.CC.2 Demonstrate safe cloud computing practices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of safe cloud computing practices such as logging on and off.

6th Grade–8th Grade

- **6-8.CS.CC Identify the advantages and disadvantages of various cloud computing models.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of cloud computing models such as public, community, and private.

9th Grade–12th Grade

- **9-12.CS.CC Evaluate the risks and benefits of cloud computing.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various risks and benefits of cloud computing. Examples of cloud computing include various "aaS" (as a service) references, such as IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (software as a service). Examples of benefits of cloud computing can include distributed storage to prevent data loss from environmental disasters, easily working with peers over long distances, and the ability to save costs by not purchasing servers that are not utilized (i.e. only pay for what is needed). Examples of risks of cloud computing can include unauthorized access through breach of cloud provider, permissions incorrectly granted to users, and data being inadvertently shared publicly.

Protocols (PROT)

Kindergarten–2nd Grade

- **K-2.CS.PROT Identify various services that are available online.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of online services such as web, email, video, and gaming.

3rd Grade–5th Grade

- **3-5.CS.PROT Describe the different services available online.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various online services such as web, email, video, gaming, Google Drive, and networked drives.

6th Grade–8th Grade

- **6-8.CS.PROT Identify the protocol connection types used for different services available online.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various online services such as web, email, video, gaming, TCP (web and email), UDP (video and gaming), HTTP, and HTTPS.

9th Grade–12th Grade

- **9-12.CS.PROT.1 Compare and contrast the ports and protocols used for different services available online.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the various online protocols associated with TCP and UDP. Examples of TCP include HTTP, HTTPS (web), IMAP, and POP3 (email). Examples of UDP include audio/voice, DNS, DHCP, and gaming.

- **9-12.CS.PROT.2 Identify the risks associated with the different services available online.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the risks that various online protocols pose, including TCP and UDP.

Data Loss (LOSS)

Kindergarten–2nd Grade

- **K-2.CS.LOSS Define data loss and service outages.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of avoiding data loss such as the process of saving work.

3rd Grade–5th Grade

- **3-5.CS.LOSS Explain the role and importance of backups.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of backups that are available through auto-save features provided by apps or cloud-based services.

6th Grade–8th Grade

- **6-8.CS.LOSS Explain the role and importance of backups.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how redundant systemscanprevent data loss or services outages.

9th Grade–12th Grade

- **9-12.CS.LOSS Develop a plan for risk mitigation that implements redundancy.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of redundancy such as backups and auxiliary power sources as tools to mitigate risk, along with the use of hot sites and cold sites in the event of an environmental disaster affecting operations.

Hardware

Network Hardware Components (HARD)

Kindergarten–2nd Grade

- **K-2.CS.HARD Identify the components or parts of computing devices.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of student devices such as headphones, screens, and where to insert plugs and accessories.

3rd Grade–5th Grade

- **3-5.CS.HARD Explain the vulnerabilities of connecting devices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of BYOD (bring your own device) and the risks of connecting to networks or opening unknown files or drives on school devices.

6th Grade–8th Grade

- **6-8.CS.HARD Develop strategies to raise awareness of hardware vulnerabilities.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the potential for danger from issues such as malicious USB drives, key loggers, and hacked webcams.

9th Grade–12th Grade

- **9-12.CS.HARD Identify methods of mitigating risk associated with connecting devices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of risk such as compromised network security or data loss due to malicious incidents.

Internet of Things (IOT)

Kindergarten–2nd Grade

- **K-2.CS.IOT Identify examples of devices that are part of the Internet of Things.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of the IoT (defined as physical devices that are connected to the internet and collecting and sharing data) by categorizing or selecting specific examples and non-examples of devices.

3rd Grade–5th Grade

- **3-5.CS.IOT Define the Internet of Things.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how the IoT can refer to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data.

6th Grade–8th Grade

- **6-8.CS.IOT Evaluate the risks and benefits of Internet of Things devices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of IoT devices and the risks and benefits associated with those devices.

9th Grade–12th Grade

- **9-12.CS.IOT Analyze the vulnerabilities of Internet of Things devices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of IoT devices and the vulnerabilities associated with the connection and use of those devices.

