Cybersecurity I - NSS

Level: 2
Career Cluster: Advanced Manufacturing, Digital Technology
Program: Engineering, Information Technology
Pathway(s): Engineering Applications UAS, Networking Systems and Security

Course Catalog Description

Introduces students to foundational cybersecurity concepts through the context of connected devices, networks, and mission-based operations. Students examine cyber threats, secure communications, access control, risk management, and data protection practices used to support safe and secure digital operations.

Summary

Introduces students to foundational cybersecurity concepts through the context of connected devices, networks, and mission-based operations. Students explore career pathways, professionalism, ethics, and postsecondary opportunities in engineering, information technology, and cybersecurity fields while building an understanding of confidentiality, integrity, availability, risk management, access control, and secure operations. The course emphasizes how networking, endpoint protection, data security, and cyber threats affect platforms, communications, digital systems, and operational safety. Students also examine secure system practices, troubleshoot connectivity and security issues using technical tools, and apply methods for protecting data through backups, access restrictions, and cryptography. By the end of the course, students will be able to analyze cybersecurity risks in digital environments, recommend safeguards for secure operations, and communicate technical findings using appropriate industry terminology.

Notes

This revised document shifts from a broad networking and information security focus to a more specialized cybersecurity context. While the earlier course emphasized general cybersecurity concepts, infrastructure, and data protection, this version strengthens the application of those ideas to connected systems, mission-based operations, digital assets, and secure communications. It also places greater emphasis on cybersecurity as part of safe and responsible technology use, helping students connect technical security concepts to real-world operational settings in engineering and emerging technology pathways. Compared to the older course, this version is more applied and career-connected, with content organized around secure operations, risk analysis, system protection, and problem solving. Major updates include clearer section objectives, revised student outcomes, added final project assessment, leadership, and work-based learning components, plus stronger emphasis on ethics, risk management, standards alignment, and instructional resource support.

Student Learning Outcomes

1. Career Exploration and Postsecondary Opportunities

Objective: *Students will analyze career pathways in engineering and cybersecurity by exploring industry roles, workplace expectations, required education, certifications, professional organizations, and postsecondary opportunities available in Colorado in order to make informed academic and career decisions.*

1) Identify employment opportunities in various fields with a focus in the area of engineering and cybersecurity
    a. Recognize the work typically performed, tools and technology used, and nature of work environments
    b. Identify potential certifications within the careers
    c. Find membership organizations associated with the careers
    d. Understand the necessary education associated within the careers
2) Define professionalism within the context of engineering and cybersecurity
    a. Criticism and evaluation
    b. Presentation
    c. Assessment
3) Recognize laws, regulations, and ethics significant to the fields of engineering and cybersecurity
4) Identify postsecondary opportunities offered in the state of Colorado
    a. Technical college, community college, 4-year institutions
    b. Certificates, associates, bachelor, and advanced degree opportunities

2. Foundations of Cybersecurity and System Security

Objective: *Students will explain the core principles of cybersecurity and connect them to the safe and secure operation of systems, networks, data, and connected devices.*

5) Define key cybersecurity concepts including confidentiality, integrity, availability, authentication, and nonrepudiation.
6) Explain why cybersecurity is essential in engineering, digital systems, and connected operations.
7) Identify common cyber threats that affect systems, mobile devices, networks, and cloud-connected platforms.
8) Describe the importance of ethical behavior, responsible data use, and legal compliance in cybersecurity.
9) Recognize the value of physical security when protecting devices, equipment, credentials, and stored media.
10) Summarize how cybersecurity failures can impact safety, privacy, operations, and public trust in UAS environments.
11) Interpret current events involving data breaches, cyberattacks, or security vulnerabilities.
12) Differentiate between secure and insecure practices when handling logs, images, video, and digital data.

3. Risk Management, Safety, and Security Compliance

Objective: *Students will analyze cybersecurity risk and apply basic risk management practices to systems, devices, and data environments.*

13) Define risk, vulnerability, threat, exploit, and mitigation in cybersecurity contexts.
14) Analyze how cybersecurity risks can affect planning, communications, data systems, and operational safety.
15) Apply a basic risk assessment process to a system deployment or data collection scenario.
16) Classify risks according to likelihood, impact, and severity.
17) Recommend appropriate safeguards to reduce technical, human, and physical risks.
18) Describe industry concepts related to standards, compliance, and security frameworks.
19) Evaluate the role of security procedures in protecting organizational and mission-critical information.
20) Justify cybersecurity decisions using evidence from a risk analysis.

