First Coast Technical College
Your Future Comes First

Applied Cybersecurity Program
Student Contract and Agreement

(Y100500)

2026-2027

Revised July 2026 | Version 3.1

Document Purpose

This handbook and agreement summarizes program-specific expectations for the Applied Cybersecurity Program and supplements the FCTC Student Handbook. Students are responsible for complying with both documents. If a conflict exists, applicable district policy and the FCTC Student Handbook govern.

Table of Contents

Purpose of This Agreement

This agreement highlights program-specific policies and procedures related to student safety and well-being, attendance, academic progress, professional conduct, and the responsible use of cybersecurity tools. It is intended to support students as they enter FCTC and prepare for the information technology industry.

Program Overview and Structure

This coursework prepares students for employment in the information technology industry. Content includes, but is not limited to, foundational knowledge and skills in computer and network security, security vulnerabilities, attack mechanisms and techniques, intrusion detection and prevention, cryptographic systems, system hardening, risk identification, incident response, penetration testing, key management, access control, and recovery. Specialized instruction addresses database security, security planning and analysis, software security, and web security.

The program is designed to prepare students for employment as Computer Network Support Specialists (SOC 15-1231). These professionals analyze, test, troubleshoot, and evaluate existing network systems, including local area networks (LANs), wide area networks (WANs), cloud networks, servers, and other data communications networks. They also perform network maintenance to support reliable operation and minimize interruption.

Purpose of the Program

The program provides a coherent sequence of rigorous coursework aligned with academic standards and the technical knowledge and skills needed for continued education and cybersecurity-related careers within the Information Technology career cluster. Competency-based, applied learning supports academic knowledge, higher-order reasoning, problem-solving, professional work habits, employability skills, technical proficiency, occupation-specific skills, and an understanding of the cybersecurity field.

Program Structure

The program consists of a planned sequence of instruction with three occupational completion points (OCPs). To complete the 750-hour program, students must complete OCP A, OCP B, and the OCP C course. Courses are assigned numbers through the Statewide Course Numbering System in accordance with section 1007.24(1), Florida Statutes. Career and technical education credit is awarded on the student transcript in accordance with section 1001.44(3)(b), Florida Statutes.

OCP	Course Number	Course Title	Length
A	CTS0010	Cybersecurity Foundations	300 hours
B	CTS0014	Applied Cyber Defense	300 hours
C	CTS0019	Information Security Manager	150 hours

Program Standards

The complete program standards from the 2026-2027 Florida Department of Education curriculum framework are included in Appendix A so the student-facing policy sections remain clear and easy to navigate.

Career Ready Practices

Career Ready Practices describe the professional skills educators seek to develop in students. These practices should be taught and reinforced throughout the program with increasing levels of complexity and expectation.

No.	Career Ready Practice
1	Act as a responsible and contributing citizen and employee.
2	Apply appropriate academic and technical skills.

No.	Career Ready Practice
3	Attend to personal health and financial well-being.
4	Communicate clearly, effectively, and with reason.
5	Consider the environmental, social, and economic impacts of decisions.
6	Demonstrate creativity and innovation.
7	Employ valid and reliable research strategies.
8	Use critical thinking to make sense of problems and persevere in solving them.
9	Model integrity, ethical leadership, and effective management.
10	Plan an education and career path aligned with personal goals.
11	Use technology to enhance productivity.
12	Work productively in teams while demonstrating cultural and global competence.

Academic Success

Grades are determined according to the published grading criteria. Students may request clarification or additional feedback regarding an assignment, assessment, or course grade.

Final grades are based on scores earned through CompTIA training activities, written assignments, assessments, quizzes, laboratory activities, projects, and employability standards, including professional conduct.

Grades are posted in FOCUS, the FCTC student information system, throughout the course. Students are responsible for reviewing FOCUS regularly for grades, relevant information, and messages.

Progression Requirement

Students who do not meet the academic requirements of a course or complete required skills, coursework, and remediation will not be permitted to progress to the next course and may be withdrawn from the program. Students may apply to repeat a course; all associated tuition and fees are the student's responsibility.