Operating Systems (OS)

Kindergarten–2nd Grade

- **K-2.CS.OS Describe the role of an operating system.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of an operating system, such as those that can be found in phones, computers, and game systems.

3rd Grade–5th Grade

- **3-5.CS.OS Distinguish between roles of various operating systems.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various operating systems such as phones, computers, and game systems.

6th Grade–8th Grade

- **6-8.CS.OS Discuss the risks of outdated operating systems.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of updates to operating systems and the importance of patches.

9th Grade–12th Grade

- **9-12.CS.OS Create a plan for hardening an operating system.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how hardening an operating system can include shutting down unnecessary services and ports, installing updates and/ or patches, removing unused programs, and reviewing user privileges.

Software

Software Updates (SOFT)

Kindergarten–2nd Grade

- **K-2.CS.SOFT Understand the need for keeping apps and devices up to date.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of apps and devices and how users can be prompted to update one or the other.

3rd Grade–5th Grade

- **3-5.CS.SOFT Understand the need for keeping apps and devices up to date.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how patching can protect systems by updating firmware, applications, and operating systems.

6th Grade–8th Grade

- **6-8.CS.SOFT Identify examples of vulnerabilities that exist in software.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of vulnerabilities that can be introduced by not installing updates to operating systems, applications, and devices.

9th Grade–12th Grade

- **9-12.CS.SOFT Compare the advantages and disadvantages of patching systems in real time.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of operating system patches such as those that are provided regularly to devices running Windows, MacOS, Linux, iOS, and Android.

Programming and Scripting (PROG)

Kindergarten–2nd Grade

- **K-2.CS.PROG Discuss how scripts can make web pages and/or apps respond to a user's action.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how a web page or app relies on code to interpret user actions such as clicking on a button or entering a value in a text box.

3rd Grade–5th Grade

- **3-5.CS.PROG Explain how web pages and/or apps can be changed with simple adjustments to code.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how web pages and/or apps can be altered by changing the supporting code. One example might be to relate concepts like repetitions (looping) and decisions (conditionals) to the way a web page and/or app responds to our actions.

6th Grade–8th Grade

- **6-8.CS.PROG Explain the role of scripting in cyber attacks.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how scripts (this might include anything from a sequence of simple system commands, advanced scripting languages used for system configurations, or complex task automations) can become events that are related to cyber attacks.

9th Grade–12th Grade

- **9-12.CS.PROG Describe the role of scripting in cyber attacks and cyber defense.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the programming and/or scripting languages that can propagate a cyber attack and the defenses that are available to mitigate cyber attacks.

Applications (APPS)

Kindergarten–2nd Grade

- **K-2.CS.APPS Recognize how applications are software that contain code.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of software applications that students are familiar with.

3rd Grade–5th Grade

- **3-5.CS.APPS Discuss how all software may have vulnerabilities.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of operating systems, applications, and malware.

6th Grade–8th Grade

- **6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the role that software plays in the protection of a secure system.

9th Grade–12th Grade

- **9-12.CS.APPS Discuss how software that exists on and across various platforms can be used to monitor, collect, and analyze information from those platforms.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate software examples such as firewalls, packet sniffers and analyzers, and network monitors. Discussions may also include SIEM (security information and event management) software.

Digital Citizenship (DC)

Online Safety

Cyberbullying (CYBL)

Kindergarten–2nd Grade

- **K-2.DC.CYBL Discuss examples of cyberbullying and model age-appropriate responses to cyberbullying.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of cyberbullying, what to do when someone is mean online, and what behavior should be modeled when online.

3rd Grade–5th Grade

- **3-5.DC.CYBL Discuss and demonstrate examples of cyberbullying and methods of age-appropriate intervention.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of interventions, such as bystander vs. upstander.

6th Grade–8th Grade

- **6-8.DC.CYBL Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how to recognize cyberbullying, what actions that students can take if they are being bullied, and how to speak up to support someone who may be a victim of cyberbullying.