4. Access Control, Identity, and Secure Operations

Objective: *Students will demonstrate how access control and authentication protect users, devices, and secure operations.*

21) Explain the difference between authentication and authorization.
22) Compare administrative, physical, and technical controls used in secure environments.
23) Demonstrate secure account practices such as strong passwords, multifactor authentication, and role-based access.
24) Apply principles of least privilege to system users, administrators, and support personnel.
25) Describe how user permissions help protect software, records, and digital assets.
26) Analyze how unauthorized access could affect a system, application, or network.
27) Recommend secure login and user-management procedures for digital operations.
28) Evaluate access control decisions for both school-based labs and work environments.

5. Networking Fundamentals for Secure Communications

Objective: *Students will examine how networks support digital operations and analyze the cybersecurity implications of wired, wireless, and internet-connected systems.*

29) Identify common LAN, WAN, and wireless networking concepts used in cybersecurity.
30) Describe how networks enable communication between devices, services, sensors, and cloud platforms.
31) Explain the purpose of topologies, perimeter networks, and segmented communication systems.
32) Summarize the role of Ethernet, cabling, wireless standards, and routing in connected systems.
33) Interpret the functions of DNS, DHCP, NAT, IP addressing, and subnetting in network communication.
34) Compare the OSI and TCP/IP models and relate them to network communications and data transfer.
35) Analyze how insecure wireless connections can expose drones to interception, spoofing, or unauthorized control attempts.

36) Design a basic secure network diagram that includes devices, connections, and protective measures.

6. Securing Platforms, Workstations, and Endpoints

Objective: *Students will investigate threats to devices and systems and apply security practices that protect computers, endpoints, and technical equipment.*

37) Identify common threats such as malware, phishing, social engineering, weak passwords, and insecure software.
38) Explain how endpoint security protects laptops, tablets, controllers, and workstations.
39) Describe the security role of updates, patches, antivirus tools, and secure configurations.
40) Distinguish between threats, vulnerabilities, and attacks in a systems environment.
41) Analyze how physical and digital security controls work together to secure a technology ecosystem.
42) Demonstrate safe procedures for storing, updating, and maintaining firmware and support software.
43) Evaluate common weaknesses in mission devices, portable media, and removable storage.
44) Propose ways to protect digital assets, captured media, and telemetry records from unauthorized access.

7. Cyber Threats to Connected Systems and Digital Data

Objective: *Students will evaluate how cyber threats can disrupt systems and recommend strategies to protect data, communications, and digital operations.*

45) Explain how cybersecurity threats can affect mission planning, flight execution, data collection, and post-flight analysis.
46) Identify risks involving interception, jamming, spoofing, signal loss, and insecure data transfer.
47) Analyze how compromised data could affect mapping, inspection, research, media, or public safety technology applications.
48) Assess the importance of securing geolocation data, imagery, video, and sensor outputs.
49) Compare security risks for autonomous, remotely piloted, and internet-connected drone systems.
50) Recommend protective practices for setup, active use, and post-use cybersecurity.
51) Investigate case studies involving cyber incidents or operational failures tied to connected systems.
52) Create a basic cybersecurity checklist for secure digital operations.

8. Command-Line Tools, Monitoring, and Troubleshooting

Objective: *Students will use technical tools to inspect networks, troubleshoot connectivity, and support secure systems.*

53) Identify common networking and command-line tools used to examine systems and connections.
54) Explain how security analysts use diagnostic tools to test and troubleshoot networks.
55) Interpret the output of common network utilities in a school lab or other environment.

56) Use technical vocabulary to describe connectivity issues, device communication problems, and network status.
57) Construct a troubleshooting flowchart for addressing basic network or mission communication problems.
58) Analyze evidence from simple diagnostics to determine possible causes of system issues.
59) Document findings clearly using cybersecurity terminology.
60) Recommend next steps for remediation based on observed symptoms.

