Arkansas Computer Science Standards for High School

Advanced Information Security

2016

Advanced Information Security

Introduction

The Arkansas Advanced Information Security Standards focus on the skills necessary to identify, understand, and analyze threats to the digital and physical security of systems. Through these standards, students will explore, apply, and advance toward mastery of the design and implementation of security protocols and policies. Students will ensure system and data integrity through troubleshooting, administration, auditing, and efficiency. Students will accomplish tasks and solve problems independently and collaboratively with the tools and skills needed to be successful in college and careers.

The Arkansas State Board of Education (SBE) does not place any pre-requisites on the Arkansas Computer Science High School Courses, but allows for schools to place students in any of the courses based on ability and desire. The Arkansas Department of Education (ADE) recommends that districts develop and formally adopt a written policy outlining placement protocols. Evaluation tools and placement criteria will be the responsibility of the local districts. Though there are no specific course prerequisites, students enrolling in Advanced Programming, Advanced Networking, or Advanced Information Security should understand and be able to apply the content/concepts found within the Arkansas Computer Science Courses Levels 1 - 4.

The SBE and ADE authorizes schools to enroll students across levels and emphases in the same sections of the master schedule (a.k.a. stacking) as long as the number of students does not exceed Standards of Accreditation maximums and/or ratios, and the school can reasonably assure a high-quality educational experience for all students within that section.

Implementation of the Arkansas Computer Science Standards for Grades 9-12 begins during the 2017-2018 school year.

Course Title:	465250 - Advanced Information Security Level 1 465260 - Advanced Information Security Level 2
Course/Unit Credit:	0.5 Credits per Course
Teacher Licensure:	Please refer to the Course Code Management System (https://adedata.arkansas.gov/ccms/) for the most current licensure codes.
Grades:	9-12
Prerequisites:	There are no ADE established course prerequisites for any of the Computer Science levels; it is up to the local district to determine placement based on student ability.

Computer Science Practices

Students will exhibit proficiency in computer science through:

Perseverance - Students expect and persist in overcoming the challenges that occur when completing tasks. They recognize that making and correcting mistakes will take place during the learning process and problem solving.

Collaboration - Students effectively work and communicate with others ensuring multiple voices are heard and considered. They understand that diverse thoughts may lead to creative solutions and that some problems may be best solved collaboratively.

Patterns - Students understand and utilize the logical structure of information through identifying patterns and creating conceptual models. They decompose complex problems into simpler modules and patterns.

Tools - Students evaluate and select tools to be used when completing tasks and solving problems. They understand that appropriate tools may include, but are not limited to, their mind, pencil and paper, manipulatives, software application programs, programming languages, or appropriate computing devices.

Communication - Students effectively communicate, using accurate and appropriate terminology, when explaining the task completion or problem solving strategies that were used. They recognize that good documentation is an ongoing part of the process, and when appropriate, provide accurate documentation of their work in a manner that is understandable to others.

Ethics and Impact - Students comprehend the ramifications of actions prior to taking them. They are aware of their own digital and cyber presence and its impact on other individuals and society.

Problem Solving - Students exhibit proficiency in Computer Science through identifying and systematically solving problems (e.g., engineering design process). They recognize problem solving as an ongoing process.

Advanced Information Security

Strand	Content Cluster
Computational Thinking and Problem Solving	
	1. Students will analyze vulnerabilities and problem-solving strategies.
	2. Students will analyze connections between elements of mathematics and computer science.
	3. Students will solve problems cooperatively and collaboratively.
Data and Information	
	4. Students will analyze various ways in which data is represented.
	5. Students will encrypt and recover data.
	6. Students will analyze server and cloud security.
Computers and Communications	
	7. Students will utilize appropriate digital tools for various applications.
	8. Students will analyze various network components and functions of computers.
Community, Global, and Ethical Impacts	
	9. Students will analyze appropriate uses of technology.

Notes for the Computer Science Standards for High School document:

1. The examples given (e.g.,) are suggestions to guide the instructor.
2. The Practices are intended to be habits of mind for all students and were written broadly in order to apply to all grades. The Practices are not content standards and are not intended to be formally assessed but may be assessed formatively.
3. This Arkansas Department of Education curriculum standards document is intended to assist in district curriculum development, unit design, and to provide a uniform, comprehensive guide for instruction.
4. Notes found within the document are not approved by the Arkansas State Board of Education, but are provided for clarification of the standards by the Arkansas Department of Education and/or the standards drafting committee. The notes are subject to change as understandings of the standards evolve.

