5-207 Form – Curriculum Adoption – Curriculum Research – Design for Course Approval

I. **Rationale** - justification of need, citing data

As part of an ongoing effort to update and strengthen Career and Technical Education (CTE) offerings within the Amphitheater School District, a program interest survey was administered to all students in grades 8–11. The survey yielded 828 total responses. Cyber/Network Security emerged as one of the three most requested program areas, following interest in Business Management and Medical Assisting/medical-focused programs. Twenty-five percent of respondents (200 students) identified Cyber/Network Security as their top choice. Although Medical Assisting/medical-focused programs scored above this program, the cost of creating that program is cost-prohibitive at this time.

In evaluating potential new program offerings, the district considered multiple factors, including student interest, alignment to postsecondary and career opportunities, availability of internships and work-based learning experiences, instructor availability, and program startup costs. Cyber/Network Security demonstrated strong alignment across these criteria and offers immediate, accessible benefits to students and possible internships within our own district, working alongside our IT team.

Survey results also indicated that a primary driver of student interest was “career opportunities after high school.” When comparing Cyber/Network Security and Medical Assisting, and considering current staffing capacity, Cyber/Network Security was determined to provide broader and more readily available employment and internship pathways for students. There are many programs across our region that offer Medical Assisting programs, so there are limited opportunities for work-based learning and internships in this field, unlike with Cyber/Network Security, as there are limited program offerings in our region.

Additionally, this program would serve as a strategic replacement for Software and App Design and Amphitheater High School, a program that has experienced declining student interest over the past several years within the district. Cyber/Network Security better reflects current student demand and labor market relevance, positioning Amphitheater School District to more effectively meet student needs and workforce expectations.

II. **Description** - course goals and objectives, prerequisites, format

The Network Security (Cybersecurity) Career and Technical Education instructional program prepares students to assess the security needs of computer and network systems, recommend appropriate safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Through a coherent sequence of instruction, students develop the technical skills necessary to analyze, test, troubleshoot, and evaluate existing network systems, including local area networks (LANs), wide area networks (WANs), and Internet-based systems, or specific segments of a network infrastructure.

_____

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)

Students will learn to perform network maintenance and security monitoring to ensure systems operate efficiently, securely, and with minimal interruption. Instruction emphasizes real-world cybersecurity practices aligned with industry standards and workforce expectations.

Throughout the program, students enhance their technical knowledge and skills related to:

- Application and data integrity
- Cyber threat identification and mitigation
- Infrastructure and network security
- Risk assessment and system vulnerability analysis

In addition to occupation-specific competencies, students completing the Network Security program develop advanced critical thinking, problem-solving, collaboration, and applied academic skills essential for success in postsecondary education and cybersecurity-related careers.

Upon successful completion of the program, students will be able to:

- Analyze and evaluate network and system security risks
- Implement and manage security controls and best practices
- Troubleshoot and maintain secure network systems
- Apply cybersecurity principles to real-world scenarios
- Demonstrate career-ready skills aligned to Network Technologies occupations

The Network Security program is delivered as a coherent, multi-year sequence of courses designed to build progressively from foundational networking and security concepts to advanced cybersecurity applications. Instruction includes a combination of classroom learning, hands-on labs, simulations, and project-based activities that reflect real-world industry practices.

Students engage with current cybersecurity tools, technologies, and scenarios to develop both technical proficiency and professional skills. Curriculum is aligned to state CTE standards and designed to prepare students for postsecondary education, industry certifications, and entry-level positions in cybersecurity and network security fields.

Coherent Course Sequence

- Network Security I – First Year
- Network Security II – Second Year
- Network Security III – Third Year

Prerequisites

- Network Security I: No prerequisite
- Network Security II: Successful completion of Network Security I
- Network Security III: Successful completion of Network Security II

_____

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)

Placement in advanced courses may be contingent upon demonstrated technical readiness and instructor approval, as appropriate.

III. Articulation - reference to state standards

Network Security courses will be aligned with and delivered in accordance with the Arizona Department of Education (ADE) Career and Technical Education Technical Standards for Network Technologies and Cybersecurity. Instruction will be guided by the Cyber.org curriculum, which is aligned to state standards and industry expectations. Instructors may make instructional adjustments to address student interests, emerging technologies, and dual enrollment requirements**,** while maintaining full alignment to ADE standards. Any supplemental instructional materials used to support these modifications will be Governing Board–approved and aligned to program outcomes and state requirements.

IV. Audience - student group (school, grade, discipline) to be served

The Network/Cybersecurity program will initially be implemented at Amphitheater High School to evaluate student demand, program relevance, and enrollment patterns. This phased approach will allow the district to verify alignment between results from the student interest survey and actual student enrollment, ensuring data-informed decision-making prior to program expansion.

The program is proposed as a replacement for Software and Application Design, leveraging existing instructional resources and infrastructure. Due to the similarity in required technology and instructional needs, minimal startup and transition costs are anticipated, supporting a fiscally responsible implementation.

The Network/Cybersecurity program is designed as a three-year sequence primarily targeting 10th, 11th, and 12th grade students, with opportunities for internships or work-based learning experiences during the senior year**.** Enrollment may also be considered for 9th grade students on a case-by-case basis, based on student readiness and scheduling availability.