9. Data Protection, Backups, and Cryptography

Objective: *Students will apply methods of data protection and explain how cryptography supports confidentiality, integrity, and secure communication.*

61) Describe the purpose of backups, secure storage, and recovery planning.
62) Explain how permissions and file protections help prevent unauthorized access to digital data.
63) Differentiate between symmetric and asymmetric encryption.
64) Summarize the historical development and modern use of cryptography.
65) Analyze how encryption protects data in transit and data at rest.
66) Apply secure handling practices to images, video files, logs, and reports.
67) Evaluate when encryption, backup procedures, and access restrictions should be used in digital operations.
68) Create a secure data-handling plan for a classroom technology project.

10. Final Project Assessment

Objective: *Students will synthesize cybersecurity knowledge and technical skills by completing a final project that demonstrates secure operations, risk analysis, data protection, and professional communication.*

69) Design and complete a final project that applies cybersecurity concepts to a system, process, or data scenario.
70) Develop a project plan that identifies goals, tasks, tools, timelines, and expected deliverables.
71) Apply appropriate cybersecurity safeguards to protect systems, communications, and mission data within the project.
72) Analyze project decisions using evidence from risk assessment, troubleshooting results, or data protection requirements.
73) Create a professional product such as a report, presentation, checklist, diagram, or demonstration that communicates project findings clearly.
74) Evaluate project outcomes and recommend improvements based on performance, security, and operational considerations.

11. Leadership

Objective: *Students will demonstrate leadership, collaboration, and professionalism while participating in cybersecurity and technology-related learning experiences.*

75) Demonstrate leadership skills such as initiative, responsibility, adaptability, and ethical decision-making in classroom and project settings.

76) Collaborate effectively with peers by contributing ideas, listening actively, and supporting shared project goals.
77) Apply professional communication skills when presenting technical information, participating in discussions, and responding to feedback.
78) Practice time management, organization, and accountability to meet deadlines and project expectations.
79) Reflect on personal strengths, growth areas, and leadership contributions in technical and team-based environments.

12. Work-Based Learning

Objective: *Students will connect classroom cybersecurity knowledge to workplace expectations, career readiness, and real-world applications in technology and engineering environments.*

80) Identify workplace roles and responsibilities related to cybersecurity, engineering, and technical support.
81) Describe how employability skills such as communication, teamwork, punctuality, and problem solving contribute to workplace success.
82) Analyze real workplace scenarios involving secure operations, data handling, or technical troubleshooting.
83) Demonstrate readiness for work-based learning experiences through professional behavior, documentation, and task completion.
84) Reflect on workplace experiences, industry expectations, and career goals to inform future education and employment plans.

13. Career and Technical Student Organizations

Objective: *Using the CTSO Resource Document, chapter activities will provide some of the best opportunities CTSO members will have to learn by doing. A successful program of work creates a positive learning atmosphere in the classroom. CTSO members learn how to accept responsibility, work as a team, manage a budget, and handle success and failure. Per the CTE Admin Handbook, CTSOs are embedded into curriculum.*

Professional Development

Prepare each member for entry into the workforce and provide a foundation for success in a career. Becoming a professional does not stop with acquiring a skill, but involves an increased awareness of the meaning of good citizenship and the importance of labor and management in the world of work.

Community Service

Promote and improve goodwill and understanding among all segments of the community through services donated by CTSO chapters, and to instill in its members a lifetime commitment to community service.

Business and Industry Connections

Increase awareness of quality job practices and attitudes, and increase the opportunities for employer engagement and eventual employment.

Financial Leadership

Plan and participate in activities to allow all members to carry out the chapter's projects. Educate members on their own personal finance for current and future success.

Public Relations

Make the general public aware of the good work that students in career and technical education are doing to better themselves and their community, state, nation, and world.

Social Activities

To increase cooperation in the school and community through activities that allow CTSO members to get to know each other in something other than a business or classroom setting.

Academic Standards Alignment

Colorado CTE courses are required to integrate academic and essential skills into course content. The following academic standards have been identified as aligned to this course and should be integrated throughout instruction.

CO CTE Academic Standards Resources (Rubrics, integration strategies, etc)
CDE Colorado Academic Standards Online (Online standards lookup tool)

Note: Mathematics and Science standards will be added in the future. Visit the Colorado Academic Standards page for the most current version.