9th Grade–12th Grade

- **9-12.DC.CYBL Prepare a plan to raise awareness of the effects of cyberbullying.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of actions that can serve to reduce and/or prevent cyberbullying.

Digital Footprint (FOOT)

Kindergarten–2nd Grade

- **K-2.DC.FOOT Differentiate between good and bad online behavior.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of online behavior, for example, students should be kind to others online.

3rd Grade–5th Grade

- **3-5.DC.FOOT Describe the concept of a digital footprint.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how an online reputation can help or harm a person's online presence.

6th Grade–8th Grade

- **6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how information can be harvested by third parties to create a digital footprint through apps, wearables, and mobile devices that may share user telemetry.

- **6-8.DC.FOOT.2 Recognize the permanence of a digital footprint.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how information posted online may not be fully removed or erased.

9th Grade–12th Grade

- **9-12.DC.FOOT Examine the implications of both positive and negative digital footprints.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of ethical, societal, and financial implications.

Public and Private Information (PPI)

Kindergarten–2nd Grade

- **K-2.DC.PPI Distinguish between private vs. public information.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of privacy and what is OK to share about themselves and how that relates to confidentiality.

3rd Grade–5th Grade

- **3-5.DC.PPI Define personally identifiable information (PII).**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of PII and how to keep personal information, including private and public information, safe online.

6th Grade–8th Grade

- **6-8.DC.PPI.1 Discuss the risks and benefits of sharing PII.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of risks or benefits of sharing PII with parties such as organizations, individuals, and applications.

- **6-8.DC.PPI.2 Examine techniques to detect, correct, and prevent disclosure of PII.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of disclosure (either intentional or unintentional, and by oneself or another party) by methods such as tagging in pictures or posts, hashtag usage, or inappropriate posts.

9th Grade–12th Grade

- **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.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the possible impacts of data-sharing in such areas as college admissions, cancel culture, careers, and relationships.

- **9-12.DC.PPI.2 Explain the individual risks of a data breach to an organization housing personal data.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of understanding that if an organization gets hacked, it can still harm the individual whose data was stolen.

Ethics

Threat Actors (THRT)

Kindergarten–2nd Grade

- **K-2.DC.THRT Describe good and bad uses of digital devices.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how devices can be used with good and bad intentions, such as taking unwanted photos, sharing information unintentionally, or sharing passwords or logins.

3rd Grade–5th Grade

- **3-5.DC.THRT Recognize the different motivations that influence good and bad online behaviors.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how devices can be used with good and bad intentions, such as sharing or tagging photos without permission or sharing passwords or logins.

6th Grade–8th Grade

- **6-8.DC.THRT Describe various types of threat actors.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various threat actors, such as nation-states, cyber terrorist groups, organized crime, or hacktivists.

9th Grade–12th Grade

- **9-12.DC.THRT Analyze the motives of threat actors.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of motives of threat actors such as financial, political, ideological, or simple malice. This analysis may occur in a variety of forms, such as supplying a scenario or case study from current events.

Ethical Integrity (ETH)

Kindergarten–2nd Grade

- **K-2.DC.ETH Identify unsafe content.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of unsafe content, such as popups and malicious links.

3rd Grade–5th Grade

- **3-5.DC.ETH Discuss examples of cyber attacks.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of cyber attacks in current events, such as those that affect corporatations, retailers, and gamers.

6th Grade–8th Grade

- **6-8.DC.ETH Distinguish between ethical and malicious hacking.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the various types of hackers, occupations, and beliefs.

9th Grade–12th Grade

- **9-12.DC.ETH Discuss the role that cyber ethics plays in current society.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how integrity and reputation can be affected by actions that are taken online.

Policy and Legal Issues

Rules, Laws, and Regulations (LAW)

Kindergarten–2nd Grade

- **K-2.DC.LAW Explain how online actions have real-world consequences and that laws and rules may also apply online.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of online and real-world consequences, such as how saying something mean to somebody online still hurts their feelings in the real world.

3rd Grade–5th Grade

- **3-5.DC.LAW Explain how certain policies and laws are created to guide online interactions.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how safety is protected through digital policies and laws, such as age-restricted applications and the fact that online actions can result in legal consequences.