Grade Categories

Classification	Weight
Assessments	**40%**
Classwork and Homework	**30%**
Employability and Labs	**30%**

Grade and Work-Ethic Scale

Grade	Percentage	Work Ethic	Definition
A	90%-100%	4	Consistently exceeds occupational expectations. Demonstrates excellent preparation, participation, task completion, teamwork, communication, responsibility, and professional conduct.
B	80%-89%	3	Meets occupational expectations. Demonstrates reliable preparation, participation, task completion, teamwork, communication, responsibility, and professional conduct.

Grade	Percentage	Work Ethic	Definition
C	70%-79%	2	Demonstrates developing performance and meets minimum occupational expectations. Improvement may be needed in consistency, preparation, participation, task completion, or professional conduct.
D	60%-69%	1	Does not consistently meet occupational expectations. Significant improvement is needed in preparation, participation, task completion, responsibility, or professional conduct.
F	Below 60%	0	Does not meet occupational expectations. Performance reflects serious deficiencies in academic progress, task completion, responsibility, or professional conduct.
IP	N/A	N/A	Course in progress; not yet complete.

Honor Graduate Requirements

Requirement	Standard
Academic Performance	Earn a grade of 90% or higher in every course.
Professional Conduct	Have no documented disciplinary actions.
Program Completion	Complete all required courses before the graduation date.
Attendance	Attend at least 90% of scheduled program instructional hours.

Academic Integrity and Academic Support

Students are expected to uphold high standards of integrity, professionalism, and scholarship. Cheating, plagiarism, unauthorized collaboration, falsification of work, violations of testing conditions, complicity in dishonest behavior, and other forms of academic misconduct are prohibited.

Unauthorized or undisclosed use of generative artificial intelligence or other digital tools is also prohibited. Any permitted use of artificial intelligence must be expressly authorized by the instructor and appropriately disclosed or cited. Violations may result in disciplinary action, up to and including dismissal, in accordance with FCTC and district procedures.

Academic Course Materials

No outside course materials are required for this program unless students are notified otherwise by the instructor or FCTC administration.

Program Academic Support

Your instructor is available to help you succeed. If you have questions or begin having difficulty with course content, assignments, or required skills, speak with your instructor as early as possible. Asking for help early gives you the best opportunity to stay on track.

Your instructor may provide clarification, feedback, individual assistance, additional practice, or remediation. These supports are intended to help you master the required skills and content. Remediation is generally completed outside official class time and does not add hours to recorded attendance. Students are expected to complete assignments and participate in recommended support.

If you continue to have difficulty after support has been provided, your instructor and the Program Dean will review your progress with you and discuss the best next steps. In some cases, repeating the course or withdrawal from the current course or program may be necessary.

Cybersecurity Laboratory and Acceptable Use

Hands-on laboratory activities are an essential component of this program. Students will use computer systems, networks, virtual environments, software tools, and other resources to develop technical competence, problem-solving skills, and professional judgment.

Laboratory Expectation	What It Means
Authorized Scope	Use cybersecurity tools only within instructor-approved laboratory environments and only for assigned educational purposes. Do not scan, access, test, disrupt, alter, or attempt to compromise any device, account, network, website, cloud service, or data source outside the authorized scope of an assignment.
Safety and Equipment Care	Follow all applicable college, district, classroom, laboratory, and network safety procedures. Treat all equipment with care and ask the instructor before proceeding whenever proper use or safety is uncertain.
Approved Technology	Use only instructor-approved software, hardware, tools, websites, cloud services, virtual machines, removable media, and network connections. Do not install, download, execute, or configure unauthorized software, scripts, tools, browser extensions, or hardware.
Personal Devices and Removable Media	Do not connect personal phones, tablets, computers, USB drives, or other electronic devices to school workstations or networks without instructor approval.
Shadow IT	Do not use unapproved technology, systems, services, or devices without the instructor's direct knowledge and permission.
Credentials and Sensitive Data	Protect passwords, credentials, access tokens, student records, institutional information, and other sensitive data. Do not share credentials or attempt to obtain another person's credentials.
Vulnerability and Incident Reporting	Report suspected vulnerabilities, security incidents, policy violations, or accidental exposure of information to the instructor immediately. Do not independently exploit or publicize a suspected vulnerability.
Monitoring and Supervision	Internet and network activity conducted through school systems may be monitored in accordance with applicable policy. Remain in the classroom or laboratory outside scheduled class hours only with instructor permission and supervision.