Reading, Writing and Communicating Crosswalk

Course: Cybersecurity 1
Colorado Academic Standards – Reading, Writing, and Communicating

Standard	Prepared Graduate Competency	Description	Course Evidence / Alignment
Standard 1: Oral Expression and Listening	Prepared Graduate 1 – Collaboration	Collaborate effectively as group members or leaders.	Students work collaboratively to analyze security threats and vulnerabilities, discuss ethical security practices and risk management scenarios, and contribute solutions during cybersecurity tasks.
Standard 1: Oral Expression and Listening	Prepared Graduate 2 – Oral Presentations	Deliver effective oral presentations for varied audiences and varied purposes.	Students verbally explain cybersecurity concepts, present findings from breach research or risk assessments, and communicate technical security information clearly to both technical and nontechnical audiences.

Standard 2: Reading for All Purposes	Prepared Graduate 4 – Informational Texts	Read a wide range of informational texts to build knowledge.	Students read and interpret technical cybersecurity documentation, network diagrams, policies, security guidelines, and reports on real-world cyber incidents.
Standard 2: Reading for All Purposes	Prepared Graduate 5 – Language in Context	Understand how language functions in different contexts.	Students use discipline-specific cybersecurity vocabulary accurately and interpret technical, legal, and ethical terminology in policy, reporting, and technical explanation contexts.
Standard 3: Writing and Composition	Prepared Graduate 6 – Craft arguments	Craft arguments using techniques specific to the genre.	Students justify security decisions, argue for appropriate safeguards based on risk analysis and evidence, and defend ethical and compliance-based cybersecurity practices.
Standard 3: Writing and Composition	Prepared Graduate 7 – Informational Writing	Craft informational/explanatory texts using techniques specific to the genre.	Students produce written explanations of cybersecurity principles, technical descriptions of threats and countermeasures, and documentation explaining security configurations and policies.
Standard 3: Writing and Composition	Prepared Graduate 9 – Writing Process	Demonstrate mastery of their own writing process.	Students draft, revise, and refine cybersecurity reports and explanations

			while applying correct terminology, formatting, and professional technical writing conventions.
Standard 4: Research Inquiry and Design	Prepared Graduate 10 – Research and Ethics	Gather information from a variety of sources; analyze and evaluate its quality and relevance.	Students research current cybersecurity breaches and standards, analyze threats and vulnerabilities, and use information ethically to inform risk management and security decisions.

Free Resource Links

1. Career Exploration and Postsecondary Opportunities

- Bureau of Labor Statistics Cybersecurity Careers (cybersecurity careers job outlook education pathways)
  https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
- FAA Unmanned Aircraft Systems Careers (drone careers FAA certification aviation pathways)
  https://www.faa.gov/uas
- CareerOneStop Technology Careers (career exploration certifications training pathways)
  https://www.careeronestop.org
- CyberSeek Career Pathway Tool (cybersecurity roles workforce skills certifications)
  https://www.cyberseek.org

2. Foundations of Cybersecurity and System Security

- CISA Cybersecurity Basics (security fundamentals CIA triad cyber threats overview)
  https://www.cisa.gov/cybersecurity
- Cisco Introduction to Cybersecurity (cybersecurity basics networking threats security concepts)
  https://www.netacad.com
- Kaspersky Cybersecurity Resource Center (cyber threats malware data protection basics)
  https://www.kaspersky.com/resource-center
- IBM Cybersecurity Overview (cybersecurity concepts data protection systems security)
  https://www.ibm.com/topics/cybersecurity

3. Risk Management, Safety, and Security Compliance

- NIST Cybersecurity Framework Overview (risk management framework security standards best practices)
  https://www.nist.gov/cyberframework
- ISO 27001 Information Security Basics (security standards compliance risk management)
  https://www.iso.org/isoiec-27001-information-security.html
- SANS Risk Management Resources (risk assessment vulnerabilities mitigation strategies)
  https://www.sans.org
- CISA Risk Management Guide (risk identification mitigation incident response planning)
  https://www.cisa.gov

4. Access Control, Identity, and Secure Operations

- Microsoft Learn Identity and Access Management (authentication authorization identity security)
  https://learn.microsoft.com
- Auth0 Identity Basics (authentication authorization identity systems security basics)
  https://auth0.com/learn
- Cloudflare Access Control Basics (access control security permissions authentication)
  https://www.cloudflare.com/learning