Strand: Computational Thinking and Problem Solving

Content Cluster 1: Students will analyze vulnerabilities and problem-solving strategies.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.1.1 Identify potential security holes and breaches in network and software	AISL2.1.1 Create policies that address security holes and breaches in network and software
AISL1.1.2 Identify various methods that can be used to attack cryptographic primitives in order to deduce the decryption key and/or extract plaintext from ciphertext	AISL2.1.2 Demonstrate passive attacks on encrypted data to either deduce the decryption key and/or extract plaintext from ciphertext
AISL1.1.3 Identify various injection techniques (e.g., buffer overflow, cross-site scripting [XSS], Structured Query Language [SQL] injection)	AISL2.1.3 Propose potential solutions to responsible parties, if a security exploit is found
AISL1.1.4 Recognize malicious behavior or website vulnerability to injection-based attacks	AISL2.1.4 *Continuation of this standard is not specifically included or excluded*

Strand: Computational Thinking and Problem Solving

Content Cluster 2: Students will analyze connections between elements of mathematics and computer science.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.2.1 Identify various cryptographic primitives (e.g., public-key primitives, symmetric-key primitives, unkeyed primitives)	AISL2.2.1 Describe various cryptographic primitives (e.g., public-key primitives, symmetric-key primitives, unkeyed primitives)
AISL1.2.2 Compare complexity of common cryptographic algorithms	AISL2.2.2 Describe mathematical complexity of common cryptographic algorithms
AISL1.2.3 Analyze the mathematical basis for various password complexity requirements	AISL2.2.3 *Continuation of this standard is not specifically included or excluded*

Strand: Computational Thinking and Problem Solving

Content Cluster 3: Students will solve problems cooperatively and collaboratively.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.3.1 Review state and federal laws pertaining to security audit processes	AISL2.3.1 Discuss processes of creating a business agreement for security audit process
AISL1.3.2 Review industry best practices for network security	AISL2.3.2 Create a comprehensive network security policy or serve on security policy committee (e.g., peer review policies)
AISL1.3.3 Audit security policies	AISL2.3.3 Participate in development of security policies within a committee

Strand: Data and Information

Content Cluster 4: Students will analyze various ways in which data is represented.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.4.1 Discuss common uses of encryption rather than plain text (e.g., email, Hyper-Text Transfer Protocol [HTTP] vs. Secured Hyper-Text Transfer Protocol [HTTPS], password storage, user authentication)	AISL2.4.1 *Continuation of this standard is not specifically included or excluded*
AISL1.4.2 Identify transactional weaknesses of an insecure network connection	AISL2.4.2 Understand processes of issuance of Secure Sockets Layer (SSL) key certificates and importance of HTTPS
AISL1.4.3 Understand the use of public-key encryption vs. private-key encryption	AISL2.4.3 *Continuation of this standard is not specifically included or excluded*

Strand: Data and Information

Content Cluster 5: Students will encrypt and recover data.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.5.1 Describe various encryption storage procedures (e.g., public, private)	AISL2.5.1 Discuss data retrieval techniques (e.g., magnetic imaging of spinning disks)
AISL1.5.2 Explain how software logs and user access privileges can be used to recreate a series of events	AISL2.5.2 Recreate a series of events based on software logs and user access privileges
AISL1.5.3 Explore examples and applications of steganography	AISL2.5.3 Demonstrate the use of steganography in a digital file (e.g., document, image, other media, program, protocol)

Strand: Data and Information

Content Cluster 6: Students will analyze server and cloud security.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.6.1 Understand component systems comprising server and/or cloud servers	AISL2.6.1 Recognize security of entire system relies on security of all component systems NOTE: This is commonly referred to as the “weakest link” in information or computer security.
AISL1.6.2 Identify importance of security patch releases and updates	AISL2.6.2 Describe commonly employed security measures (e.g., antivirus, asset management, cloud security, intrusion detection systems, malware detection)
AISL1.6.3 Discover information available in server logs and security policies	AISL2.6.3 Recreate an order of events based on a log file
AISL1.6.4 Identify the methods that Virtual Private Networks (VPN) utilizes to ensure data security	AISL2.6.4 Implement a secure VPN