Stop and Ask

When you are uncertain whether a tool, system, device, network, or activity is authorized, stop and ask the instructor before proceeding.

Violations of these requirements may result in loss of technology privileges, academic consequences, disciplinary action, referral for administrative review, and/or dismissal from the program, depending on the nature and severity of the conduct.

Course Expectations

Area	Student Expectation
Preparation and Participation	Arrive on time, prepared, appropriately dressed, and ready to learn. Be present when daily activities are reviewed, announcements are made, and important program information is provided.
Identification and Dress	Wear the required FCTC uniform and student identification badge.
Assignments and Communication	Complete and submit assignments by the established deadline. Communicate promptly with the instructor when circumstances may affect attendance, participation, or assignment completion. Late work may receive reduced or no credit unless the student communicates with the instructor and receives approval for an alternate submission arrangement. Acceptance of late work is subject to the instructor's published course procedures.

Area	Student Expectation
Laboratory Participation and Safety	Participate fully in hands-on laboratory learning, apply appropriate problem-solving strategies, and follow all classroom rules, laboratory procedures, and FCTC campus safety protocols.
Workspace and Materials	Maintain a clean, orderly, and professional workspace. At the end of class, clean work surfaces, discard trash, organize chairs, return supplies and materials to designated locations, and remove books, chargers, backpacks, and other personal items unless the instructor provides alternate directions.
Food and Beverages	Consume food and beverages only in areas designated by FCTC leadership and administration.
Parking	Park only in designated paved parking spaces and display the required FCTC parking permit in the lower-left portion of the front windshield. Vehicles may be ticketed or towed for failure to comply with parking requirements.

Student Code of Conduct and Professionalism

Students are expected to conduct themselves in a professional and responsible manner. All FCTC staff members share responsibility for maintaining appropriate student conduct on campus. Conduct that substantially disrupts college operations, interferes with teaching or learning, threatens safety, or damages property may result in discipline in accordance with FCTC regulations and the St. Johns County School District Student Code of Conduct, up to and including dismissal and/or responsibility for damaged property.

Student Code of Conduct: https://www.stjohns.k12.fl.us/schoolservices/conduct/

FCTC's primary goal is to provide an educational opportunity for all students. The learning environment must remain free from disruptions that interfere with a student's right to learn or an instructor's responsibility to teach. Students must comply with the legal and ethical standards of the college.

Academic dishonesty and nonacademic misconduct may result in disciplinary action. Misconduct includes, but is not limited to, cheating, plagiarism, knowingly providing false information, forging or altering institutional documents or academic credentials, unauthorized technology use, threatening behavior, harassment, property damage, and disruptive, antagonistic, or combative conduct.

FCTC may impose disciplinary action, probation, suspension, or withdrawal when conduct is determined to be unsatisfactory. Students who believe their rights have been denied are entitled to due process and may use the grievance procedures described in the FCTC Student Handbook.

Character and Professionalism

FCTC expects students to uphold the six pillars of character described through Character Counts! of St. Johns County.

Character Counts!: ccstjohns.com

Trustworthiness	Be honest, reliable, and accountable. Do not deceive, cheat, or steal. Have the courage to do the right thing and build a positive reputation.
Respect	Treat others with courtesy and respect. Use appropriate language and behavior, consider the feelings and perspectives of others, and resolve disagreements peacefully.
Responsibility	Complete assigned responsibilities, plan ahead, persevere, use self-control, consider consequences, and accept accountability for words, actions, and attitudes.
Fairness	Follow established rules, listen to others, remain open-minded, avoid taking advantage of others, and treat people fairly.

Caring	Be kind, compassionate, considerate, grateful, and willing to assist others.
Citizenship	Contribute positively to the school and community, cooperate, stay informed, obey laws and rules, respect authority, protect the environment, and volunteer when possible.