6th Grade–8th Grade

- **6-8.DC.LAW Analyze specific federal, state, and local laws as they relate to cybersecurity and privacy.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of federal, state, and local laws, such as the Computer Fraud Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA or Wiretap Act), Digital Millennium Copyright Act (DMCA), PATRIOT Act, and Children's Internet Protection Act (CIPA), as well as the principle of net neutrality.

9th Grade–12th Grade

- **9-12.DC.LAW Compare and contrast local, state, federal, and international cyber laws and regulations for individuals and businesses.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of local, state, federal, and international cyber laws and regulations, such as those mentioned above, as well as Children's Online Privacy Protection Rule (COPPA) and General Data Protection Regulation (GDPR).

Intellectual Property (IP)

Kindergarten–2nd Grade

- **K-2.DC.IP Discuss the concept of copyright.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how copyright can be equated to ownership and other ideas, such as "Who wrote the document," "Anything I create that is new to the world is mine," and "I need to give credit to any content NOT created by me."

3rd Grade–5th Grade

- **3-5.DC.IP Explain how copyright relates to fair use.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of how fair use can help protect an author/creator's rights while promoting the sharing of ideas.

6th Grade–8th Grade

- **6-8.DC.IP Explain how intellectual property and copyright relate to fair use.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the types of creative commons licensing that are available; the differences between copyright, trademark, patent, registered trademark, and other IP ownership types; and how fair use can help protect an author/creator's rights while promoting the sharing of ideas.

9th Grade–12th Grade

- **9-12.DC.IP Debate the importance of intellectual property laws.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of ideas around who owns content on video games with transferrable goods, copyright when content is remixed or parodied, and how fair use can help protect an author/creator's rights while promoting the sharing of ideas.

Usage and User Agreements (AUP)

Kindergarten–2nd Grade

- **K-2.DC.AUP Describe how Acceptable Use Policies are designed to protect the user.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how using certain technologies means agreeing to follow policies such as Acceptable Use Policies (AUPs), possibly through a "classroom rules" analogy, and that those policies are there to protect the user.

3rd Grade–5th Grade

- **3-5.DC.AUP Explain various agreements and illustrate their purpose.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various agreements such as AUPs, Terms of Service (TOSs), and End User License Agreements (EULAs).

6th Grade–8th Grade

- **6-8.DC.AUP Understand the various agreements and how they protect users and owners of technology.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various agreements, such as AUPs, TOSs, and EULAs.

9th Grade–12th Grade

- **9-12.DC.AUP Differentiate between the various agreements that protect individuals and organizations in their digital environments.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of global documents such as AUPs, TOSs, EULAs, and security policies. Do some documents favor the individual over the corporation and vice versa?

Security (SEC)

Information Security

CIA Triad (CIA)

Kindergarten–2nd Grade

- **K-2.SEC.CIA Identify the concepts of Confidentiality, Integrity, and Availability as presented in the CIA Triad.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of CIA concepts, such as secure passwords and trust relationships.

3rd Grade–5th Grade

- **3-5.SEC.CIA Describe the concepts of the CIA Triad and how they work to protect information.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of CIA concepts, such as secure passwords and when it is appropriate to share personal information.

6th Grade–8th Grade

- **6-8.SEC.CIA Explain the effects of a failure of the CIA Triad.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of CIA failures that make use of authentic references where possible. Given an example, students should be able to identify which of the three parts of the CIA Triad failed.

9th Grade–12th Grade

- **9-12.SEC.CIA Explain various interactions between the CIA Triad and the three states of data.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of interactions and how people, processes, and technology support those interactions. In addition, the three states of data refer to "data in use" (currently being accessed), "data at rest" (waiting to be accessed), and "data in motion" (moving from one location to another).

Access Control (ACC)

Kindergarten–2nd Grade

- **K-2.SEC.ACC Define access to private information.**

  Clarification statement: At this level, discussions should focus on grade-appropriate examples of privileged information, which is information that someone has a need to know, in any discssuions about private information.