Strand: Computers and Communications

Content Cluster 7: Students will utilize appropriate digital tools for various applications.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.7.1 Select the appropriate tool for a specific network function (e.g., Ethereal, Network Mapper [nmap], Wireshark)	AISL2.7.1 Utilize audit tools for network compliance (e.g., Microsoft Key Management Service [KMS])
AISL1.7.2 Identify value of enterprise antivirus and malware scanning software tools	AISL2.7.2 *Continuation of this standard is not specifically included or excluded*
AISL1.7.3 Understand information provided in and location of security log files available for various services	AISL2.7.3 Verify system access privileges of various system services and software

Strand: Computers and Communications

Content Cluster 8: Students will analyze various network components and functions of computers.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
AISL1.8.1 Identify various physical security tools, processes, and systems in common use	AISL2.8.1 *Continuation of this standard is not specifically included or excluded*
AISL1.8.2 Describe the value of limiting physical access to servers and network infrastructure	AISL2.8.2 *Continuation of this standard is not specifically included or excluded*
AISL1.8.3 Explain implications of sharing physical information online (e.g., doxing)	AISL2.8.3 *Continuation of this standard is not specifically included or excluded*
AISL1.8.4 Examine layers of physical security (e.g., alarms, barriers, locks, security personnel)	AISL2.8.4 *Continuation of this standard is not specifically included or excluded*

Strand: Community, Global, and Ethical Impacts

Content Cluster 9: Students will analyze appropriate uses of technology.

THE GOAL FOR EACH STUDENT IS PROFICIENCY IN ALL REQUIREMENTS AT CURRENT AND PREVIOUS LEVELS	
Level 1	Level 2
AISL1.9.1 Identify ethical and unethical uses of encryption	AISL2.9.1 Demonstrate ethical uses of encryption
AISL1.9.2 Identify ethical and unethical uses of file sharing	AISL2.9.2 Demonstrate ethical uses of file sharing
AISL1.9.3 Identify ethical and unethical uses of security vulnerabilities (black-hat, gray-hat, and white-hat hacking)	AISL2.9.3 *Continuation of this standard is not specifically included or excluded*
AISL1.9.4 Identify the ethics and legality of vulnerability research	AISL2.9.4 Demonstrate ethical and legal vulnerability research

Contributors

The following people contributed to the development of this document:

Stephany Alhajjaj – Little Rock School District	Lori Kagebein – Wonderview School District
Jeff Anderson – Rogers Public Schools	Jeff Matocha – Ouachita Baptist University
Brent Burgin – Dassault Falcon Jet	Daniel Moix – Arkansas School for Mathematics, Sciences, and the Arts
Kristian Cartwright – Fayetteville Public Schools	Larry Morell – Arkansas Tech University
Kevin Collins – Alma School District	David Nance – Arkansas Department of Education
Cecil Cossey – Hamburg School District	Thad Nipp – Alma School District
Ty Davis – Springdale Public Schools	Anthony Owen – Arkansas Department of Education
Jennifer Feltmann – Berryville Public Schools	Kenneth Powell – Metova Federal
Carl Frank – Arkansas School for Mathematics, Sciences, and the Arts	Jerry Prince – EAST Initiative
Charles Gardner – Cyber Innovation Center	Kimberly Raup – Conway Public Schools
Tammy Glass – Spring Hill School District	Sandra Rhone – Mineral Springs School District
Tommy Gober – Cyber Innovation Center	Linda Riley – Wonderview School District
Joel Gordon – Arkansas Regional Innovation Hub	Nicholas Seward – Arkansas School for Mathematics, Sciences, and the Arts
Marilyn Harris – Virtual Arkansas	Tom Simmons – El Dorado Public Schools
Andy Hostetler – Jonesboro Public Schools	Dustin Summey – Virtual Arkansas
Tim Johnston – Arkansas Department of Career Education	Travis Taylor – Little Rock School District
Linda Joplin – Fort Smith Public Schools	Karma Turner – Lake Hamilton School District