Professional Conduct Expectations

Area	Expectation
Communication	Communicate honestly, professionally, and respectfully. Avoid loud, offensive, threatening, or profane language and gestures.
Self-Management	Take responsibility for personal conduct and refrain from displays of temper or behavior that disrupts classroom or laboratory activities.
Fair Treatment	Treat all individuals fairly, regardless of status or position, and listen respectfully to differences of opinion.
Cooperation	Demonstrate kindness, consideration, cooperation, and timely responsiveness when assistance is requested.

Cell Phones, Personal Devices, and Dress Code

Personal cell phones, earbuds, and other nonapproved devices may not be used during classroom instruction unless the instructor has authorized their use for an instructional purpose. Devices must be stored or silenced as directed by the instructor. Personal use should occur outside the classroom during approved breaks.

Dress Code for Classroom and Laboratory Settings

Students must maintain a clean, safe, and professional appearance consistent with FCTC requirements and industry expectations. Clothing or footwear that creates a safety or health hazard is not permitted.

Requirement	Standard
FCTC Identification	Wear the FCTC student identification badge at all times. A student who arrives without a badge must report to the Building A lobby and obtain a temporary visitor pass before reporting to class. A lost badge must be replaced at the student's expense.
Program Uniform	Wear the designated black FCTC-logo polo each day. A jacket or sweater may be worn over the FCTC-issued polo.
Uniform Care	Maintain uniforms in clean, professional condition. Do not add symbols, signs, writing, or other markings. Replace uniforms that become permanently damaged.
Professional Representation	Do not wear the school uniform during off-campus activities in a manner that could negatively reflect the program, profession, or college, including at bars or nightclubs.
Pants	Wear long pants at the waistline. Pants worn below the waist or at mid-hip are not permitted because they may create a safety concern.
Footwear	Wear clean, neat, business-casual footwear. Flip-flops and beach-style footwear are not permitted.
Headwear and Hoods	Hats, caps, and raised hoods are not permitted in the classroom unless approved as an accommodation or for another authorized reason.

Attendance Policy

Regular attendance is necessary to obtain the full benefit of instruction and master the knowledge and skills required for successful program completion. Punctuality, self-discipline, dependability, and effective work habits are essential career-readiness skills and are included within program employability expectations.

Program Completion Standard

Students must attend and complete at least 90% of scheduled program hours. A student who exceeds 10% absence no longer meets the attendance standard for program completion unless the Dean authorizes continued enrollment and the student completes approved additional hours. Additional tuition and fees may apply.

Attendance procedures differ by enrollment classification. Full-time secondary and full-time dual enrollment students follow the adult attendance procedure. Other dual enrollment students follow the dual enrollment attendance procedure below.

Adult CTE Students

Attendance Threshold	Required Response
3% of instructional hours missed	The instructor will submit a referral and meet with the student to review the attendance policy, identify barriers, and discuss student-driven problem-solving options.
6% of instructional hours missed	The instructor will submit a referral, and the student will meet with the Program Dean. The Dean will place the student on an attendance contract that explains expectations and the possibility of program removal for continued absences.
10% of instructional hours missed	The instructor will submit a referral, and the student will meet with the Program Dean a second time. The student no longer meets the 90% attendance standard. At the Dean's discretion, the student may be permitted to remain temporarily under an attendance contract and complete approved additional hours. The student will receive formal notice that reaching 15% absence will result in removal from class.
Six instructional days missed	The student will be withdrawn from the program. Re-entry may be considered at the next enrollment period at the Dean's discretion and is subject to program space availability.
15% of instructional hours missed	The student will be removed from the program. Any later re-entry is at the Dean's discretion and subject to program space availability.

Secondary and Dual Enrollment Students

Attendance Threshold	Required Response
Three days absent within a grading period	The instructor will meet with the student to review the Student Handbook high school attendance policy and discuss strategies to improve attendance and punctuality. The Student Advisor will notify the home high school registrar and/or school counselor.
Five days absent within a grading period	The instructor will meet with the student, review the attendance policy, and develop a pro-social action plan (PSAP). The Student Advisor will notify the home high school registrar and/or school counselor of the meeting and plan.
Ten days absent within a grading period	The instructor will notify the Student Advisor. The Student Advisor will notify the home high school registrar and/or school counselor and the program instructor regarding possible dismissal.
Fifteen total days absent during the school year	The student will be referred to the Program Dean. With the Director's support, the Dean may withdraw the student from the program. The Student Advisor will notify the home high school registrar and/or school counselor.
Appeal	The student may appeal the Dean's decision to the Review Committee.