3rd Grade–5th Grade

- **3-5.SEC.ACC Describe the concept of appropriate access to private information.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of access to privileged information in any discussions about private information. Students should be able to give examples of people in authority, such as a principal or police officer, who they might share private (privileged) information with, such as their home address or parent's phone number.

6th Grade–8th Grade

- **6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of why access control is needed across user platforms and what constitutes an authorized user.

9th Grade–12th Grade

- **9-12.SEC.ACC Compare and contrast the concepts presented by access control principles, access control modules, and the principle of least privilege access.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the concepts of identify, authenticate, and authorize as access control principles, as well as MAC, RBAC, and DAC as access control modules.

Data Security (DATA)

Kindergarten–2nd Grade

- **K-2.SEC.DATA Identify the difference between information being altered accidentally or on purpose.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of information potentially being altered through either a mistake or on purpose.

3rd Grade–5th Grade

- **3-5.SEC.DATA Identify when and how data can be altered accidentally or on purpose.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of when and how data can be changed or destroyed either accidentally or on purpose.

6th Grade–8th Grade

- **6-8.SEC.DATA Describe data in its three states and potential threats to each state.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of the three states of data: data in use, data at rest, data in motion.

9th Grade–12th Grade

- **9-12.SEC.DATA Formulate a plan to apply security measures to protect data in all three states.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of protecting data in its three states.

Threats and Vulnerabilities (INFO)

Kindergarten–2nd Grade

- **K-2.SEC.INFO List examples of information that needs to be protected.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how information can be protected against digital threats, such as popups, links in texts and emails, and forgotten passwords, and how students can respond to these suspicious or uncomfortable threats.

3rd Grade–5th Grade

- **3-5.SEC.INFO Define events that are related to threats and vulnerabilities.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of events, activities, or actions, such as malware and spoofed emails, and how students can respond to these suspicious or uncomfortable threats.

6th Grade–8th Grade

- **6-8.SEC.INFO Analyze threats and vulnerabilities to information security for individuals and organizations.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as authentic, grade-appropriate examples of threats and vulnerabilities such as malware, spoofed emails, and hacks.

9th Grade–12th Grade

- **9-12.SEC.INFO Distinguish the different types of attacks that affect information security for individuals and organizations.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as authentic, grade-appropriate examples of malware, malicious users, hacks, and poor security policies.

Cryptography (CRY)

Kindergarten–2nd Grade

- **K-2.SEC.CRY Recognize how encryption safeguards information.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how encryption can be referred to as a "secret code" that can protect information. Where appropriate, discussions may touch on how methods for encoding data, such as binary (base-2), decimal (base-10), and hexadecimal (base-16), can benefit encryption.
  NOTE: Not all encoding methods are appropriate for all grade levels.

3rd Grade–5th Grade

- **3-5.SEC.CRY Discuss why and how we encrypt information and communication systems.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of some simple encryption methods that can protect information, such as Caesar, scytale, pig pen, and ROT13. Where appropriate, discussions may touch on how methods for encoding data, such as binary (base-2), decimal (base-10), and hexadecimal (base-16), can benefit encryption.
  NOTE: Not all encoding methods are appropriate for all grade levels.

6th Grade–8th Grade

- **6-8.SEC.CRY Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of more complex encryption methods, e.g., Vigenere, Bacon's cipher, and Enigma. Where appropriate, discussions may touch on how methods for encoding data, such as binary (base-2), decimal (base-10), and hexadecimal (base-16), can benefit encryption.
  NOTE: Not all encoding methods are appropriate for all grade levels.

9th Grade–12th Grade

- **9-12.SEC.CRY Analyze how modern advancements in computing have impacted encryption.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of modern advancements in encryption, such as symmetric vs. asymmetric, public key vs. private key, and encryption algorithms. Where appropriate, discussions may touch on how methods for encoding data, such as binary (base-2), decimal (base-10), and hexadecimal (base-16), can benefit encryption.
  NOTE: Not all encoding methods are appropriate for all grade levels.