Upon demonstration of program viability and sustained student interest at Amphitheater High School, the district will begin the process of expanding the Network/Cyber Security program to the other two district high schools**.**

V. Resources - specific texts, materials, equipment needed

The Network Security (Cybersecurity) program will utilize a combination of digital curriculum resources, existing instructional equipment, and phased additions aligned with Arizona Department of Education (ADE) recommendations. Initial startup costs are minimal, as many instructional tools and materials are already in use within the district.

Instructional Texts and Curriculum Resources

Primary instructional content will be provided through Cyber.org, which offers ADE-aligned lesson plans and instructional resources delivered through a digital learning platform. Students

---

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)

will also utilize the Cyber.org Range, a virtual machine–based environment that allows for hands-on practice in cybersecurity scenarios, system security, and network defense. These digital resources reduce the need for traditional textbooks and support real-world, skills-based instruction.

Instructional Materials and Equipment

The program will leverage existing hands-on learning tools currently available within the district, including:

- Sphero robotics kits
- Micro:bit devices
- Drones

These tools support instruction in coding, systems thinking, automation, cybersecurity concepts, and problem-solving, particularly at the introductory level.

Technology and Equipment Needs

Additional equipment may be required for Network Security II and III to support advanced networking, cybersecurity labs, and industry-aligned instruction. Equipment needs will be identified and phased in as the program expands, consistent with the Arizona Department of Education CTE Recommended Equipment List for Network Technologies and Cybersecurity programs.

Overall, the program is designed to maximize the use of existing resources while strategically adding equipment as needed to support advanced coursework, ensuring **a** cost-effective, scalable, and standards-aligned implementation**.**

VI. Outcome - evaluation of course effectiveness

The Network Security (Cybersecurity) program will be evaluated annually using multiple measures to ensure instructional quality, student success, and alignment with industry and workforce expectations.

1. **Student Performance and Credential Attainment**
   Program effectiveness will be measured by student performance on the Technical Skills Assessment (TSA)**,** administered upon completion of Network Security II or III**, as** appropriate. Evaluation will include analysis of TSA pass rates and overall student proficiency.

   In addition, the program will track the number and percentage of students who earn industry-recognized certifications**,** which are anticipated to be completed following Network Security III**.** Certification attainment will serve as a primary indicator of technical competency and career readiness.

_____

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)

2. Data Review and Continuous Improvement
   After two years of implementation, TSA performance data will be reviewed longitudinally. Assessment blueprints will be analyzed to identify strengths, gaps, and areas for instructional improvement. Findings will inform curriculum adjustments, instructional strategies, and professional development.
3. Industry and Stakeholder Feedback
   The district will engage business and industry partners through the annual Students in Partnership with Industry year-end breakfast and business meeting**.** This forum will provide feedback on program effectiveness, budget and resource allocation, equipment and technology needs, and the quality of student learning and work-based learning opportunities. Stakeholder input will guide ongoing program refinement and sustainability.

VII. Implementation - timeline to include pilot phase and annual evaluation of proposed course

The Network Security (Cybersecurity) program will be implemented through a phased pilot and expansion model to ensure instructional quality, sustainable enrollment, and alignment with student interest.

Year 1: Pilot Implementation (2025–2026)

- One section of Cybersecurity Level I will be offered as a pilot program.
- Enrollment will be capped at 30 students.
- Software and Application Design II will continue to be offered to allow students who previously completed Level I to meet CTE completer requirements.
- Cybersecurity Level I will be available to all interested students.

Year 2: Program Expansion (2026–2027)

- Cybersecurity Level I will continue to be offered.
- Cybersecurity Level II will be introduced for students who have successfully completed Cybersecurity Level I.
- Students completing Level I will be eligible to enroll in Level II.

Year 3: Full Program Implementation (2027–2028)

- Cybersecurity Levels I, II, and III will be offered.
- Students who have completed Cybersecurity Levels I and II will be eligible to enroll in Cybersecurity Level III.
- At this stage, the program will reach full instructional capacity, providing a complete three-year pathway toward CTE completion and advanced technical skill development.

_____

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)

This phased approach allows the district to validate program demand during the pilot year, support students transitioning from Software and Application Design, and responsibly scale the Cybersecurity program over time.

VIII. Process - how teachers, parents, and students (when appropriate) were included in the decision making process

The decision to propose Network/Cybersecurity as a new Career and Technical Education program was informed through intentional engagement with students, parents, and instructional staff over multiple years.

- **Student Input:**
  A districtwide survey was administered to all students in grades 8–11 to assess interest in potential new CTE program offerings. Survey results identified Network/Cybersecurity as one of the highest areas of student interest, providing a data-driven foundation for program consideration.
- **Parent and Community Feedback:**
  Parents and guardians shared feedback during various CTE events held throughout the year, expressing strong interest in business-related pathways that support career readiness, employability, and post-secondary opportunities for their students.
- **Teacher and Staff Collaboration:**
  Ongoing conversations with CTE teachers over the past two years focused on program relevance, enrollment trends, and instructional sustainability. These discussions included analysis of declining enrollment in Software and Application Design and exploration of viable, student-centered replacement options.

This collaborative and evidence-based process ensured that the proposed Network/Cyber Security program reflects student demand, parent expectations, instructional insight, and district priorities.

Approval:

Julie Valenzuela, Director of 21st Century Education 1/27/26

Principal date

Superintendent date

(*Note*: Must be submitted for Governing Board approval prior to the end of the current school year for implementation during the following school year.)