Tardiness and Communication

Students are required to report to class on time. Tardiness and absences may affect grades, recorded program hours, financial aid, and attendance status. Instructors may refer dual enrollment students with excessive tardiness to the Program Dean. When appropriate, Student Advisors will communicate attendance concerns and available support to the student's home high school.

Students are responsible for managing attendance and communicating absences. Anticipated absences should be discussed with the instructor and Program Dean in advance. Unplanned absences must be communicated to the instructor before class begins whenever possible.

Program Schedule and Clock-Hour Requirements

The program is scheduled from 8:00 a.m. to 4:00 p.m., Monday through Friday, with an alternate summer schedule during June and July, 7:30 a.m. to 4:00p.m. Monday- Thursday. Lunch is 30 minutes. Because FCTC is a clock-hour institution, students must accurately sign in and out for each class to receive credit for hours attended.

Attendance Records

Students may not sign another student in or out. Falsifying attendance records is considered misconduct and may result in disciplinary action, up to and including dismissal.

Students are responsible for course content and assessments missed because of an absence. Unless the instructor approves an alternate arrangement, make-up work is due and missed assessments must be completed on the next class day.

During high school testing schedules, including exam weeks, students are expected to attend FCTC dual enrollment courses when there is no conflict with the home high school exam schedule.

Safety and Substance Policies

This section implements the zero-tolerance policy for crime and victimization described in section 1006.13, Florida Statutes. Zero-tolerance policies apply equally to all students regardless of economic status, race, or disability.

Weapons and Threat Offenses

Students found to have committed either of the following offenses on School Board property, on school-sponsored transportation, or during a school-sponsored activity may be expelled, with or without continuing educational services at an alternative school, for no less than one full year and may be referred to the criminal or juvenile justice system:

Offense	Policy
Firearms or Weapons	Bringing or possessing a firearm or weapon, as defined in chapter 790, Florida Statutes, and School Board Rule 8.01, at school, at a school function, or on school-sponsored transportation. A concealed-carry permit does not authorize possession on school grounds.
Threats or False Reports	Making a threat or false report, as defined in sections 790.162 and 790.163, Florida Statutes, involving school property, school personnel or their property, school transportation, or a school-sponsored activity.

Tobacco-, Alcohol-, and Illegal Substance-Free Policy

All FCTC campuses are smoke- and tobacco-free. Prohibited products include cigarettes, cigars, pipe tobacco, snuff, dip, chewing tobacco, smokeless pouches, loose-leaf or smokeless tobacco, electronic cigarettes, and vaping devices.

FCTC campuses maintain a zero-tolerance policy for the possession, consumption, distribution, or sale of alcoholic beverages, illegal drugs, unauthorized controlled substances, intoxicating substances, counterfeit or look-alike substances, marijuana, and related paraphernalia. A student who possesses, uses, distributes, or is under the influence of a prohibited substance during a school-sponsored class or activity, whether on or off school

property, may be subject to disciplinary action. The student may be removed from campus, and law enforcement may be contacted when appropriate.

Declaration of Intent

First Coast Technical College's mission is to provide career, technical, and adult education that meets the changing needs of students, businesses, and the workforce. FCTC expects students to pursue certification and/or licensure appropriate to their field. A student enrolling primarily for personal enrichment rather than certification or employment must declare that intent below.

Select One	Declaration
_____ Option 1	I intend to pursue the applicable industry certification and/or employment aligned with this program.
_____ Option 2	I am enrolling primarily for personal enrichment and acknowledge that I am not committing to pursue the applicable industry certification and/or licensure.

Student Initials _____ Date _____

Administrative Review, Due Process, and Grievance Procedures

A violation of the FCTC Student Handbook or this Applied Cybersecurity Program Student Handbook and Agreement is subject to administrative review and discipline. Depending on the nature and severity of the violation, disciplinary action may include loss of privileges, probation, suspension, withdrawal, or dismissal from the program.