Network Security

Authentication (AUTH)

Kindergarten–2nd Grade

- **K-2.SEC.AUTH Describe the concept of a good password and its importance.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of password concepts, such as not using common words as passwords; pass phrases being more secure than passwords; and combining letters, numbers, and symbols being more secure than pass phrases.

3rd Grade–5th Grade

- **3-5.SEC.AUTH Describe the role of authentication and authorization.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of authentication and authorization concepts that do not include passwords, such as biometric authentication, which can include examples like fingerprints in amusement parks and two-factor authentication with credit card to prove age or gain access to someone's cell phone.

6th Grade–8th Grade

- **6-8.SEC.AUTH Explain how authentication and authorization methods can protect authorized users.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of more advanced authentication and authorization methods, such as two-factor, multifactor, and biometric.

9th Grade–12th Grade

- **9-12.SEC.AUTH Evaluate authentication and authorization methods and the risks associated with failure.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of authentication and authorization methods, such as certificate, token-based, two-factor, multifactor, and biometric.

Securing Network Components (COMP)

Kindergarten–2nd Grade

- **K-2.SEC.COMP Understand how Defense in Depth allows various security components to work together.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of how layered security can be compared to layers of securing your house, such as multiple locks and limited number of keys.

3rd Grade–5th Grade

- **3-5.SEC.COMP Identify Defense in Depth solutions that can be used to protect networks and devices.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of layered solutions that are available in WiFi settings, home vs. public networks, firewalls, and parental controls.

6th Grade–8th Grade

- **6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of layered strategies, such as firewalls, allow and block lists, changes to default passwords, and access points.

9th Grade–12th Grade

- **9-12.SEC.COMP Evaluate Defense in Depth strategies that can protect simple networks.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of layered strategies, such as firewalls, allow and block lists, changes to default passwords, access points, and network segmentation.

Threats and Vulnerabilities (NET)

Kindergarten–2nd Grade

- **K-2.SEC.NET Identify methods for exchanging information and why they need to be protected.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of various methods for exchanging information, such as social media feeds (e.g., YouTube) and online game platforms (e.g., Minecraft).

3rd Grade–5th Grade

- **3-5.SEC.NET Discuss vulnerabilities of open methods for exchanging information.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of vulnerabilities in various methods for exchanging information, such as social media feeds (e.g., YouTube) and online game platforms (e.g., Minecraft).

6th Grade–8th Grade

- **6-8.SEC.NET Explain how malicious actions threaten network security.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of malicious actions, such as social engineering, malware, and hacks.

9th Grade–12th Grade

- **9-12.SEC.NET Analyze the different types of attacks that affect network security.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of attacks, such as malware, hacks, malicious users, and poor security policies. In addition, risk analysis and management can be introduced through discussions around monitoring and logging of attacks.

Physical Security

Threats and Vulnerabilities (PHYS)

Kindergarten–2nd Grade

- **K-2.SEC.PHYS Define physical security as it relates to cybersecurity.**

  Clarification statement: At this level, student discussions should focus on relatable, grade-appropriate examples of physical security, such as visitors checking in at the front office, security guards at the entrance to a building, and turnstiles that prevent people without tickets from passing.

3rd Grade–5th Grade

- **3-5.SEC.PHYS Explain the need to protect people and places from malicious intent.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of people, places, or things that require protection and the threats that malicious intent might pose, such as to celebrities, political figures, landmark buildings and sites, or historical documents.

6th Grade–8th Grade

- **6-8.SEC.PHYS Explain how malicious actions threaten physical security.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of a variety of malicious actions, such as social engineering and poor security policies.

9th Grade–12th Grade

- **9-12.SEC.PHYS Analyze the different types of attacks that affect physical security.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of physical security attacks, such as social engineering, poor security policies, and malicious actors.

Security Controls (CTRL)

Kindergarten–2nd Grade

- **K-2.SEC.CTRL Define the policy of "trust but verify" for identity assurance.**

  Clarification statement: At this level, student discussions should focus on grade-appropriate examples of identity assurance, such as recognizing that all police officers carry badges.

3rd Grade–5th Grade

- **3-5.SEC.CTRL Identify physical access controls found in everyday life.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of authentic physical access controls, such as door locks, ID cards, PIN codes, bollards, lighting, fencing, cameras, and guards.