- Cybersecurity and Infrastructure Security Agency Identity Management (identity systems access control authentication)
  https://www.cisa.gov

5. Networking Fundamentals for Secure Communications

- Cisco Networking Basics (LAN WAN networking protocols communication systems)
  https://www.netacad.com
- Cloudflare Learning Network Fundamentals (networking basics DNS IP addressing internet infrastructure)
  https://www.cloudflare.com/learning
- Khan Academy Internet Basics (network communication protocols internet data transfer)
  https://www.khanacademy.org/computing
- GeeksforGeeks Networking Concepts (network models TCP IP OSI protocols overview)
  https://www.geeksforgeeks.org/computer-network-tutorials

6. Securing Platforms, Workstations, and Endpoints

- NSA Cybersecurity for Devices (device security endpoint protection system hardening)
  https://www.nsa.gov
- CISA Securing Devices Guide (endpoint security updates patch management protection)
  https://www.cisa.gov
- Avast Cybersecurity Basics (malware phishing endpoint protection practices)
  https://www.avast.com
- CrowdStrike Endpoint Security Overview (endpoint protection threats detection mitigation)
  https://www.crowdstrike.com

7. Cyber Threats to Connected Systems and Digital Data

- DHS Drone Security Awareness (drone threats security risks UAS vulnerabilities)
  https://www.dhs.gov
- MITRE ATT and CK Framework (cyber threats attack techniques threat analysis)
  https://attack.mitre.org
- CISA Threat and Vulnerability Resources (threat analysis vulnerabilities cyber risks)
  https://www.cisa.gov
- ENISA Drone Cybersecurity Guidelines (drone cybersecurity risks data protection aviation security)
  https://www.enisa.europa.eu

8. Command-Line Tools, Monitoring, and Troubleshooting

- Microsoft Command Line Basics (command line tools system diagnostics troubleshooting)
  https://learn.microsoft.com
- Linux Command Guide Ubuntu (command line tools networking diagnostics system monitoring)
  https://ubuntu.com/tutorials

- GeeksforGeeks Networking Commands (network diagnostics ping traceroute troubleshooting tools)
  https://www.geeksforgeeks.org
- Cisco Network Troubleshooting Basics (network diagnostics troubleshooting connectivity analysis)
  https://www.netacad.com

9. Data Protection, Backups, and Cryptography

- IBM Encryption Basics (encryption data protection symmetric asymmetric cryptography)
  https://www.ibm.com/topics/encryption
- Khan Academy Cryptography (cryptography fundamentals encryption algorithms security)
  https://www.khanacademy.org/computing
- Backblaze Backup Guide (data backup recovery storage protection strategies)
  https://www.backblaze.com
- Cloudflare Encryption Overview (encryption data in transit data protection security)
  https://www.cloudflare.com/learning

10. Final Project Assessment

- PBLWorks Projects and Resources (project-based learning final products rubrics assessment tools)
  https://www.pblworks.org/resources-overview
- Purdue CERIAS K-12 Teaching Resources (cybersecurity lessons presentations classroom project resources)
  https://www.cerias.purdue.edu/site/education/k-12/teaching_resources/lessons_presentations/
- CYBER.ORG Free Cyber Curricula (cybersecurity curriculum project ideas career-connected learning)
  https://cyber.org/
- University of Colorado Boulder Rubrics Guide (rubrics assessment criteria feedback student self-assessment)
  https://www.colorado.edu/center/teaching-learning/teaching-resources/assessment/assessing-student-learning/rubrics

11. Leadership

- National Clearinghouse for Leadership Programs (leadership development student leadership frameworks resources)
  https://nclp.umd.edu/
- University of Washington Student Leadership Competencies (leadership competencies reflection community engagement teamwork)
  https://cele.uw.edu/site/assets/files/1211/guide_to_building_student_leadership_competencies_for_community_based_engagement.pdf
- University of Oregon Career Preparation Toolkit (leadership professionalism teamwork career competencies)
  https://teaching.uoregon.edu/career-preparation-toolkit