Students who believe their rights have been denied are entitled to the due process and grievance procedures described in the FCTC Student Handbook.

Student Acknowledgment

I acknowledge that I have received or have been provided access to the FCTC Student Handbook and the Applied Cybersecurity Program Student Contract and Agreement. I understand that I am responsible for reviewing and complying with the policies, procedures, and expectations contained in both documents.

I understand that violations may result in administrative review and disciplinary action, up to and including dismissal, consistent with applicable FCTC and district procedures.

Student Printed Name	Student ID Number
Student Signature	Date
Program Instructor Signature	Date

Parent/Guardian Acknowledgment

Required only when the student is under 18 years of age. I acknowledge that I have reviewed the program expectations and agree to support the student in complying with the FCTC Student Handbook and the Applied Cybersecurity Program Student Handbook and Agreement.

Parent/Guardian Printed Name	Relationship to Student
Parent/Guardian Signature	Date

Dual Enrollment Student Acknowledgment

As a dual enrollment student in the Applied Cybersecurity Program, I am held to the same academic, conduct, safety, dress, technology-use, and professional standards as adult students. Attendance requirements are based on my enrollment classification as described in the Attendance Policy section of this agreement.

I have received, read, and understand the Applied Cybersecurity Program Student Handbook and Agreement. By signing, I agree to follow the program policies, rules, and guidelines and understand that compliance is a condition of acceptance and continued enrollment in the program.

Student Printed Name	Student ID Number
Student Signature	Date

Parent/Guardian Acknowledgment for Dual Enrollment Students

Required only when the student is under 18 years of age. I have reviewed and understand the Applied Cybersecurity Program Student Handbook and Agreement. By signing, I agree to support the student in complying with the program policies, rules, and guidelines.

Parent/Guardian Printed Name	Relationship to Student
Parent/Guardian Signature	Date

Appendix A: Program Standards

After successfully completing the program, the student will be able to perform the following. The standards below are reproduced from the 2026-2027 Florida Department of Education Applied Cybersecurity curriculum framework.

Outcome	Learning Standard
01.0	Demonstrate knowledge, skill, and application of computer systems.
02.0	Demonstrate knowledge of different operating systems.
03.0	Develop a familiarity with the information technology industry.
04.0	Develop an awareness of microprocessors and digital computers.
05.0	Develop an awareness of programming languages.
06.0	Develop an awareness of emerging technologies.
07.0	Demonstrate an understanding of the OSI and TCP/IP models.
08.0	Identify computer components and their functions.
09.0	Demonstrate proficiency using the Internet to locate information.
10.0	Demonstrate an understanding of Internet safety and ethics.
11.0	Demonstrate proficiency using word processing applications.
12.0	Perform email activities.
13.0	Demonstrate proficiency in using presentation software and equipment.
14.0	Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.
15.0	Describe the national agencies and supporting initiatives involved in cybersecurity.
16.0	Demonstrate an understanding of virtualization technology.
17.0	Demonstrate an understanding of basic computer components, their functions, and their operation.
18.0	Demonstrate knowledge of different operating systems.
19.0	Describe the services and protocols that operate in the application, transport, network, and data link layers of the OSI Model.
20.0	Demonstrate proficiency using computer networks.
21.0	Describe and differentiate between serial, digital subscriber line (DSL), Metro Ethernet, and cable modem WAN connections.
22.0	Demonstrate an understanding of basic security concepts.
23.0	Demonstrate an understanding of legal, ethical, and regulatory issues in cybersecurity.
24.0	Discuss the underlying concepts of terms used in cybersecurity.
25.0	Recognize and understand the administration of the following types of remote access technologies.
26.0	Understand the application of the following concepts of physical security.
27.0	Securely configure and maintain the following types of devices.
28.0	Understand the societal and security challenges of emerging technologies.
29.0	Recognize and be able to differentiate and explain the following access control models.
30.0	Understand the security concerns for the following types of media.
31.0	Explain the following security topologies as they relate to cybersecurity.