6th Grade–8th Grade

- **6-8.SEC.CTRL Describe Defense in Depth and how physical access controls work together.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of authentic and digital physical access controls, such as door locks, ID cards, PIN codes, bollards, lighting, fencing, cameras, and guards.

9th Grade–12th Grade

- **9-12.SEC.CTRL Justify the use of Defense in Depth and the need for physical access controls.**

  Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various physical access controls, such as proximity badges, PIN codes, and man traps.

Glossary of Terms

Topic	Description
Cybersecurity Education	Provides students with an understanding of how connected electronic devices interact in a digital age, how to protect digital assets from vulnerabilities, and the moral and ethical issues surrounding the uses of technology in our society.
Core Concepot	**Description**
Computing Systems	Computing Systems include hardware and software that work together to achieve objectives. Cybersecurity professionals work to prevent adversaries from exploiting weaknesses in computing systems to disrupt confidentiality, integrity, or availability.
Digital Citizenship	Digital citizenship encompasses the responsible and appropriate use of technology within society, including the norms, expectations, laws, and policies that affect organizations and individuals.
Security	Security is characterized by the user's responsibility for protection of access to computer networks, secure entry to all physical devices, and inherent accountability to protect personal identification information and organizational data.
Word or Concept	**Definition**
AAA	The AAA framework supplements the CIA Triad in describing how an organization protects its information security. The AAA Framework consists of Authentication, Authorization and Accounting.
Access Control	Access controls authenticate and authorize individuals to access the information they are allowed to see and use. Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.
Acceptable Use Policy (AUP)	A written agreement which defines activity that is allowable on a private network.
Accounting	Accounting provides a method for tracking which users are accessing a system and the resources they utilize. Accounting provides a listing for determining normal operations (baselining) and the ability to audit a user's actions to identify potential unauthorized access (forensics).
AI and Virtual Assistants	These can include so-called "smart" devices and digital personal assistants. Specific examples might include Google, Alexa (Amazon), and Siri (Apple).
Analog Network	A means of logically transmitting data by way of an analog signal (i.e., all transmitted signals are analog waveforms).

Topic	Description
Authentication	Authentication provides a method for identifying users. The authentication process typically requires valid user credentials, confirmed by something you know, something you have, something you are, somewhere you are, or something you do. Examples of each include: know: password; have: picture ID; are: fingerprint; where: location; do: gestures.
Authorization	Authorization provides access to resources and information based on an authenticated user's privileges as defined through security controls. The concept of authorization controls what a user can and cannot access.
Cellular Network	A wireless network of towers and access points to provide network connectivity to mobile devices. It is called cellular because each service area of a tower is referred to as a "cell". As a mobile device moves from one cell to the next, the connectivity of the device is transferred to the next cell.
Certificate Authority (CA)	A trusted provider of digitally signed certificates authenticating the identity of an organization.
Certificate	A virtual component of public key infrastructure (PKI) which provides a public key for encrypting communications and affirms the identity of an organization often through a trusted certificate authority (CA); though internal certificates may be used within an organization.
CIA Triad	A three-part model designed to guide policies for information security within an organization. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.
Cipher(s)	A reversible method or algorithm used to obscure a message in order to prevent unauthorized access.
Cloud Computing	Computing resources shared over a network where the internal structure is abstracted from the end user.
Communication Channel	A means or medium for the exchange of information.
Copyright	The exclusive right of an owner to produce copies of a written or published work for a fixed amount of time (similar to patent).
Cybersecurity	The protection of networks, devices, and data from unauthorized use.
Defense in Depth	A strategy where multiple defensive measures provide interlocking security, sometimes referred to as defensive layering.
Digest	The end result or output from a hashing algorithm.