- NACE Career Readiness Competencies (leadership professionalism teamwork communication employability skills)
  https://www.naceweb.org/career-readiness/competencies/career-readiness-defined/

12. Work-Based Learning

- Colorado CTE Homepage (Colorado CTE resources work-based learning toolkit program guidance)
  https://cteincolorado.org/
- Colorado Community College System Work-Based Learning (work-based learning apprenticeships employer partnerships career pathways)
  https://cccs.edu/academic-student-affairs/workforce-development/work-based-learning/
- Colorado Community College System K-12 CTE Programs (career pathways mentoring work experience college and career readiness)
  https://cccs.edu/our-colleges/programs/k-12-cte-programs/
- CTE Learn Free Resources (CTE professional development employability career readiness instructional supports)
  https://www.ctelearn.org/

Technology Student Association – National Competitive Events

Software Development

Objective: *Students will design, implement, test, document, and present a software project with educational or social value aligned with TSA Software Development competition requirements.*

- Analyze the annual TSA Software Development theme and identify a societal need that can be addressed through software.
- Design a software tool, dashboard, interface, model, or application that responds to the selected need.
- Develop a functioning software solution using an appropriate programming language, platform, or development environment.
- Test and refine the project to improve functionality, usability, reliability, and accuracy.
- Document the software's purpose, design process, features, code structure, testing, and revisions.
- Submit the required code, URL, or PDF by the TSA deadline.
- Present the project's functionality, design process, and value, then respond to judge questions about the code.

Resources

- Technology Student Association – Software Development competition guidelines https://tsaweb.org/competitions-programs/tsa/themes-problems
- Cybersecurity & Infrastructure Security Agency – Cybersecurity resources https://www.cisa.gov/cybersecurity
- OWASP – Web application security resources https://owasp.org/
- GitHub Docs – Version control and project collaboration https://docs.github.com/

Technology Student Association – National Competitive Events

Data Science and Analytics

Objective: *Students will collect, analyze, visualize, document, and present a data set connected to the annual TSA Data Science and Analytics theme.*

- Research the annual TSA Data Science and Analytics theme and identify a focused topic for investigation.
- Collect or compile a data set of at least 500 rows from credible and relevant sources.
- Analyze data to identify trends, patterns, relationships, limitations, and possible predictions.
- Create a digital scientific poster that communicates the research question, data source, visualizations, analysis, and findings.
- Prepare a documentation portfolio explaining methods, data collection, analysis, conclusions, and resources.
- Present the digital scientific poster within the TSA time limit using clear, evidence-based communication.
- Complete an on-site semifinal challenge by creating a visual representation and brief synopsis from a provided data set.

Resources

- Technology Student Association – Data Science and Analytics competition guidelines https://tsaweb.org/competitions-programs/tsa/themes-problems
- Kaggle Datasets – Public data sets for analysis https://www.kaggle.com/datasets
- Google Dataset Search https://datasetsearch.research.google.com/
- Tableau Public – Data visualization tools https://public.tableau.com/

Technology Student Association – National Competitive Events

Debating Technological Issues

Objective: *Students will research, document, organize, and defend evidence-based arguments about technological issues in alignment with TSA Debating Technological Issues competition requirements.*

- Research the annual TSA debate topic and related subtopics from credible sources.
- Prepare a one-page summary of references using MLA format according to TSA competition requirements.
- Develop evidence-based pro and con arguments for multiple technological issue subtopics.
- Organize claims, evidence, reasoning, cross-examination questions, and rebuttal points for timed debate rounds.
- Use clear, concise, and persuasive language appropriate for a formal debate setting.
- Respond to opposing arguments through questioning, analysis, and rebuttal.
- Evaluate debate performance using TSA criteria for research, argument quality, communication, reasoning, and professionalism.

Resources

- Technology Student Association – Debating Technological Issues competition guidelines https://tsaweb.org/competitions-programs/tsa/themes-problems
- Purdue OWL – MLA Formatting and Style Guide https://owl.purdue.edu/owl/researchandcitation/mlastyle/mlaformattingandstyleguide/
- National Speech & Debate Association – Debate resources https://www.speechanddebate.org/
- Cybersecurity & Infrastructure Security Agency – Cybersecurity guidance and current issues https://www.cisa.gov/cybersecurity