Outcome	Learning Standard
32.0	Describe the roles within teams, work units, departments, organizations, inter-organizational systems, and the larger environment.
33.0	Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.
34.0	Demonstrate an understanding of common information and computer system security vulnerabilities.
35.0	Demonstrate an understanding of common cyber attack mechanisms, their consequences, and motivation for their use.
36.0	Be able to identify and explain the following different kinds of cryptographic algorithms.
37.0	Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity.
38.0	Understand how cryptography and digital signatures address the following security concepts.
39.0	Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).
40.0	Demonstrate an understanding of certificates and their role in cybersecurity.
41.0	Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.
42.0	Demonstrate an understanding of Intrusion Detection Systems (IDS).
43.0	Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
44.0	Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
45.0	Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques.
46.0	Demonstrate an understanding of firewalls and other means of intrusion prevention.
47.0	Demonstrate an understanding of vulnerabilities unique to virtual computing environments.
48.0	Demonstrate an understanding of social engineering and its implications to cybersecurity.
49.0	Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability.
50.0	Demonstrate an understanding of how to configure host systems to guard against cyber intrusion.
51.0	Demonstrate an understanding of authentication methods and strategies.
52.0	Demonstrate an understanding of methods and strategies for controlling access to computer networks.
53.0	Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured.
54.0	Demonstrate an understanding of the processes involved in hardening a computer system or network.
55.0	Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations.
56.0	Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization.
57.0	Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes.
58.0	Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase.
59.0	Demonstrate proficiency in cybersecurity risk mitigation planning.
60.0	Demonstrate proficiency in establishing a risk management framework.
61.0	Demonstrate proficiency in creating a corporate security policy.

Outcome	Learning Standard
62.0	Demonstrate proficiency in addressing process risks.
63.0	Demonstrate proficiency in addressing physical security risks.
64.0	Demonstrate proficiency in cybersecurity contingency planning.
65.0	Demonstrate proficiency in cybersecurity disaster recovery planning.
66.0	Demonstrate proficiency in cybersecurity business continuity planning.
67.0	Demonstrate proficiency in the essential elements of forensic analysis.
68.0	Demonstrate an understanding of database design, structure, and operation.
69.0	Demonstrate a fundamental understanding of Structured Query Language (SQL).
70.0	Demonstrate an understanding of database security policies.
71.0	Demonstrate an understanding of database access control, functions, methods, and verification.
72.0	Demonstrate an understanding of database vulnerabilities, attack vectors, and associated countermeasures.
73.0	Demonstrate an understanding of pre- and post-intrusion actions to facilitate database recovery.
74.0	Demonstrate an understanding of software design, structure, and operation.
75.0	Demonstrate a fundamental understanding of common software attack vectors.
76.0	Demonstrate an understanding input syntax validation.
77.0	Demonstrate an understanding of best practices for processing input data to ensure safe and secure program code.
78.0	Demonstrate an understanding of the role of environment variables in the operation of software applications.
79.0	Demonstrate an understanding of program design strategies for inhibiting elevated privilege attacks.
80.0	Demonstrate an understanding of the primary security services used in Internet and intranet environments.
81.0	Demonstrate a fundamental understanding of the SSL protocol stack and its elements.
82.0	Demonstrate an understanding of IPsec, including its uses, elements, and mechanisms.
83.0	Demonstrate an understanding of S/MIME, including its uses, functions, cryptographic algorithms, and key certificates.
84.0	Demonstrate an understanding of Kerberos and its role in third-party authentication in a distributed network.
85.0	Demonstrate an understanding of identity management and ways in which secure identify information is exchanged across different domains.
86.0	Complete a safety skills inventory.
87.0	Demonstrate acceptable project values.
88.0	Demonstrate the ability to detect and resolve system vulnerabilities.
89.0	Plan, organize, and carry out a penetration-testing plan.
90.0	Demonstrate proficiency in conducting forensic analysis.
91.0	Successfully work as a member of a team.
92.0	Manage time according to a plan.
93.0	Keep acceptable records of progress problems and solutions.

Outcome	Learning Standard
94.0	Manage resources.
95.0	Use tools, materials, and processes in an appropriate and safe manner.
96.0	Research content related to the project and document the results.
97.0	Use presentation skills, and appropriate media to describe the progress, results and outcomes of the experience.
98.0	Demonstrate competency in the area of expertise related to the Applied Cybersecurity education program previously completed that this project is based upon.