Topic	Description
Digital Citizenship	The responsible and appropriate use of computing technology to engage with society.
Digital Footprint	Public and private information available on the internet which comprise an identity, both real and virtual.
Digital Network	A means of logically transmitting data by way of a digital signal (i.e. all transmitted signals are analog waveforms).
Discretionary Access Control (DAC)	Access to information is controlled by the user creating or storing the data.
Encryption	The reversible process of obscuring a message in order to prevent unauthorized access. Reversal is known as decryption.
Fair Use	Allowable, limited use of a copyrighted work when appropriate attribution is provided, as defined by law.
Firewall	A network device which filters authorized and unauthorized network traffic based on certain criteria.
Hacking	The act of gaining unauthorized access to a system.
Hardware	Electrical circuits working together to execute software to carry out operations.
Hash Collision	When two unique inputs for a hashing algorithm produce the same outputs (digests).
Hashing	A one-way, irreversible process or algorithm which produces a unique digest or fixed-length sequence of letters and numbers for any given input. No two digests will be the same.
Intellectual Property	Intangible (not physical) creation such as a process, idea, or design owned by a person or organization.
Internet Protocol (IP)	The primary protocol that comprises the Internet. Data in this format is broken into packets which can be routed from a source to a destination based on a network address. IP packets are formatted as either TCP or UDP packets.
Internet of Things (IoT)	Internet-connected devices that automatically carry out some function in daily life (e.g. thermostat, doorbell).
Local Area Network (LAN)	A private network contained within a small single geographic area (often identified by use of private network addresses such as 10.x.x.x or 192.168.x.x).
Mandatory Access Control (MAC)	Access to information is controlled by the operating system of the computer housing or accessing the data.

Topic	Description
Media Access Control Address (MAC)	A unique identifier used by a network interface to differentiate itself from others when establishing network communications. The address is set by the manufacturer and cannot be changed, though software can allow for it to be reported differently.
Network Components	Devices (hardware) that are connected to or comprise a network.
Network Neutrality (Net Neutrality)	Net neutrality is a principle that suggests that all internet service providers must treat all internet communications equally, without discrimination. Essentially, net neutrality entrusts ISPs to never intentionally block, slow down, or charge money for access to online content.
Network Topology	The conceptual organization or structure of a network.
Nonrepudiation	The inability to dispute ownership/authorship of an item.
Patching	Updates to software to limit unexpected operation such as security vulnerabilities or fatal errors in a program.
Patent	The exclusive right of an owner to produce a product or use a unique process of production for a fixed amount of time (similar to copyright).
Permanence (digital)	The inability to remove online, digital content with absolute certainty.
Personally Identifiable Information (PII)	Data which can be used to identify a specific individual.
Protocol	A communications standard often consisting of the structure and formatting used in the exchange of information.
Public Key Cryptography	Use of a public key to encrypt data which can only be (easily) decrypted by a user possessing the matching private key.
Public Key Infrastructure (PKI)	Processes and technology which make up the trust system of signing and securing certificates necessary for public key cryptography.
Role-Based Access Control (RBAC)	Access to information is dependent upon an individual's role within the organization.
Software	A series of steps written in code for a computing device to carry out operations.
Terms of Service (ToS)	A written agreement by an organization which explains the type of service a provider will render to an end user and how the organization will operate regarding the end user and their data.
The Three States of Data	The three states of data refer to "data in use" (currently being accessed), "data at rest" (waiting to be accessed), and "data in motion" (moving from one location to another).

Topic	Description
Trademark	A unique graphic, symbol, or logo used to identify a brand or organization.
Transmission Control Protocol (TCP)	Packets of data within the Transmission Control Protocol are intended to be reliable (ensure delivery), sequential, and free from transmission errors. TCP packets contain information to acknowledge successful receipt of a packet, the sequence in which the packets were sent, and a checksum to ensure the data arrived intact. The benefit of TCP is assurance of delivery.
User Datagram Protocol (UDP)	Packets of data within the User Datagram Protocol are sent without acknowledgement and may arrive out of sequence. UDP packets may or may not arrive at all. UDP packets that arrive late or out of sequence are simply ignored. The benefit of UDP is less network overhead.
Wide Area Network (WAN)	A network spread across a large geographic area.
Wireless Local Area Network (WLAN)	A network utilizing wireless radio links between devices on a network, often utilizing a Wireless Access Point (WAP) to access resources over a wired network.